



media5
corporation
Discover the Power of 5

Reference Manual

Mediatrix[®] 4102 **Mediatrix[®] 4102S** MGCP/NCS Version

Product Version 5.0

Document Revision 04

December 5, 2011



Media5 Corporation
4229 Garlock Street
Sherbrooke, Québec, Canada J1L 2C8

Mediatrix® 4102 Reference Manual

© 2011, 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 Mediatrix® 4102 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	xiii
Document Objectives.....	xiii
Intended Audience.....	xiii
Related Documentation	xiii
Document Structure.....	xiv
Document Conventions	xvi
Warning Definition.....	xvi
Where to find Translated Warning Definition.....	xvi
Other Conventions	xvi
SCN vs PSTN.....	xvi
Standards Supported	xvi
Obtaining Documentation	xvii
Media5 Web Site	xvii
Media5 Download Portal	xvii
Documentation Feedback	xvii
Unit Manager Network – Element Management System.....	xvii
End User Technical Support.....	xviii

Installation and Web Page Configuration

Chapter 1

Installation	3
Requirements	3
Safety Recommendations.....	3
Package Contents	3
Overview.....	4
About the Mediatrrix 4102	4
Placing a Call	4
Management Choices	5
Panels.....	5
Front Indicators	5
Rear Connectors	6
Choosing a Suitable Installation Site	7
Location.....	7
Wall-Mounting	8
Free Standing Unit	8
Condensation	8
Cleaning	8
Hardware Connection	9
Reserving an IP Address.....	9
Before Proceeding.....	9
Single Computer Installation	10
Multiple Computer Installation	12
Starting the Mediatrrix 4102 for the First Time.....	13

IP Address Discovery or Configuration	14
Initial Provisioning Sequence	15
LED Behaviour in Starting Mode	16
LED Indicators	16
Ready LED	16
In Use LED	17
ETH LED	17
Power LED	17
LED Patterns	17
Bootling LED Pattern Description.....	18
NormalMode LED Pattern Description	19
AdminMode LED Pattern Description.....	19
Recovery Mode LED Patterns	20
Reset / Default Switch	20
At Run-Time	20
At Start-Time	21
Recovery Mode	21
Factory Reset	22
Software Restart	23
Restart Behaviour.....	24
Verifying the Installation.....	24

Chapter 2

Web Interface – Introduction.....	25
Introduction	25
Using the Web Interface	25
Web Interface Access Limitation	25
System Status of the Mediatix 4102.....	27
Menu Frame	27
Content Frame	28
Submitting Changes	28

Chapter 3

Web Interface Parameters	29
System Page	29
WAN Page.....	29
LAN Page	31
STUN Page	32
Configuration File Upload Page.....	33
HTTP Server Password Page.....	34
Default User Name and Password	34
Issue: Factory Reset does not Reset the Default Password Value	35
System Log Page	36

SNMP Configuration

Chapter 4

MIB Structure and SNMP	39
SNMP Overview	39
Definitions.....	39
SNMP Versions	40
SNMP Behaviour	41
SNMPv3 Special Behaviour	42
SNMP Configuration via a Configuration File	43
MIB Structure	47
Textual Conventions.....	48
Objects, Conformance, and Events.....	48
IP Addresses	49
Persistence.....	49
Changing a Parameter Value	49
Tables	50
Generic Variables.....	50
Variables for Administrative Commands	51
SNMP Access Limitation	52
Current MIB Version	52
Sending Configuration Data to the Mediatix 4102	52
Configuration File	52
Management Information Base – MIB	52
Switching Protocols	53

Chapter 5

IP Address and Network Configuration	55
IP Addresses	55
IP Addresses Formats in the DHCP Server	55
Provisioning Source	56
Services	56
Configuration Source.....	56
Local Host	57
Static DNS.....	60
Image	61
Management Server	62
Configuration File Fetching	63
Syslog.....	63
MGCP Call Agent	64
NCS Call Agent	64
SNTP	65
LAN Connector Static IP Address.....	65
DHCP Server Configuration	66
Connection to the DHCP Behaviour	66
Network Configuration.....	67
Vendor and Site Specific DHCP Options	67
Vendor Specific Options.....	67
Site Specific Options	68
Option Codes	69
Entering IP Addresses.....	69

Entering FQDNs	70
Settings Example	71
Error Handling.....	72
DHCP Server Failures.....	72
Vendor/Site Specific Option Missing	72
DNS Failures	72
Ethernet Connection Speed.....	73
Speed and Duplex Detection Issues	73

Chapter 6

MGCP Protocol Features 75

Introduction	75
MGCP Information.....	75
Services Provided	75
Call Agent Information	76
Configuration Source.....	76
Establishing a MGCP Session	78
MGCP Commands	79
MGCP Responses.....	79
Basic Information	80
Endpoints	81
Retransmission Parameters	82
Packages	84
Setting the Default Package.....	84
Dynamic Timeout Values	84
Generic Media Package	84
DTMF Package	85
Line Package.....	85
Extended Analog Line (XL) Package	87
X-P Package	88
Redirecting to a Different Call Agent	89
Meter Pulse.....	89
MGCP Conference Mode	89
Firewall Traversal	92
Interoperability Configuration	93
Offer/Answer Model.....	93
Offered Stream Format	94
Session ID and Session Version	94
Multiple Fax Tone Detection.....	95
Connected RTP Sockets	95
UDP Checksum	95
T.38 Capabilities Using Audio Codec 98.....	96
Immediate Modem Tone Reporting	96
Brief OSI Signal	96
Fake RFC 3407 Recognition	97
T.38 Negotiation Syntax	97
Brackets Around IP Address in Domain Name	98
Polarity Reversal on Calling Card Service Tone	98

Chapter 7

NCS Protocol Features 99

Introduction	99
NCS Information	99

Services Provided	99
Call Agent Information	100
Configuration Source.....	100
Basic Information	101
Endpoints	102
Retransmission Parameters	103
Line Package	105
Encoding Name of the Payload Type 18	106
Compatibility Version	107
Interoperability Configuration	107

Chapter 8

Country-Specific Configuration 109

Caller ID Information	109
Caller ID Generation.....	109
ADSI	110
Setting the Location (Country)	110
Caller ID Selection.....	111

Chapter 9

Transparent Address Sharing..... 113

What is Transparent Address Sharing?	113
Router Mode.....	114
Cable vs DSL Modem	115
Multicast and IGMP	115
Configuration Steps.....	115
PPPoE Service	116
Enabling the PPPoE Service	116
Setting a User Name and Password	117
WAN Information Configuration Source.....	118
Configuring TAS	119
QoS Differentiated Services Fields	120
LAN Interface	120
MAC Address Spoofing	121
Enabling TAS	122
Ports Settings	123
UDP and TCP Ports	123
T.38 Base Port Range.....	123
RTP/RTCP Base Port Range	124
Restarting the Mediatix 4102.....	124
DHCP Server	125
DHCP Server Compliance.....	125
Supported DHCP Options	125
DSL Modem Specific Information	126
Establishing a Connection.....	126
Error Handling	127
Routing Mechanism	128
Blocked Ports	128
Using the Mediatix 4102 with a Low Bandwidth Connection	128
What is Considered a Low Bandwidth Connection?	128
Configuration for a Low Bandwidth Connection	129

Chapter 10

Configuration File Download	131
Configuration File Download Server	131
Configuring the TFTP Server	131
Configuring the SNTP Server	131
Configuring the HTTP Server	131
Configuration File Server Settings	131
Setting up the Configuration File Download	133
Configuration Update Status	134
Configuration Files Encryption	136
Configuration Download via TFTP	137
Configuration Download via HTTP	138
Automatic Configuration Update	139
Error Handling	141
Management Server	144
Management Server Configuration	144
Downloading from the Management Server	144
Error Handling	145
Syslog Messages	146
Configuration File Example	147
Supported Characters	147

Chapter 11

Software Download	149
Before Downloading	149
Configuring the TFTP Server	149
Configuring the SNTP Server	149
Configuring the HTTP Server	149
Software Servers Configuration	150
DHCP Configuration	150
Static Configuration	151
Download Procedure	152
Extracting the Zip File	152
Setting up the Image Path	152
Software Download Status	154
Download via TFTP	156
Download via HTTP	157
Automatic Software Update	158
Software Downgrade	160
Emergency Software Procedure	160
Using the Emergency Software	160

Chapter 12

Line Configuration	163
Lines Administrative State	163
Temporary Administrative State	163
Permanent Administrative State	164
Multiple Connections on Endpoints (Lines)	164
Flash Hook Detection	164
Loop Current	165

Chapter 13

Voice Transmissions	167
Codec Descriptions.....	167
G.711 PCMA and PCMU.....	167
G.726.....	168
G.729.....	168
Preferred Codec	169
Enabling Individual Codecs	169
Packetization Time	170
DTMF Transport Type	172
DTMF Payload Type	173
DTMF Detection.....	173
DTMF Frequencies.....	173
DTMF Detection Configuration.....	173
Adaptative Jitter Buffer	175
About Changing Jitter Buffer Values	176
Voice Activity Detection	176
G.711 and G.726 VAD	176
G.729 VAD	177
Echo Cancellation.....	178
Comfort Noise.....	178
User Gain.....	179

Chapter 14

Fax Transmission.....	181
Introduction	181
Clear Channel Fax.....	182
T.38 Fax.....	183
T.38 No-Signal	185

Chapter 15

STUN Configuration	187
What is STUN?	187
Restrictions on the Media5 STUN Implementation	187
STUN Client Configuration	188

Chapter 16

SNTP Settings.....	189
Enabling the SNTP Client.....	189
Configuration Source	190
DHCP Configuration.....	190
Static Configuration	190
Defining a Custom Time Zone	191
STD / DST	191
OFFSET	191
START / END	191
Example	192

Chapter 17

Management Server Configuration..... 193

Using the Management Server	193
Configuration Source.....	193

Chapter 18

Quality of Service (QoS) 195

Differentiated Services (DS) Field	195
IEEE 802.1q.....	196
VLAN	197
VLAN Substitution	198
VLAN ID Filtering.....	199
LAN and WAN with VLAN substitution	199

Chapter 19

Syslog Daemon 201

Syslog Daemon Configuration	201
Configuration Source.....	202
Customizing Syslog Messages	203
Configuring the Syslog Daemon Application	203
Local Syslog	204

Chapter 20

Statistics 205

MGCP / NCS Statistics	205
RTP Statistics	205
Statistics Buffers.....	205
How are Statistics Collected?.....	206
Example	206

Chapter 21

Maximum Transmission Unit (MTU) 209

What is MTU?	209
Mediatrix 4102 MTU	209
Possible Hardware Problem	209

Chapter 22

Troubleshooting 211

General Operation Issues.....	211
Calling Issues	214
Fax Issues	215
Software Upgrade Issues	216
SNMP Management Software Issues.....	217

Appendices

Appendix A

Standards Compliance and Safety Information	223
Standards Supported	223
Disclaimers	224
Federal Communications Commission (FCC) Part 15	224
CE Marking	224
RoHS China	225
Translated Warning Definition	226
Safety Warnings	227
Circuit Breaker (20A) Warning	227
TN Power Warning	227
Product Disposal Warning	227
No. 26 AWG Warning	227
WAN, LAN, Phone-Fax 1 and Phone-Fax 2 Connectors Warning	227
LAN and FXS Ports Connectors Warning	228
Socket Outlet Warning	228
Safety Recommendations	228

Appendix B

Standard Hardware Information	229
Industry Standard Protocols	229
Hardware Features	230
Display	230
Interfaces	230
Power	230
Casing / Installation	230
Product Architecture Details	230
Real Time Fax Router Technical Specifications	231
Analog Line Interface (FXS)	231
Audio Specifications	232
DTMF Tone Detection	232
DTMF Tone Generation	232
MTBF Value	232
Power Consumption	233
Measurements at the DC input	233
Operating Environment	233
Dimensions and Weight	233
Warranty	233

Appendix C

Cabling Considerations	235
RJ-45 Cable	235
Straight Through Cable	235
Crossover Cable	236
RJ-11 (Telephone) Cable	237
Wiring Conventions	237

Appendix D

Country-Specific Parameters	239
Definitions	239
Supported MGCP/NCS Signals	240
Conventions	240
Australia	242
Australia 1	242
Australia 2	243
Austria	244
Austria 1	244
Austria 2	245
China	246
France	247
Germany	248
Germany 1	248
Germany 2	249
Hong Kong	250
Indonesia	251
Israel	252
Italy	253
Japan	254
Malaysia	255
Netherlands	256
North America	257
North America 1	257
North America 2	258
Russia	259
Spain	260
Sweden	261
Switzerland	262
Thailand	263
United Arab Emirates	264
UK	265

Appendix E

Glossary	267
-----------------------	------------

Appendix F

List of Acronyms	275
-------------------------------	------------

Appendix G

List of MIB Parameters	277
-------------------------------------	------------



About this Manual

Thank you for purchasing the Mediatrix 4102 from Media5.

The Mediatrix 4102 offers two Ethernet connectors switches enabling to establish two connections between conventional analog telephones or Group 3 fax machines and either a WAN, a LAN or a personal computer. It can be used to provide connectivity to broadband access equipment for a Service Provider's IP Telephony offering to residential or SME markets. There are two Mediatrix 4102 models:

Table 1: Mediatrix 4102 Models

Model	Interfaces	VoIP Call Capacity	Additional Memory
Mediatrix 4102	2 FXS ports	up to 2	No
Mediatrix 4102S	2 FXS ports	up to 2	Yes

To ensure maximum flexibility, the Mediatrix 4102 can:

- ▶ dynamically detect the most commonly used IP Telephony codecs and fax protocols, including T.38
- ▶ be auto-provisioned and remotely managed and upgraded

Document Objectives

The *Mediatrix 4102 Reference Manual* provides technical information for the Mediatrix 4102.

Use the *Mediatrix 4102 Reference Manual* in conjunction with the appropriate publications listed in ["Related Documentation" on page xiii](#).

Intended Audience

This manual provides all the technical information needed to install and manage the Mediatrix 4102. It is intended for network administrators and system managers who install and set up network equipment; consequently, it assumes a basic working knowledge of LANs.

From the perspective of the LAN administrator, a Mediatrix 4102 presents itself like another device to add to the LAN. It requires the same kind of TCP/IP addressing. The Mediatrix 4102 can also use a DHCP server on the LAN to automatically receive its IP configuration assignment.

Related Documentation

In addition to this manual, the Mediatrix 4102 document set includes the following:

- ▶ *MIB Reference Manual*
Lists and explains all parameters in the MIB structure.
- ▶ *Mediatrix 4102 Quick Start Guide*
This printed booklet allows you to quickly setup and work with the Mediatrix 4102.

► *Third Party Software Copyright Information*

This document lists the third-party software modules used in the Mediatrix 4102 along with any copyright and license information. This document is available at: <http://www.media5corp.com/downloads>

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

Document Structure

The Mediatrix 4102 Reference Manual has three parts:

- [“Installation and Web Page Configuration” on page 1](#). This part describes the installation scenarios of the Mediatrix 4102 and how to configure the unit via its web interface.
- [“SNMP Configuration” on page 37](#). This part describes all SNMP-related parameters of the Mediatrix 4102.
- [“Appendices” on page 221](#). This part contains supplemental information useful to the reader.

The Mediatrix 4102 Reference Manual contains the following information.

Table 2: Mediatrix 4102 Reference Manual Chapter/Appendices

Title	Summary
Installation	
“Chapter 1 - Installation” on page 3	Describes the installation of the Mediatrix 4102. Also presents the possible states and LED patterns of the Mediatrix 4102, as seen from an operator perspective.
“Chapter 2 - Web Interface – Introduction” on page 25	Describes how to access the embedded web server of the Mediatrix 4102 to set parameters by using the HTTP protocol.
“Chapter 3 - Web Interface Parameters” on page 29	Describes the web page parameters.
SNMP Configuration	
“Chapter 4 - MIB Structure and SNMP” on page 39	Describes how the Mediatrix 4102 uses the SNMP protocol for its configuration.
“Chapter 5 - IP Address and Network Configuration” on page 55	Describes how to set IP information in the Mediatrix 4102 and how to configure a DHCP server.
“Chapter 6 - MGCP Protocol Features” on page 75	Describes how to set information exclusive to the Media Gateway Control Protocol (MGCP).
“Chapter 7 - NCS Protocol Features” on page 99	Describes how to set information exclusive to the Network-based Call Signalling (NCS) protocol.
“Chapter 8 - Country-Specific Configuration” on page 109	Describes how to set the Mediatrix 4102 with the proper country settings.
“Chapter 9 - Transparent Address Sharing” on page 113	Explains how to properly configure the Transparent Address Sharing service for a cable or DSL modem.
“Chapter 10 - Configuration File Download” on page 131	Describes how to use the configuration file download feature to update the Mediatrix 4102 configuration.
“Chapter 11 - Software Download” on page 149	Describes how to download a software version available on the designated software server into the Mediatrix 4102.

Table 2: Mediatrix 4102 Reference Manual Chapter/Appendices (Continued)

Title	Summary
“Chapter 12 - Line Configuration” on page 163	Describes the features available on the lines connected to the Mediatrix 4102.
“Chapter 13 - Voice Transmissions” on page 167	Describes the various codecs the Mediatrix 4102 supports for transmitting audio signals.
“Chapter 14 - Fax Transmission” on page 181	Describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 4102.
“Chapter 15 - STUN Configuration” on page 187	Describes how to configure the STUN client of the Mediatrix 4102.
“Chapter 16 - SNTP Settings” on page 189	Describes how to configure the Mediatrix 4102 to enable the notion of time (date, month, time) into it.
“Chapter 17 - Management Server Configuration” on page 193	Describes how to configure the Mediatrix 4102 to connect to a module or software that is used to remotely set up Mediatrix units.
“Chapter 18 - Quality of Service (QoS)” on page 195	Defines the QoS (Quality of Service) features available on the Mediatrix 4102.
“Chapter 19 - Syslog Daemon” on page 201	Describes how to configure and use the Syslog daemon.
“Chapter 20 - Statistics” on page 205	Defines the statistics the Mediatrix 4102 can collect.
“Chapter 21 - Maximum Transmission Unit (MTU)” on page 209	Describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 4102.
“Chapter 22 - Troubleshooting” on page 211	Examines some of the problems you may experience when connecting the Mediatrix 4102 to the network and provides possible solutions.
Appendices	
“Appendix A - Standards Compliance and Safety Information” on page 223	Lists the various standards compliance of the Mediatrix 4102.
“Appendix B - Standard Hardware Information” on page 229	Lists the technical hardware information of the Mediatrix 4102.
“Appendix C - Cabling Considerations” on page 235	Describes the pin-to-pin connections for cables used with the Mediatrix 4102.
“Appendix D - Country-Specific Parameters” on page 239	Lists the various parameters specific to a country such as loss plan, tones and rings, etc.

Document Conventions

The following information provides an explanation of the symbols that appear on the Mediatrix 4102 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, see [“Appendix A - Standards Compliance and Safety Information” on page 223.](#)

This Appendix describes the international agency compliance and safety information for the Mediatrix 4102. It also includes a translation of the safety warning listed in the previous section.

Other Conventions

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



Caution: 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: Note indicates important information about the current topic.

Standards Supported

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



This symbol indicates you can also set the current configuration by using the Unit Manager Network Graphical User Interface. The text will provide the location in the *Unit Manager Network Administration Manual* where to find information related to the specific configuration.

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.

Standards Supported

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

The Mediatrix 4102'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>.

Obtaining Documentation

These sections explain how to obtain documentation from Media5.

Media5 Web Site

Media5 offers the latest version of its products' documentation on its web site. You will thus be able to access and download the most current Media5 documentation. Follow this link: <http://www.media5corp.com/en/documentation>.



Note: This site does not contain any firmware versions.

Media5 Download Portal

Media5 offers online documentation via a self register web-portal. You will thus be able to access and download the most current Media5 documentation. Follow this link to register: <http://www.media5corp.com/en/support-portal>.



Note: This site does not contain any firmware versions.

Documentation Feedback

Media5 welcomes your evaluation of this manual and any suggestions you may have. These help us to improve the quality and usefulness of our publications.

Please send your comments to:

Media5 Corporation
Attention: Documentation Department
4229, Garlock Street
Sherbrooke, Quebec
Canada J1L 2C8
FAX: +1 (819) 829-5100

We appreciate your comments.

Unit Manager Network – Element Management System

The Unit Manager Network is a user-friendly element management system designed to facilitate the deployment, configuration and provisioning of Mediatrix access devices and gateways.

The Unit Manager Network offers the following key features, enabling the simple and remote configuration and deployment of numerous Mediatrix units:

- ▶ Detection of the state of each Mediatrix unit (e.g. power on/off).
- ▶ Automatic update of the list with installation of new Mediatrix units.
- ▶ Real-time graphical presentation of actual configuration.
- ▶ Tracking of all configuration options of the Mediatrix units on the network.
- ▶ Control of configuration parameters of all Mediatrix units within the same network.
- ▶ Storage of backup configuration file of each Mediatrix unit.
- ▶ Display of firmware release for any Mediatrix unit.
- ▶ Field-upgrade of all Mediatrix units.
- ▶ Controlled Implementation of new software.

- ▶ Supports SNMP requests: GET, GET NEXT, GET TABLE, GET WALK, SET, TRAP.
- ▶ SNMP abstraction layer: configuration can be changed without SNMP MIB knowledge.

The demo version of the Unit Manager Network is available on the Media5 Download Portal at: <https://support.mediatrix.com/DownloadPlus/Download.asp>.

See the *Unit Manager Network Administration Manual* for more details on how to use it to configure any Mediatrix 4102 unit on the network.

End User Technical Support

In order to maximize technical support resources, Media5 works through its partners to resolve technical support issues. All end users requiring technical support are encouraged to contact their vendor directly.

Installation and Web Page Configuration

Page Left Intentionally Blank

This chapter describes the installation and initial provisioning of the Mediatrix 4102.

Requirements

The Mediatrix 4102 requires the following items to work properly:

Table 3: Required Items

Item	Description
DHCP Server (optional)	Supplies network parameters to the Mediatrix 4102. This applies to the DHCP connection type (usually with a cable modem installation).
DNS Server (optional)	Translates domain names into IP addresses.
Call Agent	Manages the active calls of the Mediatrix 4102.
Management Server (optional)	Module or software used to remotely manage and configure the Mediatrix 4102. Such software could be the Media5 Unit Manager Network. See "Unit Manager Network – Element Management System" on page xvii for more details.
TFTP Server or HTTP Server	Necessary for software updates.
Syslog Daemon (optional)	Receives all status messages coming from the Mediatrix 4102.

Safety Recommendations

To ensure general safety, follow these guidelines:

- ▶ Do not open or disassemble the Mediatrix 4102.
- ▶ Do not get the Mediatrix 4102 wet or pour liquids into it.
- ▶ Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Package Contents

The Mediatrix 4102 package contains the following items:

- ▶ the Mediatrix 4102 unit
- ▶ a power cord for the country in which you are using the Mediatrix 4102
- ▶ a universal power supply
- ▶ a printed Flyer

You also need additional 10/100 BaseT Ethernet RJ-45 cables.

Overview

The Mediatrix 4102 is a standalone Internet telephony access device that connects to virtually any business telephone system supporting standard analog lines.

The Mediatrix 4102 offers two Ethernet connectors switches enabling to establish two connections between conventional analog telephones or Group 3 fax machines and either a WAN, a LAN or a personal computer.

The Mediatrix 4102 can be used to connect up to two analog phones or fax machines to a broadband access equipment for a Service Provider's IP Telephony offering to residential users.

This version of the Mediatrix 4102 can use either one of the following signalling protocols:

- ▶ the Media Gateway Control Protocol (MGCP), which is a protocol for controlling Voice over IP (VoIP) Gateways from intelligent external call control elements.
- ▶ the Network-based Call Signalling (NCS) protocol, which is a profile of the MGCP protocol.

You can switch from one signalling protocol to the other as described in ["Switching Protocols" on page 53](#).

About the Mediatrix 4102

The Mediatrix 4102:

- ▶ Merges voice and data traffic onto a single unified network. Carrying telephone traffic over data networks uses less bandwidth (as compared to telephone trunks), resulting in a more cost-effective network solution.
- ▶ Easily integrates with existing telephone equipment. It converts any conventional analog telephone or fax machine into an Internet device.
- ▶ Bypasses long-distance toll charges for realized savings.
- ▶ Supports 10 Mb/s and 100 Mb/s Ethernet networks.
- ▶ Upgrades software easily for future enhancements.
- ▶ Uses the latest standards in Internet Telephony.
 - MGCP or NCS protocol for call management
 - T.38 for fax relay
- ▶ Supports the following Codecs:
 - G.711 (μ -law, A-law)
 - G.726
 - G.729 A
 - G.729 A rev. B
 - T.38 (fax) over UDP only
- ▶ Supports Quality of Service technologies.
 - Differentiated Services (DS) Field
 - IEEE 802.1p user priority tagging
- ▶ Offers an intuitive Web-based management interface to simplify operation and support.

Placing a Call

You can place a call from a telephone or fax connected to a Mediatrix 4102. The unit automatically detects if the call originates from a voice or fax transmission and acts accordingly.

When placing a call, the Mediatrix 4102 collects the DTMF digits dialed and sends a message to the Call Agent. The Call Agent sends back a list of contacts where the dialed number could be located.

You can dial on a telephone/fax machine connected to the Mediatrix 4102 as you normally do.

Management Choices

The Mediatrix 4102 offers various management options to configure the unit.

Table 4: Management Options

Management Choice	Description
Web Interface	The Mediatrix 4102 web interface offers the following options: • Password-protected access via basic HTTP authentication, as described in RFC 2617 • User-friendly GUI Refer to “Chapter 2 - Web Interface – Introduction” on page 25 for more details.
SNMPv1/2/3	The Mediatrix 4102 SNMP feature offers the following options: • Password-protected access • Remote management • Simultaneous management Refer to “Chapter 4 - MIB Structure and SNMP” on page 39 for more details.
Auto-Update	The Mediatrix 4102 auto-update options are as follows: • Frequent polling • Automatic software and configuration files downloads • Configuration file encryption Refer to “Chapter 11 - Software Download” on page 149 and “Chapter 10 - Configuration File Download” on page 131 for more details.

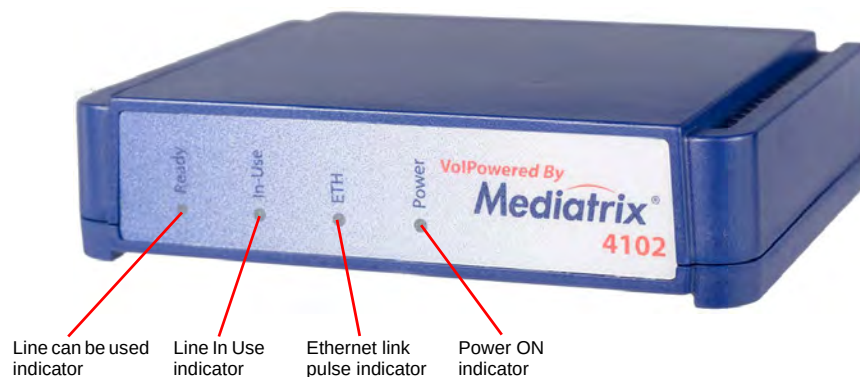
Panels

This section provides an overview of the front and rear panels of the Mediatrix 4102.

Front Indicators

[Figure 1](#) shows the visual indicators located on the front of the Mediatrix 4102.

Figure 1: Front Panel Indicators



[Table 5](#) describes the LEDs on the front panel of the Mediatrix 4102.

Table 5: Front Panel Indicators

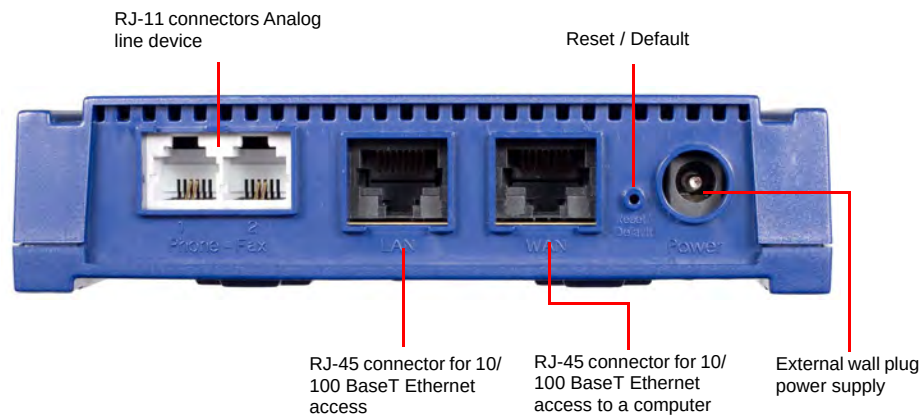
Indicator	Description
Ready	When lit, at least one of the FXS lines configured to be registered with a Call Agent is properly and successfully registered.
In Use	When lit, at least one of the FXS lines is in use.
ETH	Provides the state of the network connected to the WAN and LAN connectors.
Power	When lit, power is applied to the Mediatrix 4102.

See [“LED Indicators” on page 16](#) for a detailed description of the LED patterns the Mediatrix 4102 may have and the states they represent.

Rear Connectors

The Mediatrix 4102 has several connections that must be properly set. [Figure 2](#) shows the back panel of the Mediatrix 4102.

Figure 2: Back Panel Connectors



[Table 6](#) describes the back panel connections.

Table 6: Back Connections of the Mediatrix 4102

Connection	Description
WAN1	A 10/100 BaseT Ethernet RJ-45 connector for access to a LAN, WAN or computer.
LAN	A 10/100 BaseT Ethernet RJ-45 connector that can be connected into the network card of a computer.
Phone-Fax 1 / Phone-Fax 2	Two RJ-11 connectors to attach a conventional telephone or G3 fax machine.
Power connector	External 12 Vdc power supply.
Reset / Default switch	Resets configuration parameters of the Mediatrix 4102 to default (known) values. It can be used to reconfigure the unit. Warning: Read Section “Reset / Default Switch” on page 20 before attempting to reset the unit.

Choosing a Suitable Installation Site



Warning: The analog lines of the Mediatrix 4102 are not intended for connection to a telecommunication network that uses outside cable.



Warning: To prevent fire or shock hazard do not expose the unit to rain or moisture.

The Mediatrix 4102 is suited for use in an office or residential environment where it can be wall-mounted or free standing.

Location

Install the Mediatrix 4102 in a well-ventilated location where it will not be exposed to high temperature or humidity. Do not install the Mediatrix 4102 in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components.

When deciding where to position the Mediatrix 4102, ensure that:

- ▶ The Mediatrix 4102 is accessible and cables can be easily connected.
- ▶ The cabling is away from the following:
 - Sources of electrical noise such as radios, transmitters, and broadband amplifiers.
 - Power lines and fluorescent lighting fixtures.
 - Water or moisture that could enter the casing of the Mediatrix 4102.
- ▶ The airflow is not restricted around the Mediatrix 4102 or through the vents on the top of the unit. The unit requires a minimum of 25 mm (1 in.) clearance.
- ▶ The operating temperature is between 0°C and 40°C.
- ▶ The humidity is not over 85% and is non-condensing.

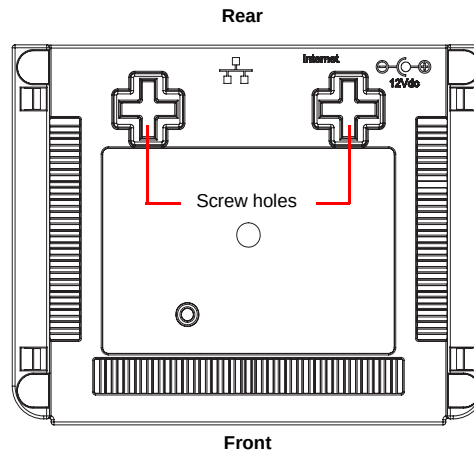
Wall-Mounting

The Mediatrix 4102 has two screw holes on its bottom surface, allowing a single unit to be wall-mounted.

► **To wall-mount the Mediatrix 4102:**

1. Disconnect all of the cables from the Mediatrix 4102 before mounting.
2. Ensure that the wall you are using is smooth, flat, dry and sturdy. Attach a piece of plywood, approximately 250 mm x 200 mm x 12 mm (10 inches x 8 inches x 0.5 inches) securely to the wall, if necessary.
3. Position the Mediatrix 4102 against the wall (or plywood) as illustrated in [Figure 3](#).

Figure 3: Bottom View - Wall Mounting Screw Holes



You can position the Mediatrix 4102 any way you want.

4. Mark the position of the screw holes on the wall. Drill the two holes and install two screws.
5. Place the screw holes of the Mediatrix 4102 over the screws installed in the previous step.
6. Proceed to [“Hardware Connection” on page 9](#).

Free Standing Unit

When installing the Mediatrix 4102 on a desk or table, it should be located at least 20 cm from your monitor, computer casing or other peripherals, including speakers. Never put books or paper on the Mediatrix 4102.

Condensation

When bringing the unit into a warm environment from the cold, condensation may result that might be harmful to the unit. If this occurs, allow the unit to acclimatize for an hour before powering it on.

Cleaning

To clean the Mediatrix 4102, wipe with a soft dry cloth. Do not use volatile liquids such as benzene and thinner that are harmful to the unit casing.

For resistant markings, wet a cloth with a mild detergent, wring well and then wipe off. Use a dry cloth to dry the surface.

Hardware Connection



Warning: Do not connect the Mediatrix 4102 directly to Telecommunication Systems.

The Mediatrix 4102 may be installed in various ways. This section describes two of these installations: in a single computer configuration without a router and multi-computer configuration with a router.

See ["Appendix C - Cabling Considerations" on page 235](#) for more details on the cables the Mediatrix 4102 uses.

Reserving an IP Address



Note: Perform this step only for a cable modem installation.

Before connecting the Mediatrix 4102 to the network, Media5 strongly recommends that you reserve an IP address in your DHCP 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.

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 4102 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 located in the `sysMgmtMIB` under the `sysMacAddress` variable.

Before Proceeding

Most computers are configured by default to automatically obtain an IP address via DHCP. If the computer connected to the Mediatrix 4102 is set with a static IP address, you must change the setting. Please refer to your operating system's documentation to perform this task.

10/100 BaseT Ethernet RJ-45 Cable

When connecting an Ethernet cable to the Mediatrix 4102, use a standard telecommunication cord with a minimum of 26 AWG wire size.

You can either use a crossover or straight Ethernet cable to connect in the *WAN* or *LAN* connectors. These connectors perform automatic MDI / MDIX detection, meaning that they adapt to the type of cable connected to them.

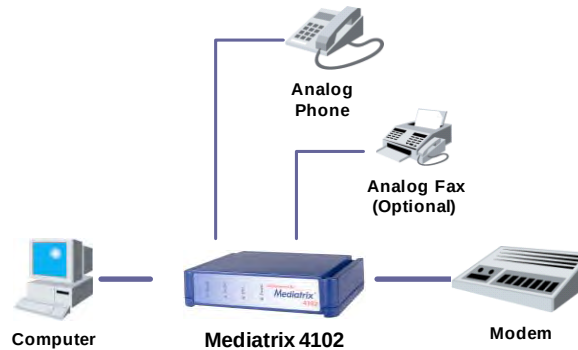
The auto MDI / MDIX feature works only when the connectors are configured in auto detect mode (see ["Ethernet Connection Speed" on page 73](#) for more details).

Whenever you force the Mediatrix 4102 to use a specific Ethernet mode (for example 100Mb Full Duplex), the type of cable to use depends on the other peer. For example, a straight cable is required to connect the Mediatrix 4102 to a hub or a switch, while a crossover cable is required to connect the Mediatrix 4102 to a PC. See ["Appendix C - Cabling Considerations" on page 235](#) for more details.

Single Computer Installation

The following steps describe how to install the Mediatrix 4102 with a single computer. The installation may either be performed with a cable or DSL modem. The resulting layout could be something similar to [Figure 4](#).

Figure 4: Single Computer Network Configuration



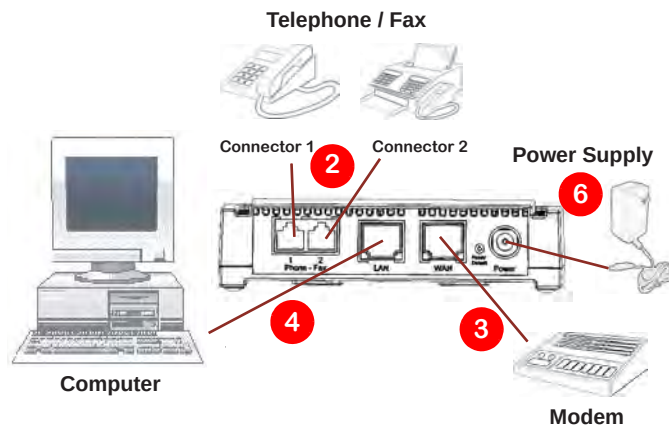
If your Internet connection requires PPPoE authentication, enter a PPPoE user name and password in the Mediatrix 4102 as described in [“System Page” on page 29](#).



Note: Do not set the PC to use PPPoE because the Mediatrix 4102 will take care of the authentication.

The following figure illustrates the hardware connections.

Figure 5: Single Computer Installation



► To install the Mediatrix 4102 with a single computer:

1. Before you begin, be sure that all of your hardware is powered off, including the PC, modem, and Mediatrix 4102.
2. Connect analog telephones or fax machines into the *Phone/Fax* connectors.
3. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *WAN* connector of the Mediatrix 4102. Connect the other end to the cable or DSL modem.
See [“10/100 BaseT Ethernet RJ-45 Cable” on page 9](#) for more details on this cable.
4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *LAN* connector of the Mediatrix 4102. Connect the other end to the network card of your computer.
See [“10/100 BaseT Ethernet RJ-45 Cable” on page 9](#) for more details on this cable.

5. Power on the cable or DSL modem. Depending on your modem, you may have to wait a few minutes before it properly establishes the Internet connection. Refer to your modem's documentation for more details.
6. Once the modem is ready, connect the power cord to the Mediatrix 4102 and then connect the other end to an electrical outlet.



Warning: The electrical outlet must be installed near the Mediatrix 4102 so that it is easily accessible.

This turns the Mediatrix 4102 on. You should not unplug it when not in use.

- If the *Power* LED is steady on, proceed with the next step.
- If the *Power* LED is blinking, wait until the *In Use* LED blinks before proceeding with the next step. This may take up to three minutes.

Most DSL users will need to enable PPPoE after they have installed the Mediatrix 4102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to ["Chapter 2 - Web Interface – Introduction" on page 25](#).

7. Power on the PC.

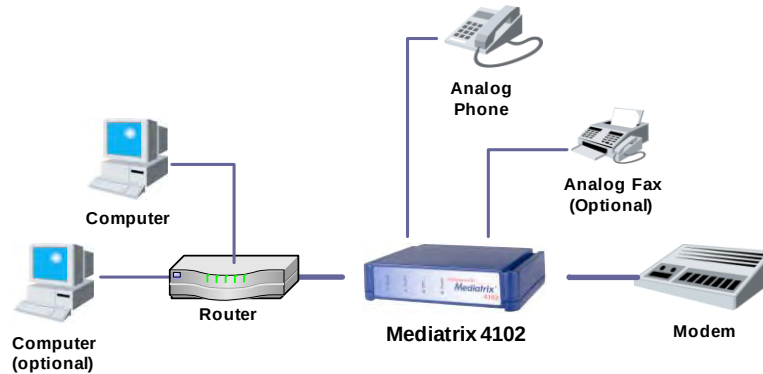
Your computer does not have to be turned on for the telephone or fax services.

Media5 suggests to access the unit's web interface to configure its basic uplinks parameters. See ["Chapter 2 - Web Interface – Introduction" on page 25](#) for more details.

Multiple Computer Installation

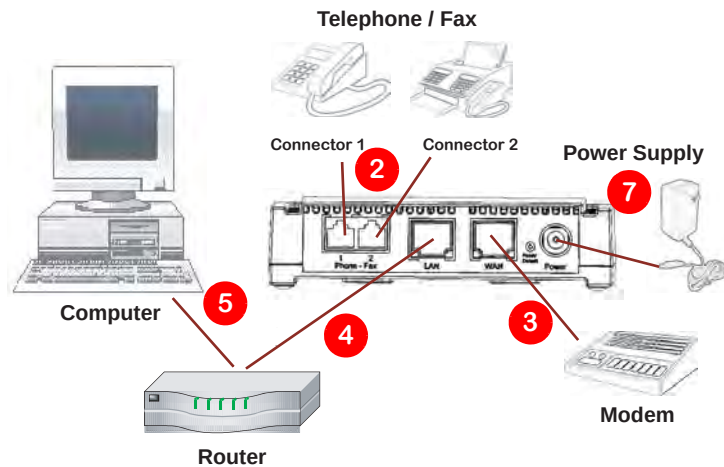
You can use a router with the Mediatrix 4102 to provide Internet connectivity to more than one PC or other device. The following steps describe how to install the Mediatrix 4102 with a router. The installation may either be performed with a cable or DSL modem. The resulting layout could be something similar to [Figure 6](#).

Figure 6: Router Network Configuration



The following figure illustrates the hardware connections.

Figure 7: Router Installation



If your Internet connection requires PPPoE authentication, enter a PPPoE user name and password in the Mediatrix 4102 as described in ["System Page" on page 29](#).



Note: Most home routers are configured by default to automatically obtain an IP address via DHCP. If the router connected to the Mediatrix 4102 is set with a static IP address, you must change the setting. Please refer to your router's documentation to perform this task.

► To install the Mediatrix 4102 with a router:

1. Before you begin, be sure that all of your hardware is powered off, including the PC, router, modem, and Mediatrix 4102.
2. Connect analog telephones or fax machines into the *Phone/Fax* connectors.
3. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *WAN* connector of the Mediatrix 4102. Connect the other end to the cable or DSL modem.
See ["10/100 BaseT Ethernet RJ-45 Cable" on page 9](#) for more details on this cable.
4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *LAN* connector of the Mediatrix 4102. Connect the other end to the *WAN / Uplink* connector of the router.

See [“10/100 BaseT Ethernet RJ-45 Cable” on page 9](#) for more details on this cable.

5. Connect a 10/100 BaseT Ethernet RJ-45 cable into the LAN connector of the router. Connect the other end to the network card of your PC.

See [“10/100 BaseT Ethernet RJ-45 Cable” on page 9](#) for more details on this cable.

6. Power on the cable or DSL modem. Depending on your modem, you may have to wait a few minutes before it properly establishes the Internet connection. Refer to your modem's documentation for more details.
7. Once the modem is ready, connect the power cord to the Mediatrix 4102 and then connect the other end to an electrical outlet.



Warning: The electrical outlet must be installed near the Mediatrix 4102 so that it is easily accessible.

This turns the Mediatrix 4102 on. You should not unplug it when not in use.

- If the *Power* LED is steady on, proceed with the next step.
- If the *Power* LED is blinking, wait until the *In Use* LED blinks before proceeding with the next step. This may take up to three minutes.

8. Power on the router. Depending on your router, you may have to wait a few minutes before it is ready. Refer to your router's documentation for more details.

Most DSL users will need to enable PPPoE after they have installed the Mediatrix 4102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to [“Chapter 2 - Web Interface – Introduction” on page 25](#).

9. Power on the PC.

Your computer does not have to be turned on for the telephone or fax services.

Media5 suggests to access the unit's web interface to configure its basic uplinks parameters. See [“Chapter 2 - Web Interface – Introduction” on page 25](#) for more details.

Starting the Mediatrix 4102 for the First Time

This step depends on the WAN connection type set in the web interface (see [“Chapter 2 - Web Interface – Introduction” on page 25](#)).

Most DSL users will need to enable PPPoE after they have installed the Mediatrix 4102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to [“Chapter 2 - Web Interface – Introduction” on page 25](#).

If you are using a cable modem, the default MIB parameters are set so that the unit can be directly plugged into a network and provisioned with a DHCP server. Media5 strongly recommends to set your DHCP server before installing the unit on the network. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

If you are experiencing problems, or if you do not want to use a DHCP server, perform a Recovery Mode procedure, as explained in [“Recovery Mode” on page 21](#).

IP Address Discovery or Configuration

Once the physical connection is complete and the Mediatrix 4102 is powered up, the first thing to do is find out the IP address the Mediatrix 4102 is using. The Mediatrix 4102's IP address can be set either dynamically or statically. The default behaviour of the Mediatrix 4102 is to try to obtain a dynamic IP address through a DHCP server.



Caution: If you set a Mediatrix 4102 with a static *eth1-4* IP address in a subnet (for instance, 192.168.200.1) and the *eth5* interface receives a dynamic IP address in the same subnet (via a DHCP server or PPP peer), you will not be able to contact the unit via the WAN. You must be careful that a dynamic IP address does not overlap a static IP subnet that is already configured. Note that the current default value of the Mediatrix 4102 is 192.168.0.10.

Dynamic IP Address Discovery

Before connecting the Mediatrix 4102 to the network, Media5 strongly suggests that you reserve an IP address in your DHCP server for the unit you are about to connect (["Reserving an IP Address" on page 9](#)).

If you have not reserved an IP address, you can discover which IP address has been assigned to the Mediatrix 4102 by either:

- ▶ consulting your DHCP server's logs to find out details on the DHCP lease that was given to the Mediatrix 4102.
- ▶ using a network packet sniffer (e.g., Wireshark) to examine the DHCP messages exchanged between the Mediatrix 4102 and your DHCP server while the Mediatrix 4102 boots up.

▶ To start the Mediatrix 4102 with a dynamic IP address:

1. If you need to discover the IP address of the Mediatrix 4102, install and start your network packet sniffer.
2. Power on the Mediatrix 4102 by connecting the other end of the power cord to an electrical outlet. The electrical outlet must be installed near the Mediatrix 4102 so that it is easily accessible.



Note: If the *Power* LED is always blinking and never turns on, this means that the Mediatrix 4102 cannot find a DHCP server. Check that you have a DHCP server properly configured on your network. If you do not have a DHCP server, go to the section ["Default Static IP Address Configuration" on page 14](#).

Default Static IP Address Configuration

If there is no DHCP server in your network, then the IP address has to be configured statically.

▶ To start the Mediatrix 4102 with a static IP address:

1. With a 10/100 Hub and two 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the Hub; one of them is connected into the *WAN* connector of the Mediatrix 4102 and the other one links the computer to the Hub.
2. Reconfigure the IP address of your computer to 192.168.0.10 and the Subnet Mask to 255.255.255.0. Restart the computer.
3. Power on the Mediatrix 4102 by connecting the other end of the power cord to an electrical outlet. The electrical outlet must be installed near the Mediatrix 4102 so that it is easily accessible.
4. Insert a small, unbent paper clip into the *Reset / Default* switch hole located at the of the Mediatrix 4102. The *Power* LED will start blinking, and after a few seconds, all the LEDs will start blinking. Release the paper clip after all the LEDs start blinking and before they all stop blinking (between 5-10 seconds). Only the *Power* and *Ready* LEDs should go on blinking to inform you that the recovery mode procedure has been performed.

After a recovery mode is performed, the Mediatrix 4102 uses the default IP address 192.168.0.1. Refer to ["Recovery Mode" on page 21](#) for details on the recovery mode procedure.

You must perform the recovery mode in a closed network and perform it on only one Mediatrix 4102 at a time, since the default IP address is the same on every unit.

Initial Provisioning Sequence

When starting the Mediatrix 4102 for the first time, it needs to be configured before it can support calls. This process is known as *provisioning*. This sequence assumes that you have installed the Mediatrix 4102 hardware as per [“Hardware Connection” on page 9](#).

The Mediatrix 4102 requests its configuration only on the first restart. You can change the configuration at will after the initial provisioning and the provisioning system can refresh the Mediatrix 4102 configuration. The provisioning system consists of the Management Server and a DHCP server. The Management Server includes a provisioning client, provisioning server, and SNMP proxy server.

Provisioning Sequence in DHCP

The following describes the initial provisioning sequence of a Mediatrix 4102 that uses a DHCP connection type.

► **Initial provisioning sequence:**

1. When the Mediatrix 4102 starts, it broadcasts a message requesting DHCP services (if the unit is configured to start in DHCP mode).
2. The DHCP server responds with a set of IP addresses and network parameters, one of which is the Mediatrix 4102 IP address.

The following are some of the network parameters assigned via DHCP:

- Mediatrix 4102 IP address
 - Subnet Mask
 - Default Router IP address
 - Primary and Secondary DNS IP addresses
 - Management Server IP address and port number (optional)
 - Configuration file server IP address and port number (optional)
 - Call Agent IP address and port number
3. The Mediatrix 4102 may request its configuration in two ways:
 - by using the IP address of the Management Server to request its configuration.
 - by using a configuration file.

Provisioning Sequence in PPPoE

If the WAN connection type is set to PPPoE (see [“Chapter 2 - Web Interface – Introduction” on page 25](#)), the Mediatrix 4102 establishes a PPP session with an access concentrator. This access concentrator sends the following information to the unit:

- WAN IP address
- Default Router IP address (0.0.0.0).

The access concentrator may also supply primary and secondary DNS servers. If this is the case, the new DNS servers supersede the servers defined locally.

Refer to [“Chapter 9 - Transparent Address Sharing” on page 113](#) for more details.

This implies that you may have to enter static values for additional network parameters.

► **To set static information:**

1. In the *ipAddressConfig* folder, locate the *localHostSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group).
2. Set this variable to **static**.

3. Set a static value for the following network parameters:

Table 7: Network Parameters Static Variables

Variable	Default Static Value
localHostStaticPrimaryDns ^a	"192.168.0.10"
localHostStaticSecondaryDns ^a	"192.168.0.10"
localHostStaticSubnetMask	"255.255.255.0"

a. If you do not want to use a DNS, set the variable to 0.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *IP Configuration*.



Caution: These variables are vital to the proper operation of the Mediatrix 4102. If a variable of this group is not set properly, the unit may not be able to start or be contacted after it has started.



Note: Media5 recommends not to set the *localHostStaticSubnetMask* variable to 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.

4. Set other static information as required.
See ["Services" on page 56](#) for more details.
The next step would be to configure the IP routing information of the Mediatrix 4102 as described in ["Chapter 9 - Transparent Address Sharing" on page 113](#).

LED Behaviour in Starting Mode

When the Mediatrix 4102 starts and it is not configured to use a DHCP server, it uses static IP addresses. If the static information is not valid, the *LAN* LED blinks at 1 Hz with 75% duty cycle. This lets you know that you must perform a Factory reset or Recovery mode operation. See ["Reset / Default Switch" on page 20](#) for more details.

LED Indicators

A LED can be ON, OFF, BLINKING or controlled by hardware (HW). The blinking behaviour is described in terms of rate (in Hertz – Hz) and duty cycle (in percentage). For instance, a LED that turns on every two seconds and stays on for one second would be described as: blink 0.5 Hz 50%. The hardware (HW) behaviour is not defined. It is usually the standard state for the *ETH* LED.

Ready LED

The *Ready* LED provides an "at-a-glance" view of the Mediatrix 4102 operational status. It is an aid for installation and on-site support. This LED is:

- ▶ ON when all elements of the *ifAdminOpState* column are "enabled".
- ▶ OFF when all elements of the *ifAdminOpState* column are "disabled".
- ▶ Blinking when at least one element of the *ifAdminOp State* column is "enabled" and at least one element is "disabled".

Patterns and meanings of the *Ready* LED are described in [Table 10 on page 19](#).

Refer to the *MIB Reference Manual* for more details on the *ifAdminOpState* variable.

In Use LED

The *In Use* LED provides feedback of the activity on the line. If a line is ringing, off-hook, or displaying information (ADSI), then this LED is ON. The *In Use* LED is ON when at least one element in the *ifAdminUsageState* column is “busy”. Patterns and meanings of the *In Use* LED are described in [Table 10 on page 19](#).

Refer to the *MIB Reference Manual* for more details on the *ifAdminState* variable.

ETH LED

The *ETH* LED provides the Link and Heartbeat status of the network connected to the Ethernet connector. If there is no link under HW control, the LED is OFF. When a link is established, but no activity is detected, the LED is ON; it turns off for very short periods of time when activity is detected and blinks rapidly when the Ethernet is loaded. Patterns and meanings of the *ETH* LED are described in [Table 10 on page 19](#).

Power LED

The *Power* LED indicates whether or not the Mediatix 4102 is operational at its most basic level. It does not imply that the unit can be used, only that it is capable of being used. Healthy operation would be steady ON. Patterns and meanings of the *Power* LED are shown in [Table 10 on page 19](#).

LED Patterns

[Table 8](#) describes the different states a Mediatix unit can have and their associated LED patterns.

Table 8: States and LED Patterns

State	Description	LEDs Pattern			
		Ready	In Use	ETH	Power
Booting	Follows a hardware start or a reset.	See “Booting LED Pattern Description” on page 18			
Normal Mode	“Normal” state of the unit where calls can be initiated. Each LED has a separate behaviour.	See “NormalMode LED Pattern Description” on page 19			
AdminMode	Calls are not permitted and maintenance actions can be performed.	See “AdminMode LED Pattern Description” on page 19			
Recovery Mode	The IP addresses for local host, image server, syslog server, etc., are temporarily set to known values. Calls are not allowed.	Blink 1 Hz 75%	Off	Misc. ^a	Blink 1 Hz 75%
Reset Pending	Triggered when the <i>Reset / Default</i> switch is pressed and held for at least 2 seconds.	Off	Off	Off	Blink 1 Hz 50%
Reboot Pending	Triggered when the <i>Reset / Default</i> switch is pressed in either the <i>ResetPending</i> or <i>RecoveryMode Pending</i> states. The unit prepares for a physical shutdown and restart.	Off	Off	Off	Off
Recovery Mode Pending	Triggered when the <i>Reset / Default</i> switch is held at start-time or for at least 7 seconds.	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%

Table 8: States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	In Use	ETH	Power
Default Settings Pending	Triggered when the <i>Reset / Default</i> switch is not released while in <i>RecoveryModePending</i> state. At run time, if the <i>Reset / Default</i> switch is released within 5 seconds, the unit applies default settings, otherwise the action is cancelled and the unit goes back to the Operation Modes state or it resets. At start time, the unit stays in this state until the <i>Reset / Default</i> switch is released. The unit then applies the default settings and restarts.	On	On	On	On
Image DownloadIn Progress	A software image is downloaded into the unit and written to persistent storage.	LEDs are blinking at 1 Hz 75%, <i>one at a time</i> , from left to right.			
Image Download Error	Triggered after a failure of an image download operation. After 4 seconds, the unit restarts.	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%
InitFailed	Triggered when bad initialization parameters are detected and the unit cannot start correctly. Note: If the network configuration is dynamic, the unit stays in the <i>Booting</i> state and continues to query the DHCP until it receives valid values. If the configuration is static, the LED pattern indicates that the unit must be reset to default settings or put into recovery mode for maintenance and correction of network values.	Off	Off	Blink 4 Hz 50%	Off
DiagFailed	Triggered at start-time when the hardware or software diagnostic fails. This is a critical error and the unit may require RMA.	Off	Off	Off	Blink 4 Hz 50%
NetworkRescue	The unit tries to download and install a firmware given by the Network Rescue server.	Off	LEDs are blinking to show a LED displacing light from left to right and right to left.		

a. See the corresponding LED pattern in ["NormalMode LED Pattern Description" on page 19](#).

Booting LED Pattern Description

While in the *Booting* state, the LEDs of the Mediatrix 4102 behave independently; the following table indicates the behaviour for each LED.

Table 9: LED Patterns in Booting Mode

LED	Pattern	Meaning
Ready	Steady Off	Not Ready.
In Use	Steady Off	Cannot be in use.
ETH (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected or hardware control not activated.
	Blinking (variable rate)	Ethernet activity detected.

Table 9: LED Patterns in Booting Mode (Continued)

LED	Pattern	Meaning
Power	Steady On	Power is On.
	Blinking 1 Hz 75%	Waiting for a DHCP answer.

NormalMode LED Pattern Description

While in the *NormalMode* state, the LEDs of the Mediatrix 4102 behave independently; the following table indicates the behaviour for each LED.

Table 10: LED Patterns in Operation Mode

LED	Pattern	Meaning
Ready	Steady On	All lines are enabled (operational state).
	Steady Off	All lines are disabled (operational state).
	Blink 0.25 Hz 75%	At least one line is enabled and at least one line is disabled (operational state).
In Use	Steady On	At least one line is busy (usage state).
	Steady Off	All lines are not busy (usage state) or the unit is not connected to the network.
ETH (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected.
	Blinking (variable rate)	Ethernet activity detected.
Power	Steady On	Power is On.
	Steady Off	Power is Off.
	Blinking 1 Hz 75%	Waiting for a DHCP answer.

AdminMode LED Pattern Description

While in the *AdminMode* state, the LEDs of the Mediatrix 4102 behave independently; the following table indicates the behaviour for each LED.

Table 11: LED Patterns in AdminMode

LED	Pattern	Meaning
Ready	Blinking 1 Hz 75%	<i>Ready</i> and <i>Power</i> LEDs blink off phase at 180 degrees.
In Use	Steady Off	All analog lines are not available.
ETH (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected.
	Blinking (variable rate)	Ethernet activity detected.
Power	Blinking 1 Hz 75%	<i>Ready</i> and <i>Power</i> LEDs blink off phase at 180 degrees.

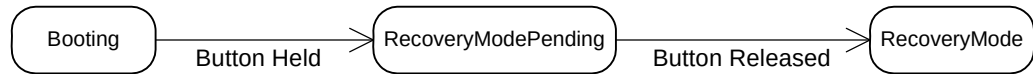
Recovery Mode LED Patterns

There are two different sequences of LED patterns indicating that a recovery is in process.

At Start-Time

When pressing the *Reset / Default* switch at start-time, the state sequence goes as follows:

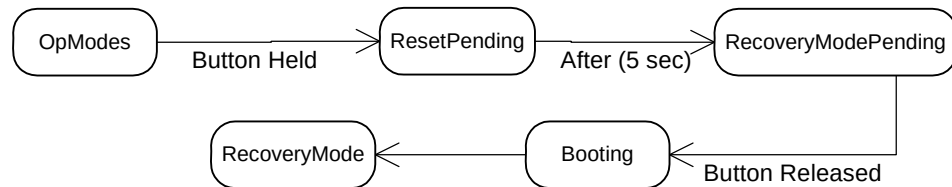
Figure 8: LED Pattern at Start-Time



At Run-Time

When pressing the *Reset / Default* switch at run-time, the state sequence goes as follows:

Figure 9: LED Patterns at Run-Time



Reset / Default Switch

The *Reset / Default* switch allows you to:

- ▶ Cancel an action that was started.
- ▶ Revert to known factory settings if the Mediatrix 4102 refuses to work properly for any reason or the connection to the network is lost.
- ▶ Reconfigure a unit.

At Run-Time

The *Reset / Default* switch can be used at run-time – you can press the switch while the Mediatrix 4102 is running without powering the unit off. [Table 12](#) describes the actions you can perform in this case.

Table 12: Reset / Default Switch Interaction

Reset / Default Switch Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	ETH	Power
2 to 5 seconds	Restarts the Mediatrix 4102	No changes are made to the Mediatrix 4102 settings.	Off	Off	Off	Blink
5 to 10 seconds	Restarts the Mediatrix 4102 in Recovery Mode	Sets the Mediatrix 4102 IP address to its default value in the MIB and restarts the unit.	Blink	Blink	Blink	Blink ^a

Table 12: Reset / Default Switch Interaction (Continued)

Reset / Default Switch Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	ETH	Power
10 to 15 seconds ^b	Restarts the Mediatrix 4102 in Factory Reset	Deletes the persistent MIB values, creates a new configuration file with the default factory values, and then restarts the unit.	On	On	On	On

a. Synchronized blinking at 2 Hz (50% duty cycle).

b. You can disable the Factory reset procedure to avoid users deleting the existing configuration. See [“Disabling the Factory Reset” on page 23](#) for more details.

At Start-Time

The *Reset / Default* switch can be used at start-time – you power the unit off, and then depress the *Reset / Default* switch and power the unit back on. In this case, the following explains the reset behaviour:

- ▶ Pressing the *Reset / Default* switch at startup until all the LEDs start blinking restarts the Mediatrix 4102 in “Recovery Mode”.
- ▶ Pressing the *Reset / Default* switch at startup until all the LEDs stop blinking and remain ON applies the “Factory Reset” procedure. This feature reverts the Mediatrix 4102 back to its default factory settings.

See [“LED Indicators” on page 16](#) for a detailed description of the LED patterns related to the *Reset / Default* switch.

Recovery Mode

The recovery mode restarts the Mediatrix 4102 in a known, static, and minimal state. It is used to recover from a basic configuration error that prevents you to reach the unit through the network. It may serve as a last resort before the Factory reset command. You must perform it in a closed network and on only one Mediatrix 4102 at a time, because the default IP address is the same on every unit.

The recovery mode is not intended to address configuration and/or software problems. For those types of problems, you must use the Factory reset.



Note: The procedure below assumes that you are performing it at run-time.

▶ To trigger the Recovery Mode:

1. With a 10/100 Hub and two 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the hub; one of them is connected into the *WAN* connector of the Mediatrix 4102 and the other one links the computer to the hub.
Alternatively, you can connect a 10/100 BaseT Ethernet RJ-45 crossover cable into the *WAN* connector of the Mediatrix 4102 and connect the other end to your computer.
2. Reconfigure the IP address of your computer to *192.168.0.10* and enter the Subnet Mask of *255.255.255.0*. Restart the computer.
3. Insert a small, unbent paper clip into the *Reset / Default* switch hole located at the of the Mediatrix 4102.
4. Hold the *Reset / Default* switch between 5 and 10 seconds – until the LEDs start blinking.
5. Release the paper clip.
Only the *Power* and *Ready* LEDs should go on blinking to inform you that the recovery reset has been performed.

In recovery mode, the provisioning source of the *localhostConfigSource* variable is set to **default**, meaning that the default factory setting is used.

The following variables use their default values in the MIBs:

- localhostAddress
- localhostPrimaryDns
- localhostSecondaryDns
- localhostDefaultRouter
- localhostSnmpPort
- localhostSubnetMask
- imagePrimaryHost
- imagePrimaryPort
- imageSecondaryHost
- imageSecondaryPort
- msHost
- msTrapPort
- syslogHost
- syslogPort

The following variables of the *mediatrixMgmt* group are all set to static:

- imageConfigSource
- configFileFetchingConfigSource
- msConfigSource
- syslogConfigSource
- snmpConfigSource

All the persistent MIB values are kept.

In this mode, MGCP/NCS is deactivated. Only SNMP or HTTP can be used to set the IP addresses listed above and the protocol-specific IP addresses (all IP addresses located under the *ipAddressConfig* folder in the MIB structure).

You can also download a software version, but you cannot download a configuration file.

6. When the Mediatrix 4102 has finished its provisioning sequence, perform the changes, and then turn it off, plug it on the network, and turn it on again.

When restarting, the Mediatrix 4102 will not be in Recovery mode and will use the IP addresses configuration set forth in the MIBs.

See [“Changing a Parameter Value” on page 49](#) for more details.



Note: The recovery mode does not alter any persistent configuration data of the Mediatrix 4102.

Factory Reset

The Factory reset reverts the Mediatrix 4102 back to its default factory settings. It deletes the persistent MIB values of the unit, including:

- ▶ The entire *mediatrixMIBs* configuration.
- ▶ The MIB-II setup.
- ▶ The software download configuration files.
- ▶ The SNMP configuration, including the SNMPv3 passwords and users.
- ▶ The PPPoE configuration, including the user names and passwords.

The Factory reset creates a new configuration file with the default factory values. It should be performed with the Mediatrix 4102 connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, it sends requests indefinitely.

You can disable the Factory reset to avoid users deleting the existing configuration. See [“Disabling the Factory Reset” on page 23](#) for more details.

► **To trigger the Factory Reset:**

1. Power the Mediatrix 4102 off.
2. Insert a small, unbent paper clip into the *Reset / Default* switch hole located at the rear of the Mediatrix 4102. While depressing the *Reset / Default* switch, plug the power cord back in to power up the unit.
Do not depress before all the LEDs stop blinking and are steadily ON.
3. Release the paper clip.
The Mediatrix 4102 restarts.
This procedure resets all variables in the MIB modules to their default value; defaults include the *localhostSelectConfigSource* variable set to **dhcp**.
When the Mediatrix 4102 has finished its provisioning sequence, it is ready to be used with a DHCP-provided IP address and MIB parameters.



Note: The Factory reset alters any persistent configuration data of the Mediatrix 4102.

Disabling the Factory Reset

You can disable the factory reset procedure, even if users depress the *Reset / Default* switch. Disabling the factory reset means that users will not be able to revert the Mediatrix 4102 back to its factory settings if there are configuration problems.

► **To change the factory reset behaviour:**

1. In the *sysAdminMIB*, set the *sysAdminDefaultSettingsEnable* variable to **disable**.
In this case, users can only perform a Recovery Mode procedure. See [“Reset / Default Switch” on page 20](#) for more details.

Software Restart

You can initiate a software restart of the Mediatrix 4102 by using MIB parameters.



In the *Unit Manager Network Administration Manual*, refer to chapter *Performing Actions on Mediatrix Units*, section *Restarting a Unit*.

► **To perform a software restart:**

1. In the *groupAdminMIB*, locate the *groupAdminMIBObjects* group.
2. Set the *groupSetAdmin* variable to the appropriate type of restart:
 - *Locked*: waits for the state of all lines to be locked, and then restarts. This is called a graceful restart.
 - *ForceLock*: restarts immediately. This is called an abrupt restart.
 - *Unlock*: the command is discarded.
3. Set the *groupReset* variable to **SoftReset**.
The Mediatrix 4102 restarts.

Restart Behaviour

This feature affects the behaviour of the Mediatrix 4102 when it restarts.

You can instruct the Mediatrix 4102 to check its TCP/IP stack before declaring the restart successful.

This could be useful when the unit is subjected to a broadcast storm (such as a TCP/IP flood) while it is restarting. In this case, and when the TCP/IP stack check is enabled, the unit enters into the rescue mode and cannot be contacted through SNMP. You thus need to restart the Mediatrix 4102 manually. However, when the TCP/IP stack check is disabled, a broadcast storm during a restart will cause the unit to continuously restart until the storm subsides.

► **To define the restart behaviour:**

1. In the *bootBehaviorMIB*, enable the *checkTcpIpStackForSuccessfulBoot* variable.
When the variable is enabled, the TCP/IP stack must initialize properly to consider the restart a success. In a flood scenario, the unit may end up in the rescue mode.
When the feature is disabled, even if the TCP/IP stack fails to initialize during a TCP/IP flood, the restart is considered successful and the unit does not enter into the rescue mode.

Verifying the Installation

There are two ways to verify that the Mediatrix 4102 is properly connected to the IP network and is working:

- By contacting it with a SNMP Browser
- By pinging it

These two procedures assume that you know the IP address of the Mediatrix 4102 you want to verify. If the Mediatrix 4102 does not respond, do the following:

- Verify that the LAN cable is securely connected to the Mediatrix 4102 and to the network connector.
- Be sure that you did not connect a crossover network cable.
- Verify the state of the IP network to ensure it is not down (the LED should be ON or blinking).
- Verify that the call agent is operational.

Web Interface – Introduction

The Mediatrix 4102 contains an embedded web server to set parameters by using the HTTP protocol. This web server may either be accessed via the LAN or WAN interface of the Mediatrix 4102, depending on the current access limitation. This access limitation may be modified in ["Web Interface Access Limitation" on page 25](#).

Standards Supported

RFC 2616 – Hypertext Transfer protocol - HTTP/1.1.

Introduction

The web interface may be used to:

- ▶ View the status of the Mediatrix 4102.
- ▶ Set the basic uplink parameters of the Mediatrix 4102.
- ▶ Peruse syslog messages the Mediatrix 4102 sends.
- ▶ Upload a configuration file to the Mediatrix 4102.
- ▶ Modify the password required to access the web interface.
- ▶ Set numerous parameters of the Mediatrix 4102.

All parameters located in the web interface may also be configured via SNMP. Each section of the web interface suggests a link to the corresponding SNMP section.

Before using the web-based configuration service, you must ensure that it is enabled.

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

1. In the *ipAddressConfig* folder, set the TCP port on which to listen for HTTP requests in the *httpServerPort* variable (under the *ipAddressConfigHttpEngine* group).
2. In the *httpServerMIB*, enable the service by setting the *httpServerEnable* variable to **enable**.

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.

Web Interface Access Limitation

Access to the web interface can be limited to only one of the Mediatrix 4102's interface or all its interfaces. This can be modified only by using the proper MIB variable.

► **To limit the access to the web interface:**

1. In the *httpServerMIB*, configure the interface where the web pages can be accessed in the *httpServerAccess* variable.

You have the following choices:

Table 13: Web Access Limitation Parameters

Access	Description
lanOnly	You can access the web interface from the LAN side, which is usually associated with the <i>LAN</i> connector.
wanOnly	You can access the web interface from the WAN side, which is usually associated with the <i>WAN</i> connector.
all	You can access the web interface from both the LAN and WAN sides.



Note: This variable is changed to **all** if Transparent Address Sharing is disabled. See [“Configuring TAS” on page 119](#) for more details.

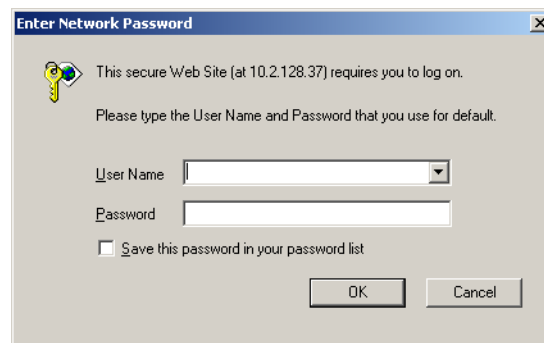
2. Restart the Mediatix 4102 so that the changes may take effect.

► **To use the web interface configuration:**

1. In your web browser’s address field, type the IP address of the Mediatix 4102 (if you have performed a recovery mode, this is **192.168.0.1**).

The following opens:

Figure 10: Login Window



2. Enter the proper user name and password.
The user name and password must be valid. They are case sensitive hence they must be entered properly. Default factory values are:

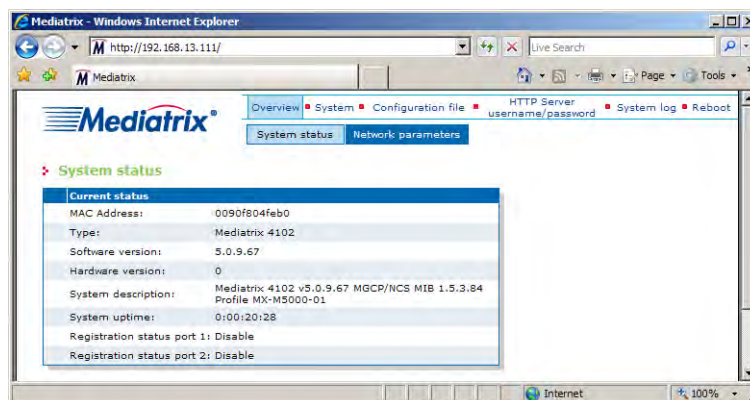
- **User Name:** admin
- **Password:** 1234

Once you have accessed the web interface, you can change the password as described in [“HTTP Server Password Page” on page 34](#).

3. Click *Login*.

The *Overview* web page displays. It has two sub-pages: *System status* and *Network parameters*. It stays accessible for as long as the Internet browser used to access the Mediatix 4102 web interface is opened.

Figure 11: Overview Web Page



System Status of the Mediatrix 4102

The *Overview – System status* page displays the current system status of the Mediatrix 4102.

Table 14: System Status Page

IP Information	Description
MAC Address	MAC address of the Mediatrix 4102.
Type	Product name.
Software version	Software version of the Mediatrix 4102.
Hardware version	Version of the analog circuit board of the Mediatrix 4102.
System description	A textual description of the Mediatrix 4102. It usually includes the full name and version identification of its hardware type, software operating-system, and networking software.
System uptime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
Registration status port1 Registration status port2	May have one of the following: Ready if the operational state of the current interface is enabled. Not ready if the component is operationally non-functional because of an internal condition that would not allow it to participate in a normal VoIP call.

Menu Frame

The Menu frame is displayed at the top of the browser window. It contains management links that allow you to display web pages in the Content frame.

Table 15: Menu Frame Links

Link	Description
Overview	System status: Links to the <i>System status</i> sub-page of the <i>Overview</i> web page, which displays, in read-only format, the system parameters of the Mediatrix 4102.
	Network parameters: Links to the <i>Network parameters</i> sub-page of the <i>Overview</i> web page, which displays, in read-only format, the IP addresses used by the Mediatrix 4102.

Table 15: Menu Frame Links (Continued)

Link	Description
System	WAN: Links to the <i>WAN</i> sub-page of the <i>System</i> web page, which allows you to set the uplink information used by the Mediatrix 4102. See “WAN Page” on page 29 for more details.
	LAN: Links to the <i>LAN</i> sub-page of the <i>System</i> web page, which allows you to set the LAN interface of the Mediatrix 4102. See “LAN Page” on page 31 for more details.
	STUN: Links to the <i>STUN</i> sub-page of the <i>System</i> page, which allows you to configure the STUN client of the Mediatrix 4102. See “STUN Page” on page 32 for more details.
Configuration File	Links to the <i>Configuration File upload</i> web page, which allows you to upload a configuration file from a computer to the Mediatrix 4102. See “Configuration File Upload Page” on page 33 for more details.
HTTP Server password	Links to the <i>HTTP server password</i> web page, which allows you to change the password. See “HTTP Server Password Page” on page 34 for more details.
System log	Links to the <i>System log</i> page, which displays, in read-only format, the syslog messages the Mediatrix 4102 sends. See “System Log Page” on page 36 for more details.

Content Frame

The Content frame is displayed in the lower part of the browser window. It contains the various web pages that allow you to manage the Mediatrix 4102.

Submitting Changes

When you perform changes in the web interface and click the *Submit* button, the Mediatrix 4102 validates the changes. A message informs you that the Mediatrix 4102 must be restarted if one or more non-dynamic value was changed. If at least one modified value is invalid, a message informs you that some values are invalid. Most changes are not dynamic and require to restart the Mediatrix 4102.

The Reboot page then opens. You must click *Reboot*.

This restarts the Mediatrix 4102. If the unit is in use when you click *Reboot*, all calls are terminated.

Web Interface Parameters

This chapter describes the parameters you can set with the web interface.

System Page

The *System* page allows you to set the following information:

- ▶ WAN uplink connection
- ▶ LAN interface information
- ▶ STUN parameters

WAN Page

The WAN page allows you to set the uplink information used by the Mediatix 4102.

▶ **To set WAN parameters:**

1. In the web interface, click the *System* link.
This links to the *System – WAN* web page.

Figure 12: System – WAN Web Page

2. Set the *WAN connection type*.
You have the following choices:

Table 16: WAN Connection Type

Connection Type	Description
DHCP	In this connection type, the PPPoE service (<i>pppoeEnable</i> variable) disabled and the configuration source (<i>localHostSelectConfigSource</i> variable) is set to "DHCP". However, some locations may require to manually enter static IP information instead. If this is the case, select the Static connection type and proceed to Step 3.
Static	This connection type may be used for locations where cannot use the DHCP connection type. You are thus required to manually provide the IP information. See Step 3. In this connection type, the PPPoE service (<i>pppoeEnable</i> variable) is disabled and the configuration source (<i>localHostSelectConfigSource</i> variable) is set to "static".
PPPoE	In this connection type, the PPPoE service (<i>pppoeEnable</i> variable) is enabled and the configuration source (<i>localHostSelectConfigSource</i> variable) is set to "static".

3. If the WAN connection type is **Static** (as set in Step 2), enter the following static IP information.

Table 17: IP Addresses Parameters

Parameter	Definition
WAN IP Address	Public IP address of the Mediatrix 4102. This address is used for incoming signalling, media and management traffic.
WAN Network Mask	Subnet mask IP address used by the Mediatrix 4102. The subnet mask enables the network administrator to further divide the host part of the address into two or more subnets. Note: Media5 recommends not to set a network mask of 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.
Default gateway	Default router IP address used by the Mediatrix 4102. A router is a device that connects any number of LANs.
Primary DNS	Primary Domain Name Server IP address used by the Mediatrix 4102. A DNS is an Internet service that translates domain names into IP addresses.
Secondary DNS	Secondary Domain Name Server IP address used by the Mediatrix 4102.

4. If the WAN connection type is **PPPoE** (as set in Step 2), set the PPP user name and password.
When connecting to an access concentrator, it may request that the Mediatrix 4102 identifies itself with a specific user name and password.
There are no restrictions, you can use any combination of characters.
5. Click *Submit* if you do not need to set other parameters.

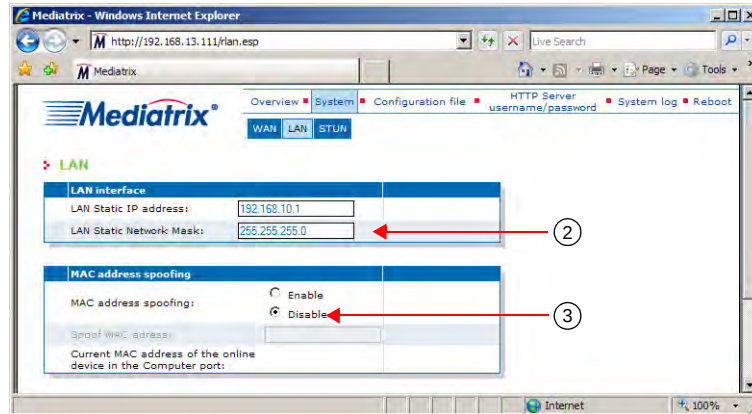
LAN Page

The *LAN* page allows you to set the LAN interface of the Mediatrix 4102.

► **To set LAN parameters:**

1. In the *System* pages, click the *LAN* link.
This links to the *System – LAN* web page.

Figure 13: LAN Web Page



2. Set the static IP address and network mask of the LAN interface.
This is the IP information of the *Computer* connector, where you connect the PC or other IP equipment. The LAN interface is normally used to connect a PC that will have access to the WAN by sharing the Mediatrix 4102 WAN address. See ["LAN Interface" on page 120](#) for more details.



Note: Media5 recommends not to set a network mask of 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.

3. If applicable, enable the MAC Address Spoofing feature.
Spoofing the MAC address is useful in the case of ISPs that use the MAC address of the device connected to the *Computer* interface of the Mediatrix 4102 (e.g., a PC) to identify the connection. Enter the proper MAC address in the *Spoof MAC address* field. The current MAC address of the online device in the *Computer* connector is displayed below the field. A valid MAC address is a series of 12 alphanumeric characters without colons. See ["MAC Address Spoofing" on page 121](#) for more details.

The following MAC addresses are not allowed:

- 000000000000
- FFFFFFFFFFFF
- 01xxxxxxxxxx, where x can be any digit or letter

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

STUN Page

Standards Supported

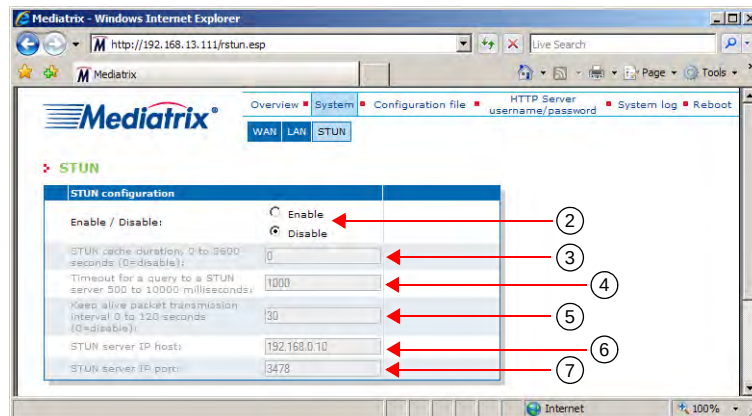
RFC 3489 – STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)

The *STUN* web page allows you to configure the STUN client of the Mediatrix 4102. See "[Chapter 15 - STUN Configuration](#)" on [page 187](#) for more information.

► To set STUN parameters:

1. In the *System* pages, click the *STUN* link.
This links to the *System – STUN* web page.

Figure 14: STUN Web Page



2. Enable the STUN client by selecting the *Enable* option.
3. Set the amount of time, in seconds, the Mediatrix 4102 should keep a STUN query result in its internal cache in the *STUN cache duration* field.
Keeping a query in a cache helps to reduce the amount of unnecessary STUN queries when an RTP or T.38 socket is re-used within a short period of time. Available values range from 0 s to 3600 s. When set to 0, the cache is disabled and the unit performs a STUN query each time a socket needs to be used.
4. Set the maximum amount of time, in milliseconds, the Mediatrix 4102 should wait for an answer to a STUN query sent to a STUN server in the *Timeout for a query to a STUN server* field.
Available values range from 500 ms to 10000 ms.
Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure.
5. Define the interval, in seconds, at which the Mediatrix 4102 sends blank keepalive messages to keep a firewall hole opened in the *Keepalive packet transmission interval* field.
Keepalive messages are used by both the signalling protocol socket and the RTP socket to keep those connections opened through a firewall. Available values range from 0 s to 120 s. When set to 0, no keepalive packet is sent.



Note: Keepalive messages are not supported on the T.38 socket.

6. Set the static STUN server IP address or Fully Qualified Domain Name (FQDN) in the *STUN server IP host* field.
7. Set the static STUN server IP port number in the *STUN server IP port* field.
The default value is **3478**.

8. Click *Submit*.

Configuration File Upload Page

The *Configuration file upload* web page allows you to upload a configuration file from the computer connected to the *Computer* connector of the Mediatrix 4102 into the unit.

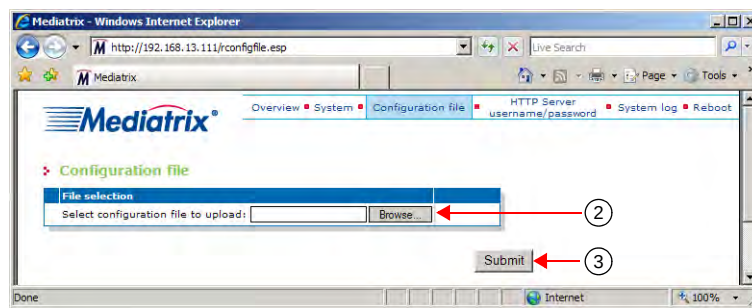
The configuration file is transferred by using the HTTP POST method.

See ["Chapter 10 - Configuration File Download" on page 131](#) for more information on configuration files.

► **To upload a configuration file:**

1. In the web interface, click the *Configuration file* link.
This links to the *Configuration file upload* web page.

Figure 15: Configuration file upload Web Page



2. Select the configuration file you want to upload to the Mediatrix 4102 in the *Select configuration file to upload* field.
You can click the *Browse* button to select a file. This button may not be available, depending on the web browser you are using.
3. Click the *Submit* button.
If a valid configuration file is successfully uploaded, then the Mediatrix 4102 automatically restarts to apply all the new settings. If the Mediatrix 4102 does not restart, this could mean the upload failed.

HTTP Server Password Page

Standards Supported

RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication

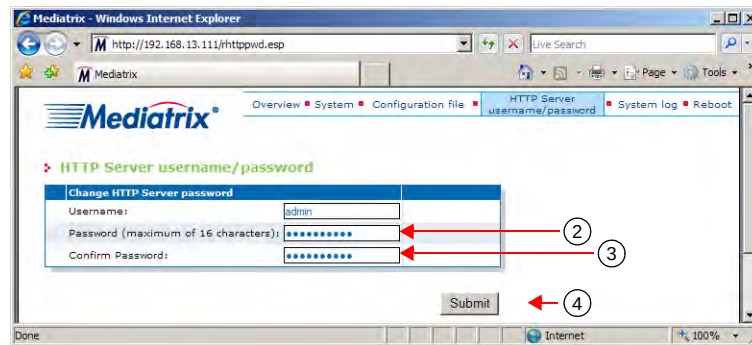
The *HTTP server password* page allows you to modify the default password to access the web interface. The Mediatrix 4102 supports basic HTTP authentication, as described in RFC 2617.

► To change the password:

1. In the web interface, click the *HTTP server password* link.

The following opens:

Figure 16: HTTP server password Page



2. Enter the new password.
The password is case sensitive. It can be a string of 0 to 16 characters. All characters are allowed. However, some special characters, such as accented characters (é, à, etc.), may not work.
3. Retype the password in the *Confirm Password* field.
4. Click *Submit*.
The password resets back to the default value when:
 - Resetting the password by using the `httpServerResetToDefaultPwd` variable (see [“Default User Name and Password” on page 34](#) for more details).
 - Performing a factory reset (see [“Factory Reset” on page 22](#) for more details).

Default User Name and Password

The default user name and password the web interface uses are stored in MIB variables you can modify.

► To modify the default user name and password:

1. In the *httpServerMIB*, set the default user name for the web interface access authentication in the `httpServerUsername` variable.
2. Set the default password for the web interface access authentication in the `httpServerDefaultPassword` variable.
Both changes are immediate and take effect on all new web accesses.

► To reset the web authentication password to the default value:

1. In the *httpServerMIB*, set the `httpServerResetToDefaultPwd` variable to **reset**.
The web password is reset to the default value specified by the `httpServerDefaultPassword` variable.
2. Restart the Mediatrix 4102 so that the change may take effect.

Issue: Factory Reset does not Reset the Default Password Value

The following describes three cases in which the factory reset may not properly reset the HTTP server password. Each case defines the password you must use to access the web interface.

Case #1

You do not modify the password via the Web page and you upgrade to a new software version with a new default password in the profile.

Table 18: Case 1 Issue

Item	Description
Wanted Behaviour	The password to use is the default password in the new profile.
Current Behaviour	The password to use is the default password in the <i>previous</i> version of the profile.
Workaround	Once using the new software version, use the <code>httpServerResetToDefaultPwd</code> variable as described in "Default User Name and Password" on page 34 .

Case #2

You modify the password via the web interface and you upgrade to a new software version with a new default password in the profile.

Table 19: Case 2 Issue

Item	Description
Wanted Behaviour	The password to use is the password modified via the web interface in the older software version.
Current Behaviour	Same as the wanted behaviour.
Workaround	None required.

Case #3

You are performing a factory reset.

Table 20: Case 3 Issue

Item	Description
Wanted Behaviour	The password to use is the default password in the profile.
Current Behaviour	Same as the wanted behaviour.
Workaround	Once using the new software version, use the <code>httpServerResetToDefaultPwd</code> variable as described in "Default User Name and Password" on page 34 .

System Log Page

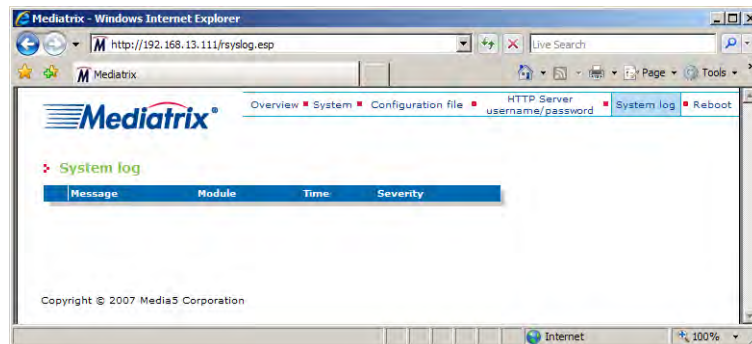
The *System log* page allows you to peruse the last n system log (syslog) messages sent by the Mediatrix 4102 since it last restarted.

► **To access the System log page:**

1. In the web interface, click the *System log* link.

The following opens:

Figure 17: System log Page



Please refer to "[Local Syslog](#)" on page 204 for information on how to set the system log parameters.

SNMP Configuration

Page Left Intentionally Blank

MIB Structure and SNMP

This chapter describes how the Mediatrix 4102 uses the SNMP protocol for its configuration.

SNMP Overview

The Mediatrix 4102 uses the Simple Network Management Protocol (SNMP) for initial software configuration provisioning and subsequent software configuration.

SNMP is a simple request-reply protocol for Internet network management services. It consists of *network management stations* (in this document, they are referred to as a management server) communicating with *network elements*. Management stations are normally workstations that display relevant facts about the elements being monitored.

SNMP works over the IP (Internet Protocol) communication stack. SNMP network management consists of three pieces:

- ▶ The protocol between the manager and the element (SNMP). This details the format of the packets exchanged. Although a wide variety of transport protocols could be used, UDP is normally used with SNMP.
- ▶ A set of common structures and an identification scheme used to reference the variables in the MIB. This is called the *Structure of Management Information (SMI)*.
- ▶ A *Management Information Base (MIB)* that specifies what variables the network elements maintain (the information that can be queried and set by the manager).

Definitions

Structure of Management Information (SMI)

The SMI is the set of rules for specifying the management information that a device maintains. The management information is actually a collection of managed objects, and these rules are used to both name and define these managed objects.

Management Information Base (MIB)

A MIB is a structured collection of all the managed objects a device maintains. The managed objects are structured in the form of a hierarchical tree. At the top of the tree is the most general information available about a network. Each branch of the tree then gets more detailed into a specific network area, with the leaves of the tree as specific as the MIB can get.

Object Identifier (OID)

Object Identifiers (OID) are strings of numbers. They are allocated in a hierarchical manner, so that, for instance, the authority for “1.2.3” is the only one that can say what “1.2.3.4” means. The formal definition of OIDs comes from ITU-T recommendation X.208 (ASN.1), which is available from the ITU.

SNMP Versions

The Mediatrix 4102 supports three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. SNMP defines a few types of messages that are exchanged between the manager and agent.

SNMPv1 Messages

The following messages are specific to SNMPv1.

Table 21: SNMPv1 Message Types

Operator	Description
messages sent from the manager to the agent	
get-request	Get the value of one or more variables.
get-next-request	Get the next variable after one or more specified variables.
set-request	Set the value of one or more variables.
messages sent from the agent to the manager	
get-response	Return the value of one or more variables. This is the message returned by the agent to the manager in response to the get-request , get-next-request , and set-request operators.
trap	Notify the manager when something happens on the agent.

SNMPv2c Messages

There are a few flavours of SNMPv2, SNMPv2c being the most common. The following message is specific to SNMPv2.

Table 22: SNMPv2 Message Type

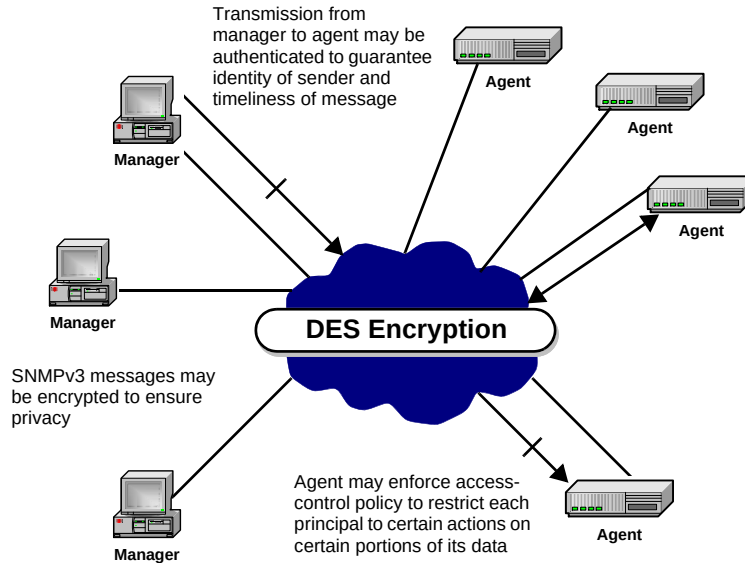
Operator	Description
get-bulk	Uses BULK Requests to query for a tree of information about a network entity. A variable put in command line specifies which portion of the object identifier space will be searched using BULK Requests. All variables in the subtree below the given variable are queried as a single request and their values presented to the user.

This message is sent from the manager to the agent.

SNMPv3 Messages

To correct the security deficiencies of SNMPv1/v2, SNMPv3 was defined with an overall SNMP architecture and a set of security capabilities. SNMPv3 includes three important services: *authentication*, *privacy*, and *access control* (Figure 18). To deliver these services in a flexible and efficient manner, SNMPv3 introduces the concept of a *principal*, which is the entity on whose behalf services are provided or processing takes place.

Figure 18: SNMPv3 Services



SNMP Behaviour

When using SNMP, the following rules apply:

- ▶ Media5 recommends to copy the SNMPv3 user attributes only twice.
- ▶ The administrator may edit the SNMPv3 user attributes:
 - Authentication algorithm (none, MD5, or SHA)
 - Authentication password
 - Encryption algorithm (NULL or DES)
 - Encryption password
 - All SNMPv3 passwords (encryption and authentication) must be at least 8 characters long. You should use the *Unit Manager Network* product to perform SNMPv3 setup. Whatever the MIB browser you use, the unit follows the SNMPv3 standard RFCs.

SNMP can be used in a non-secure or secure management mode.



Warning: The SNMPv3 method for changing the password or encryption key contains a flaw which may result in setting the incorrect password. This problem can happen if you use an incorrect “oldpassword” when changing your password. Always exercise great caution when changing your password or encryption key. Note that you can use the factory reset to clear the SNMPv3 password. See [“Factory Reset” on page 22](#) for more details. See also the *Unit Manager Network Administration Manual*.

Non-Secure Management Mode

In non-secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-write on all MIB tree
- ▶ SNMPv2c: read-write on all MIB tree
- ▶ SNMPv3: read-write on all MIB tree by using:
 - MD5 authentication
 - Authentication password: "Md5Password" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)
- ▶ SNMPv3: read-write on all MIB tree by using:
 - SHA authentication
 - Authentication password: "ShaPassword" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)

Secure Management Mode

In secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-only on all MIB tree
- ▶ SNMPv2c: read-only on all MIB tree
- ▶ SNMPv3: the same values as for SNMPv3 in non-secure management mode



Note: If you forget or lose a password, perform a Factory Reset to reset the unit to the non-secure management mode. See ["Factory Reset" on page 22](#) for more details.

Notes

- ▶ When using SNMPv3 with encryption (DES), you may experience delays when accessing MIB variables. This is normal because encrypting an IP packet takes in general longer than sending it over IP. If you experience any timeout, add some seconds to the timeout period of your MIB browser, and then try to reach the unit again.
- ▶ Suppose that the Mediatrix 4102 accepts requests with authentication only. If you perform requests by using encryption and authentication, assuming that the authentication password is valid, the SNMP agent still responds as if the requests were only authenticated.
- ▶ If you clone an SNMPv3 user, and then remove authentication or privacy for it, ensure that a row in *vacmGroupName* matches its new constraints. If not, the unit is not accessible by using the new clone parameters.

SNMPv3 Special Behaviour

Mediatrix units coming out of factory are set so that you can use all MIB variables by using SNMPv1, SNMPv2c, or SNMPv3. However, you can decide to accept only SNMPv3 access by using passwords known by administrators only for enhanced security. In this case, you should manually disable SNMPv1 / SNMPv2 so that SNMPv3 works properly. The Mediatrix 4102 thus refuses any SNMPv1 or SNMPv2 request it receives. You can disable / enable SNMPv1 / SNMPv2 by using the MIB Browser included in the Media5 Unit Manager Network (or any other MIB Browser) to modify the permissions related to SNMPv1 / SNMPv2 (security model). These permissions are located in the *VacmAccessTable* of the SNMP-VIEW-BASED-ACM-MIB (RFC 2575).

When using exclusively SNMPv3, a row from one of the following tables:

- ▶ *usmUserTable*
- ▶ *vacmSecurityToGroupTable*
- ▶ *vacmAccessTable*
- ▶ *vacmViewTreeFamilyTable*

is saved in flash memory only if these conditions are met:

- ▶ The RowStatus variable (e.g., *vacmAccessRowStatus*) is equal to **active(1)**.
- ▶ The StorageType variable (e.g., *vacmAccessStorageType*) is equal to **nonVolatile(3)**.



Note: The *vacmContextTable* is not saved under any condition.

SNMP Configuration via a Configuration File

You can modify the SNMP configuration of the Mediatrix 4102 by inserting an SNMP Agent section in a configuration file and then transferring this configuration file into the unit. This configuration replaces any configuration set in a profile. For more information on how to use a configuration file for updating the Mediatrix 4102, see [“Chapter 10 - Configuration File Download” on page 131](#).



Caution: The SNMP Agent section contains the default Media5 parameters related to SNMP. Default values enable SNMPv1, SNMPv2, and SNMPv3 and provide default Media5 credentials for SNMPv3.

The SNMP Agent section is located in the *SnmGenericTemplate.xml* file located under *Unit Manager Network 3.2\UnitManager\DefaultCfgFile* folder. The contents of the *SnmGenericTemplate.xml* file may be appended at the end of the generated XML file. See the Unit Manager Network documentation for more details.

The SNMP agent section must not be separated by other comments or OIDs in the configuration file.

If you transfer a configuration file with an SNMP Agent section that constitutes a change from the SNMPv3 configuration currently in use, the new configuration is applied and the unit then restarts so that the changes take effect.

A few notes:

- ▶ Once an SNMPv3 configuration is in effect in the Mediatrix 4102, it is not possible to revert the unit back to SNMPv1 or SNMPv2c by sending it a configuration file that does not include an SNMP Agent configuration section.
- ▶ If you perform a factory reset, all settings previously applied via the configuration file (including the SNMPv3 configuration) are lost and the unit reinitializes by using the current profile.

Figure 19: SNMP Agent Section Example

```
<SnmAgentConfig>
<snmpV2>
  <snmpModules>
    <snmpUsmMIB>
      <usmMIBObjects>
        <usmUser>
          <usmUserTable>
            <a>
              <usmUserSecurityName ValueType="OCTET_STRING" Value="Md5DesUser"/>
              <usmUserAuthProtocol ValueType="OID" Value="1.3.6.1.6.3.10.1.1.2"/>
              <usmUserAuthPassword ValueType="OCTET_STRING" Value="Md5DesUser"/> ← 🔒
              <usmUserPrivProtocol ValueType="OID" Value="1.3.6.1.6.3.10.1.2.2"/>
              <usmUserPrivPassword ValueType="OCTET_STRING" Value="Md5DesUser"/> ← 🔒
              <usmUserStorageType ValueType="UINT32" Value="4"/>
              <usmUserStatus ValueType="UINT32" Value="1"/>
            </a>
            <b>
              <usmUserSecurityName ValueType="OCTET_STRING" Value="ShaDesUser"/>
              <usmUserAuthProtocol ValueType="OID" Value="1.3.6.1.6.3.10.1.1.3"/>
              <usmUserAuthPassword ValueType="OCTET_STRING" Value="ShaDesUser"/> ← 🔒
              <usmUserPrivProtocol ValueType="OID" Value="1.3.6.1.6.3.10.1.2.2"/>
              <usmUserPrivPassword ValueType="OCTET_STRING" Value="ShaDesUser"/> ← 🔒
              <usmUserStorageType ValueType="UINT32" Value="4"/>
              <usmUserStatus ValueType="UINT32" Value="1"/>
            </b>
          </usmUserTable>
        </usmUser>
      </usmMIBObjects>
    </snmpUsmMIB>
    <snmpVacmMIB>
      <vacmMIBObjects>
        <vacmMIBViews>
```

```

<vacmViewTreeFamilyTable>
  <a>
    <vacmViewTreeFamilyViewName ValueType="OCTET_STRING" Value="PublicView"/>
    <vacmViewTreeFamilySubtree ValueType="OID" Value="1"/>
    <vacmViewTreeFamilyMask ValueType="OCTET_STRING" Value="&#128;"/>
    <vacmViewTreeFamilyType ValueType="UINT32" Value="1"/>
    <vacmViewTreeFamilyStorageType ValueType="UINT32" Value="4"/>
    <vacmViewTreeFamilyStatus ValueType="UINT32" Value="1"/>
  </a>
  <b>
    <vacmViewTreeFamilyViewName ValueType="OCTET_STRING" Value="PrivateView"/>
    <vacmViewTreeFamilySubtree ValueType="OID" Value="1"/>
    <vacmViewTreeFamilyMask ValueType="OCTET_STRING" Value="&#128;"/>
    <vacmViewTreeFamilyType ValueType="UINT32" Value="1"/>
    <vacmViewTreeFamilyStorageType ValueType="UINT32" Value="4"/>
    <vacmViewTreeFamilyStatus ValueType="UINT32" Value="1"/>
  </b>
</vacmViewTreeFamilyTable>
</vacmMIBViews>
<vacmSecurityToGroupTable>
  <a>
    <vacmSecurityModel ValueType="UINT32" Value="1"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="PublicUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="Snmpv1RWPublicGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </a>
  <b>
    <vacmSecurityModel ValueType="UINT32" Value="1"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="PrivateUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="Snmpv1RWPrivateGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </b>
  <c>
    <vacmSecurityModel ValueType="UINT32" Value="2"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="PublicUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="Snmpv2cRWPublicGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </c>
  <d>
    <vacmSecurityModel ValueType="UINT32" Value="2"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="PrivateUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="Snmpv2cRWPublicGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </d>
  <e>
    <vacmSecurityModel ValueType="UINT32" Value="3"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="Md5DesUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="AuthPrivGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </e>
  <f>
    <vacmSecurityModel ValueType="UINT32" Value="3"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="ShaDesUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="AuthPrivGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </f>
  <g>
    <vacmSecurityModel ValueType="UINT32" Value="3"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="AuthNoPrivUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="AuthNoPrivGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </g>
  <h>
    <vacmSecurityModel ValueType="UINT32" Value="3"/>
    <vacmSecurityName ValueType="OCTET_STRING" Value="NoAuthNoPrivUser"/>
    <vacmGroupName ValueType="OCTET_STRING" Value="NoAuthNoPrivGrp"/>
    <vacmSecurityToGroupStorageType ValueType="UINT32" Value="4"/>
    <vacmSecurityToGroupStatus ValueType="UINT32" Value="1"/>
  </h>
</vacmSecurityToGroupTable>
<vacmAccessTable>
  <a>
    <vacmAccessContextPrefix ValueType="OCTET_STRING" Value="AuthPrivGrp"/>
    <vacmAccessSecurityModel ValueType="UINT32" Value="3"/>
    <vacmAccessSecurityLevel ValueType="UINT32" Value="3"/>
  </a>

```

```

<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PublicView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</a>
<b>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="AuthNoPrivGrp"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="3"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="2"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PublicView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</b>
<c>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="NoAuthNoPrivGrp"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="3"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="1"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv3
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PublicView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</c>
<d>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="SnmPV1RWPUBLICGRP"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="1"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="1"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv1
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv1
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PublicView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</d>
<e>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="SnmPV1RWPRIVATEGRP"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="1"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="1"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv1
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv1
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PrivateView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</e>
<f>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="SnmPV2cRWPUBLICGRP"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="2"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="1"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv2
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv2
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PublicView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</f>
<g>
<vacmAccessContextPrefix ValueType="OCTET_STRING" Value="SnmPV2cRWPRIVATEGRP"/>
<vacmAccessSecurityModel ValueType="UINT32" Value="2"/>
<vacmAccessSecurityLevel ValueType="UINT32" Value="1"/>
<vacmAccessContextMatch ValueType="UINT32" Value="1"/>
<vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv2
<vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/> ← Enable/Disable SNMPv2
<vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PrivateView"/>
<vacmAccessStorageType ValueType="UINT32" Value="4"/>
<vacmAccessStatus ValueType="UINT32" Value="1"/>
</g>
</vacmAccessTable>
</vacmMIBObjects>
</snmpVacmMIB>
</snmpModules>
</snmpV2>
</SnmAgentConfig>

```


Enabling/Disabling SNMPv1, SNMPv2 and SNMPv3

By default, the parameters in the SNMP Agent section enable SNMPv1 and SNMPv2. However, you may want to disable them.

► To enable SNMPv1 and SNMPv2:

1. Ensure that the *Value* parameters of the fields `<vacmAccessReadViewName>` and `<vacmAccessWriteViewName>` are set to "PublicView" in the following groups:
 - Snmpv1RWPUBLICGrp
 - Snmpv1RWPrivateGrp
 - Snmpv2cRWPUBLICGrp
 - Snmpv2cRWPrivateGrp

These fields are identified in [Figure 19 on page 43](#) with the following icon:  Enable/Disable SNMPv1-2.

► To disable SNMPv1 and SNMPv2:

1. Ensure that the fields `<vacmAccessReadViewName>` and `<vacmAccessWriteViewName>` are empty in the following groups:
 - Snmpv1RWPUBLICGrp
 - Snmpv1RWPrivateGrp
 - Snmpv2cRWPUBLICGrp
 - Snmpv2cRWPrivateGrp

These fields are identified in [Figure 19 on page 43](#) with the following icon:  Enable/Disable SNMPv1-2.

► To enable SNMPv3:

1. Ensure that the *Value* parameters of the fields `<vacmAccessReadViewName>` and `<vacmAccessWriteViewName>` are set to "PublicView" in the following groups:
 - AuthPrivGrp
 - AuthNoPrivGrp
 - NoAuthNoPrivGrp

These fields are identified in [Figure 19 on page 43](#) with the following icon:  Enable/Disable SNMPv3.

► To disable SNMPv3:

1. Ensure that the fields `<vacmAccessReadViewName>` and `<vacmAccessWriteViewName>` are empty in the following groups:
 - AuthPrivGrp
 - AuthNoPrivGrp
 - NoAuthNoPrivGrp

These fields are identified in [Figure 19 on page 43](#) with the following icon:  Enable/Disable SNMPv3.

Changing SNMPv3 Credentials

The SNMP Agent section provides default Media5 credentials for SNMPv3. You can change these credentials.

► To change SNMPv3 credentials:

1. Change the password in the following fields:
 - usmUserAuthPassword (section **Md5DesUser**)
 - usmUserPrivPassword (section **Md5DesUser**)
 - usmUserAuthPassword (section **ShaDesUser**)
 - usmUserPrivPassword (section **ShaDesUser**)

These fields are identified in [Figure 19 on page 43](#) with the following icon : .



Caution: SNMPv3 passwords must be at least 8 characters long.

MIB Structure

The current MIB structure is defined in the SMI file, called *MX-SMI.my*. The SMI contains seven main groups.

Table 23: Structure of Management Information

Group	Description
mediatrixProducts	Each Media5 product has been assigned with its own sysObjectID value.
mediatrixAdmin	Root of the modules used for the administration of the products.
mediatrixMgmt	Root of the modules used to manage the products.
mediatrixConfig	Root of the modules used to configure the products.
mediatrixIpTelephony Signaling	Root of the modules used to configure the signalling protocols.
mediatrixModules	Provides a root in which modules can register their module entity. No MIB variables actually appear under this node.
mediatrixExperimental	The experimental sub-tree is the area where objects and events in MIBs under development can be placed without fear of conflicting with other MIBs. When the items rooted under an experimental sub-tree are ready for release, the sub-tree is re-attached under a permanent branch. Please note that Media5' configuration tool – the Unit Manager Network – does not support MIBs that are located under the <i>mediatrixExperimental</i> branch of the MIB structure. The Unit Manager Network does not have specific tasks to manage variables in experimental MIBs. Even though the Unit Manager Network can view experimental MIBs, SNMP operations may not work properly on them.

All parameters in the MIBs have been configured by default upon start up. However, if you need to modify some of these parameters (for example, parameters related to the country in which you are), use a MIB browser.

Textual Conventions

Textual conventions are defined in a module to ensure that all variables throughout the MIB structure use the same syntax and types. The type of each variable is defined in the *Composed syntax* line.

Table 24: Textual Conventions

Type	Definition
MxIpHostName	Represents an IP address or a domain name.
MxIpAddress	Represents an IP address.
MxIpPort	The TCP or UDP port number range. Values can be between 1 and 65535.
MxIpSubnetMask	Represents an Internet subnet mask.
MxIpSelect ConfigSource	Indicates the source to use during the next restart sequence for the provisioning of the localHost MIB objects. - static: uses static values provided by the user (such as DNS addresses, router, etc.). - dhcp: uses the DHCP server to retrieve the configuration of the localHost MIB objects.
MxIpConfigSource	Indicates the source used during the last restart sequence for the provisioning of the localHost MIB objects. - static: the user provided static values such as DNS addresses, router, etc. - dhcp: the DHCP server was used to retrieve the configuration of the localHost MIB objects. - Default: hardcoded values for recovery mode were used.
MxIpDhcpSite SpecificCode	Represents a DHCP site specific code. Values can be between 128 and 254 or 0. You can enter this code in your DHCP server to define IP addresses. Refer to "Chapter 5 - IP Address and Network Configuration" on page 55 for more details.
MxFloatingPoint	Represents a floating point number.
MxAdvancedIpPort	The TCP or UDP port number range. Values can be between 0 and 65535. The port number value 0 is used for special functionality defined in the variable definition.
MxEnableState	Represents an enabled/disabled state (boolean value).
MxActivationState	Represents an active/inactive state (boolean value).
MxSignalingAddress	Represents a valid signalling address.
MxDigitMap	A digit map is a sequence used to determine when the dialing of DTMFs is completed. See "Chapter 21 - Digit Maps" on page 285 for more details.

Objects, Conformance, and Events

Each MIB may have three types of data.

Table 25: MIB Data Types

Type	Description
Object	Represents the actual variables that can be set.
Conformance	Describes one or more groups to which the product may conform. This allows to have an exact idea of what a unit supports by glancing at the conformance information.
Event	An event is sent to tell what type of data will be received, but not the data itself. This is used to "warn" in advance what is coming.

IP Addresses

The MIB structure contains many IP addresses that can be set or viewed. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

Persistence

A variable may either be persistent or volatile.

Table 26: Storage Clauses

Clause	Definition
Persistent	<i>Persistent</i> parameters are saved into the unit's memory and restored when it restarts. All the variables with the <i>Access = Read Write</i> attribute are persistent, except the variables representing commands (such as <i>sysAdminCommand</i>).
Volatile	<i>Volatile</i> parameters are lost every time the unit restarts. This type of parameter includes toggling parameters such as requesting a configuration file or a software download. <i>Statistics</i> are also volatile parameters that are lost every time the unit restarts.

Changing a Parameter Value

The Mediatrix 4102 software parameters are fully programmable by using the SNMP protocol. There are two ways to set up and configure a unit:

- ▶ By using a SNMP browser to contact the MIBs of the Mediatrix 4102. It is assumed that you have basic knowledge of TCP/IP network administration.
You can use the MIB browser built in the Media5' Unit Manager Network. See [“Unit Manager Network – Element Management System” on page xvii](#) for more details.
You can also use any third-party SNMP browser or network management application running the SNMP protocol to monitor and configure the Mediatrix 4102. However, the information may not be presented in the same manner depending on the SNMP browser used.
- ▶ By using the graphical user interface of the Management Server.
The Management Server could be Media5's Unit Manager Network. See [“Unit Manager Network – Element Management System” on page xvii](#) for more details.

Be sure to use the MIB files that match the version of the MIB located inside the current software build of the unit.

Locate the proper parameter to modify and change (SET) its value. Most of the parameters require to restart the Mediatrix 4102 unit. A restart may be software-initiated or manually initiated by unplugging the unit. It deletes all statistics stored and overwrites all volatile parameter values in the configuration file. A restart also reinitiates the entire unit's initial provisioning sequence.



Note: When performing a SET operation on any MIB variable, Media5 recommends to wait at least 30 seconds before shutting down the unit. This gives time to the software to update configuration data in flash memory.

Tables

There are two types of tables used in the MIB structure. They contain:

- ▶ Generic variables that apply to each line of a unit. This avoids to repeat each set of variables for each line it has.
- ▶ The administrative commands and status related to a managed object.

Generic Variables

All tables used to set variables for one or more lines (such as the *voiceIfTable*) are based on the *ifTable*, or interface table.

The *ifTable* lists the interfaces of a unit. In other words, it basically defines the lines that are used by the unit. It contains an *ifIndex*, which defines the interfaces. It may also contain interfaces such as:

- ▶ the LoopBack (*lo*) and Ethernet (*eth0*) interfaces.
- ▶ the actual voice interfaces (lines) of the unit.

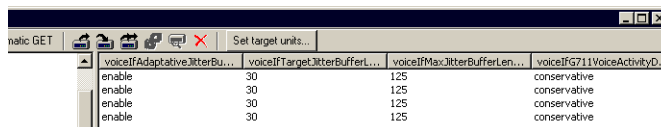
[Table 27](#) gives an example of the *ifTable*.

Table 27: ifTable Example

ifIndex	Type	Description
1	LoopBack	lo
2	Ethernet(0)	eth0
3	Voice FXS	(0)
4	Voice FXS	(1)
5	Voice FXS	(2)
...	...	...
26	Voice FXS	(24)

[Figure 20](#) shows a table built in the Unit Manager Network from the *voiceIfTable* parameters.

Figure 20: voiceIfTable Example



voiceIfAdaptiveJitterBu...	voiceIfTargetJitterBufferL...	voiceIfMaxJitterBufferLen...	voiceIfG711VoiceActivityD...
enable	30	125	conservative
enable	30	125	conservative
enable	30	125	conservative
enable	30	125	conservative

You can perform GET and SET operations on these parameters.

Variables for Administrative Commands

Administrative commands are built on a hierarchical structure of parents-children. A command applied on a parent is propagated to all of its children.

There are two tables used to define administrative commands to groups:

- ▶ *groupAdmin*: A group may be the unit itself (gateway) or other instances. There are no instances other than the gateway defined at this moment.
- ▶ *ifAdmin*: This table applies to each interface of the unit.

groupAdmin Table

The *groupAdmin* table sends administrative commands at the highest instance in a hierarchy (such as the gateway).

Table 28: groupAdmin Parameters

Parameter	Description
groupSetAdmin	Command to set the administrative state of the system.
groupAdminState	The administrative state of the group. Indicates the current maintenance state of a group. Available states are unlocked, shutting down, and locked.
groupOpState	The operational state of the group. It reflects the group's internal state. Available states are enabled and disabled.
groupUsageState	The usage state of the group. Indicates the running state of a group. Available states are idle, active, busy, and idle-unusable.
groupAdminType	The type of resources managed by the group.
groupAdminDescription	The description of the group.
groupAdminParent Group	The parent's group. This is the index (<i>groupAdminIndex</i>), taken from this table (<i>groupAdminTable</i>), of the group that is the parent. If there is no parent, the value "-1" is used.

ifAdmin Table

The *ifAdmin* table is similar to the *groupAdmin* table, except that it applies to interfaces.

Table 29: ifAdmin Parameters

Parameter	Description
ifAdminSetAdmin	Command to set the administrative state of the current interface.
ifAdminAdminState	The administrative state of the current interface. It indicates the current maintenance state of a gateway component. Available states are unlocked, shutting down, locked, and permanentLock.
ifAdminOpState	The operational state of the current interface. This state reflects the component's internal state. Available states are enabled and disabled.
ifAdminUsageState	The usage state of the current interface. It indicates the running state of a voice component. Available states are idle, active, busy, and idle-unusable.
ifAdminParentType	The parents type of this interface.
ifAdminParent	The index of the parent of this interface.

SNMP Access Limitation

The SNMP access to the Mediatrix 4102 can be limited to only one of its interface or all interfaces.

► **To limit the access to the SNMP interface:**

1. In the *snmpAgentMIB*, select the interface where the Mediatrix 4102 can be accessed via SNMP in the *snmpAgentAccess* variable.

You have the following choices:

Table 30: SNMP Access Limitation Parameters

Access	Description
lanOnly	SNMP connections are only permitted on the LAN side, which is usually associated with the <i>LAN</i> connector. The LAN IP address is provisioned by the <i>lanStaticAddress</i> variable.
wanOnly	SNMP connections are only permitted on the WAN side, which is usually associated with the <i>WAN</i> connector. However, if the WAN interface is down and the unit reverts to its LAN configuration, the SNMP agent can access the Mediatrix 4102 on its LAN interface.
all	SNMP connections are permitted on both the LAN and WAN sides.

Current MIB Version

You can find out the version of the MIB currently in the Mediatrix 4102.

1. In the *sysMgmtMIB*, locate the *sysMibVersion* variable.
This variable displays the current version of the MIB.

Sending Configuration Data to the Mediatrix 4102

The configuration data can be provisioned into the Mediatrix 4102 in two ways:

- as a configuration file sent from the Management Server to the Mediatrix 4102 via TFTP
- as a MIB sent from the Management Server to the Mediatrix 4102 via SNMP

Configuration File

The configuration file is the fastest way to deliver the necessary information. This may be important when initializing a large number of units at the same time. The configuration file is mostly used for the initial provisioning sequence (see [“Initial Provisioning Sequence” on page 15](#) for more details).

For more information on how to use a configuration file for updating the Mediatrix 4102, see [“Chapter 10 - Configuration File Download” on page 131](#).

Management Information Base – MIB

Sending information via SNMP means that individual variables can be changed without sending the whole MIB. You could use a dual system where a configuration file is sent for initial configuration and a MIB browser / SNMP browser is used to implement minor changes.

The Mediatrix 4102 has several configurable MIBs. All variables in these MIBs have been configured by default upon start up. However, if you need to modify some of these variables, use a MIB browser.

Switching Protocols

You can switch between protocols and the proper settings are activated upon restart.

► **To switch protocols:**

1. In the *telephonyMIB*, locate the *telephonyIpSignalingProtocol Selection* variable.
This variable allows you to switch from one protocol to another. It can only be used to toggle between the MGCP and NCS signalling protocols. Attempting to switch from MGCP/NCS to SIP or from SIP to MGCP/NCS has no effect.
2. Set the *telephonyIpSignalingProtocolSelection* variable to either **MGCP** or **NCS**.
3. Restart the Mediatrix 4102 unit.
After the unit restarts, it uses the selected protocol. See:
 - [“Chapter 6 - MGCP Protocol Features” on page 75](#)
 - [“Chapter 7 - NCS Protocol Features” on page 99](#)

IP Address and Network Configuration

The Mediatrix 4102 must be provisioned with various IP addresses and network parameters to be fully functional. This occurs each time the Mediatrix 4102 is started or when an IP address value is changed in the MIB. The Mediatrix 4102 can use static network parameters as well as parameters provided by a DHCP server, an access concentrator, or even a DNS.

This chapter assumes that you know how to set up and use a DHCP and DNS server. If not, ask your network administrator to set up DHCP-related variables.

This chapter also refers to the MIB structure of the configuration variables. Refer to [“Chapter 4 - MIB Structure and SNMP” on page 39](#) for more details.

IP Addresses

The MIB structure contains IP addresses that can be set or viewed. These IP addresses are physically located in their relevant MIB. For instance, the IP addresses for the Syslog daemon are located in the *syslogMIB*. However, when viewing the MIB structure in a MIB browser such as the Media5 Unit Manager Network, the IP addresses are grouped in two distinct folders for easy management.

Table 31: IP Addresses Folders

Folder	Description
ipAddressStatus	Lists all the IP addresses used by the unit, in read-only format.
ipAddressConfig	Lists all the IP addresses you can set. Changes made in this folder are reflected in the <i>ipAddressStatus</i> folder.

IP Addresses Formats in the DHCP Server

You can use a number of formats when defining IP addresses in the DHCP server.

Table 32: IP Addresses Formats in DHCP Server

Format	Description	Allowed Char.
Decimal	You can enter IP addresses in the widely-used (base 10) decimal format. For instance, a decimal IP address would be 192.168.0.9. IP addresses cannot contain decimal numbers higher than 255.	0..9
Hexadecimal	You can enter IP addresses in (base 16) hexadecimal format. Prepending “0x” to the value instructs the unit to interpret it as hexadecimal. For instance, the decimal IP address 192.168.0.9 translates to 0xC0.0xA8.0x0.0x9 in hexadecimal format.	0..9, A..F
Octal	You can enter IP addresses in (base 8) octal format. Prepending “0” to the value instructs the unit to interpret it as octal. For instance, the decimal IP address 192.168.0.9 translates to 0300.0250.00.011 in octal format.	0..7

You can make combinations of the three bases in a single string, because each number in the string is interpreted separately. For instance, 0300.0xA8.000.9 translates to the decimal IP address 192.168.0.9.

There may be some confusion between the three available IP address formats. In particular, it is important to understand that prefixing “0” to the values makes them interpreted as octal values. For instance, the string 192.168.0.009 is not valid because 009 is interpreted in octal, and the digit “9” does not exist in that base.

Provisioning Source

The Mediatrix 4102 IP information may come from a variety of sources.

Table 33: IP Address Provisioning Sources

Source	Description
Static	You manually enter the value and it remains the same every time the Mediatrix 4102 restarts. If you do not specify a value, a default static value applies.
DHCP	The value is obtained at start-time by querying a DHCP server and using standard DHCP fields or options. See RFC 2131 section 2 and RFC 2132.
DHCP – Site specific options	The value is obtained at start-time by querying a DHCP server and using a non-standard option specific to the site where the Mediatrix 4102 is used. See “Site Specific Options” on page 68 for more details.
DHCP – Vendor specific options	The value is obtained at start-time by querying a DHCP server and using a standard option that is reserved for storing vendor specific information. See “Vendor Specific Options” on page 67 for more details.
DNS	The value is obtained at start-time by querying a DNS server.
None	The value is not provisioned. The application provides an acceptable default.
Automatic	The configuration source is selected by the Mediatrix 4102, following a preference order and the availability of some services.
PPP-IPCP ^a	The value is obtained during the PPP network-layer protocol phase from the IPCP configuration options.

a. See RFC 1332 “The PPP Internet Protocol Control Protocol (IPCP)”, for more details.

Services

This section describes the services the Mediatrix 4102 uses and their settings. Most of these services require that you define their IP address and, if required, port number. See [“DHCP Server Configuration” on page 66](#) for more details.

Configuration variables of network parameters are defined in the MIB structure under the *ipAddressConfig* folder. This folder is subdivided into groups, one for each service that requires a network parameter.

Configuration Source

The configuration your Mediatrix 4102 uses can either be:

- ▶ dynamically assigned (network parameters assigned by a DHCP Server)
- ▶ static (network parameters you manually defined in the MIB structure)

DHCP Configuration

Using DHCP-assigned IP addresses ensures that the Mediatrix 4102 receives the addresses that are stored in the DHCP server. This assumes that you have previously set the DHCP server with the proper values. See [“DHCP Server Configuration” on page 66](#) for more details.

The Mediatrix 4102 can receive numerous information from the DHCP server, including the vendor or site specific information. Note that the Mediatrix 4102 does not make a DHCP request in the following cases:

- ▶ If all MIB variables *xxSelectConfigSource* are set to **static** at start-up.
- ▶ If one of the MIB variables *xxSelectConfigSource* is set to **dhcp** after the initialization process.

When the Mediatrix 4102 uses a DHCP server for network parameters, it must always have at least the following three valid parameters:

- ▶ IP Address
- ▶ Subnet Mask
- ▶ Default Gateway

If the parameters are not valid (i.e., the default gateway is not in the same subnet as the IP address), the Mediatrix 4102 will not work properly.

Verifying the DHCP-Assigned IP Addresses

You can query the MIB structure to see the IP addresses that have been assigned to the Mediatrix 4102. Those IP addresses are located under the *ipAddressStatus* folder in read-only variables.

This assumes that you know the local host IP address. To get the local host IP address of a Mediatrix unit, use the autodetect feature of the Media5' Unit Manager Network product. See ["Unit Manager Network – Element Management System" on page xvii](#) for more details.

Static Configuration

Using static IP addresses allows you to bypass the DHCP server or still be able to use the Mediatrix 4102 if you are not running a DHCP server.

In this case, having one or more configuration source variable set to DHCP slows down the restart process. If any information is set to come from the DHCP server (for example, SNTP address), the restarting unit waits for a maximum period of two minutes if the DHCP server cannot be reached, even if most other settings are set to "static".

The reason for this delay is that the Mediatrix 4102 cannot function as configured if part of its configuration (the DHCP information) is unavailable. To avoid this problem, you can set all configuration sources the Mediatrix 4102 supports to "static".



In the *Unit Manager Network Administration Manual*, refer to chapter *Performing Actions on Mediatrix Units*, section *Removing all DHCP Options*.

▶ To set all configuration sources to static:

1. In the *sysAdminMIB*, set the *sysAdminCommand* variable to *setConfigSourcesStatic*.

Local Host

The *ipAddressConfigLocalHost* group allows you to set the IP information the Mediatrix 4102 needs to work properly. This group is vital to the proper operation of the Mediatrix 4102. If a variable of this group is not properly set, the Mediatrix 4102 may not be able to restart and be contacted after it has restarted.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *IP Configuration*.

▶ To select the local host configuration source:

1. In the *ipAddressConfig* folder, locate the *localHostSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group).

2. Set this variable to either **static** or **dhcp**.

Table 34: Local Host Variables

Variable	Default Static Value	DHCP Source
localHostAddress	"192.168.0.1"	Yiaddr field
localHostPrimaryDns ^a	"192.168.0.10"	Option 6 (first of the list)
localHostSecondaryDns ^a	"192.168.0.10"	Option 6 (second of the list)
localHostDefaultRouter ^b	"192.168.0.10"	Option 3 (first of the list)
localHostSubnetMask	"255.255.255.0"	Option 1
localHostDhcpServer	"" (cannot be set)	Siaddr field

a. If you do not want to use a DNS, set the variable to **0**.

b. If you are not using a default router, set the variable to **0.0.0.0**. Setting the default router IP address to "0.0.0.0" may lead to software download problems. See the troubleshooting section ["Software Upgrade Issues" on page 216](#) for more details.



Note: Media5 recommends not to set a static subnet mask address of 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.



Note: If the *localHostDnsOverrideEnable* or *telephonyDnsOverrideEnable* variable is enabled, the primary and secondary DNS addresses are set with static values. See ["Static DNS" on page 60](#) for more details.

In the table above, the only variables that allow an empty string are: *localHostPrimaryDns*, *localHostSecondaryDns* and *localHostDefaultRouter*.

3. Restart the Mediatix 4102 so that the changes may take effect.

WAN Address Configuration Source

The Wide Area Network (WAN) address is the public IP address attributed to the Mediatix 4102. This address is used for incoming signalling, media and management traffic.

► To set the WAN IP address configuration source:

1. In the *ipAddressConfig* folder, locate the *localHostWanAddressSelectConfigSource* variable (under the *ipAddressConfigLocalHost* group).
This variable indicates the source to be used for the provisioning of the WAN address. It offers the following choices:

Table 35: WAN IP Address Source Settings

Option	Description
localAddress	The WAN address is the one that is set in the <i>localHostAddress</i> variable, whereas the <i>localHostStaticWanAddress</i> is ignored.
static	The Mediatix 4102 has a static WAN address. The address is configured in the <i>localHostStaticWanAddress</i> variable. Note that this setting allows a limited NAT traversal scheme.
pppoe	The Mediatix 4102 uses the PPP over Ethernet in order to obtain its WAN IP address. The PPPoE service must be enabled for the WAN address to be configured.
automatic	If the PPPoE service is enabled, the Mediatix 4102 uses <i>pppoe</i> as the configuration source. Otherwise it uses <i>localAddress</i> .

Table 36: WAN IP Address Source

Variable	Default Static Value	DHCP Source
localHostWanAddress	"192.168.0.1"	Option IP-Address

- Restart the Mediatrix 4102 so that the changes may take effect.

LAN Interface Configuration

No DHCP value is available, you can define LAN information with only static values.

Table 37: LAN Interface Source

Variable	Default Static Value	DHCP Source
lanStaticAddress	192.168.10.1	N/A
lanStaticNetworkMask	255.255.255.0	N/A



Note: Do not set the *lanStaticAddress* variable to 0.0.0.0. This could prevent the unit from properly sending a DHCP discover request.



Note: Media5 recommends not to set the *lanStaticNetworkMask* variable to 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.

FQDN Configuration Source

You can select where to get the Fully Qualified Domain Name (FQDN) of the gateway. The Mediatrix 4102 uses the FQDN to register to the MGCP/NCS call agent.

► To select the FQDN configuration source:

- In the *ipAddressConfig* folder, locate the *localHostFqdnSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group).
This variable indicates the source to be used for the provisioning of the Mediatrix 4102 FQDN information.

Table 38: FQDN Configuration Source

Source	Comment
static	Set the <i>localHostStaticFqdn</i> variable in the <i>ipAddressConfigLocalHostStatic</i> group.
dhcp	The DHCP-provided "host name" (option number 12) is used. No site specific code is provided. The Mediatrix 4102 takes the FQDN in the DHCP offer.
dns	The FQDN is set with the name associated to the host IP address. This DNS may be provided by the DHCP server or taken from the <i>localHostStaticPrimaryDns</i> or <i>localHostStaticSecondaryDns</i> variables.
none	The FQDN is blank. In this case, the domain name is replaced by an IPv4 address in dotted decimals represented as a text string inserted within angle brackets, e.g., [128.96.41.1]. This domain name is used to register the unit to the call agent.

The default value is **none**.

You can see the source used during the last restart sequence in the read-only variable *localHostFqdnConfigSource* (*ipAddressStatusLocalHost* group).

You can see the FQDN value assigned to the Mediatrix 4102 in the read-only variable *localHostFqdn* (*ipAddressStatusLocalHost* group).

2. Restart the Mediatrix 4102 so that the changes may take effect.

SNMP Configuration

No DHCP value is available, you can define SNMP information with only static values.

Table 39: SNMP Source

Variable	Default Static Value	DHCP Source
localHostSnmpPort	161	N/A



In the *Unit Manager Network Administration Manual*, refer to chapter *Working with SNMP*, section *Setting Unit SNMP Preferences*.

The Mediatrix 4102 uses the SNMP protocol for software configuration. Set the following SNMP-related variable to properly use the protocol.

Table 40: SNMP Configuration Variables

Variable	Description
localHostStaticSnmpPort	Default SNMP agent port, which is the port number to use to reach the local host via SNMP protocol. Restart the unit to update this parameter. Default Value: 161 Note: If you change the SNMP agent port, change the port used in the management server or MIB Browser. Not doing so will prevent you from contacting the unit. The Management Server could be the Media5 Unit Manager Network. See “Unit Manager Network – Element Management System” on page xvii for more details.

You can query the SNMP information assigned by the DHCP server in the following variables (in the *ipAddressStatus* folder):

- ▶ localHostSnmpPort
- ▶ msTrapPort

Static DNS

By default, the Mediatrix 4102 and the networked PC (linked in a LAN with the unit) receive DNS IP addresses according to the configuration source you have defined in the *localHostSelectConfigSource* variable. In general, these addresses are provided by an ISP (Internet Service Provider) via PPPoE or DHCP.

However, you may require that the Mediatrix 4102 and the networked PC use different DNS addresses. If that is the case, you can set static values for the primary and secondary DNS IP addresses, even when the Mediatrix 4102 is set by DHCP. These static values can thus override PPPoE and DHCP provisioning. This feature could be useful in the case where your ISP (Internet Service Provider) and your ITSP (Internet Telephony Service Provider) use different DNS IP addresses or when a Mediatrix 4102 and a networked PC need to use a different DNS. e Mediatrix 4102 may receive DNS addresses from three sources:

- ▶ PPPoE or from the static local host DNS IP addresses
- ▶ from the static telephony DNS IP addresses

[Table 41](#) explains how DNS addresses are attributed to the Mediatrix 4102 and the networked PC.

Table 41: DNS Addresses Possibilities

localHostDns OverrideEnable	telephonyDns OverrideEnable	DNS address of Mediatrix 4102	DNS address of the Networked PC
disabled	disabled	DNS from ISP	DNS from ISP
disabled	enabled	static telephony DNS	DNS from ISP

Table 41: DNS Addresses Possibilities

localHostDnsOverrideEnable	telephonyDnsOverrideEnable	DNS address of Mediatrix 4102	DNS address of the Networked PC
enabled	disabled	static local host DNS	static local host DNS
enabled	enabled	static telephony DNS	static local host DNS

► **To use static DNS IP addresses:**

1. In the *ipAddressConfig* folder, set the *localHostDnsOverrideEnable* variable (under the *ipAdressConfigLocalHost* group) to **enable**.
The primary DNS and secondary DNS addresses are set with the static values defined in the *localHostStaticPrimaryDns* and *localHostStaticSecondaryDns* variables.
If you set the variable to **disable**, the primary DNS and secondary DNS addresses provisioning depends on the setting of the *telephonyDnsOverrideEnable* variable.
2. In the *ipAddressConfig* folder, set the *telephonyDnsOverrideEnable* variable (under the *ipAddressConfigTelephonyDns* group) to **enable**.
The primary DNS and secondary DNS addresses are set with the static values you define in the next step.
3. Set the *telephonyDnsStaticPrimaryDns* and *telephonyDnsStaticSecondaryDns* variables with the proper static DNS IP addresses of your ITSP.
If you set the *telephonyDnsOverrideEnable* variable to **disable**, the primary DNS and secondary DNS addresses provisioning depends on the setting of the *localHostDnsOverrideEnable* variable.
4. Restart the Mediatrix 4102 so that the changes may take effect.

Image

The *ipAddressConfigImage* group provides the configuration necessary to download applications into the Mediatrix 4102. This includes emergency downloads in case of repetitive failure to start the main application.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Software and Emergency Download*.

► **To select the Image configuration source:**

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable (under the *ipAddressConfigImage* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 42: Image Information Source

Variable	Default Static Value	DHCP Source
imagePrimaryHost	"192.168.0.10"	Use option specified in variable <i>imageDhcpPrimarySiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 117, bytes 0-3.
imagePrimaryPort	69 ^a	Use option specified in variable <i>imageDhcpPrimarySiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 117, bytes 4-5. If bytes 4-5 are not present, use the default static value.

Table 42: Image Information Source (Continued)

Variable	Default Static Value	DHCP Source
imageSecondaryHost	"192.168.0.10"	Use option specified in variable <i>imageDhcpSecondarySiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 118, bytes 0-3.
imageSecondaryPort	69 ^a	Use option specified in variable <i>imageDhcpSecondarySiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 118, bytes 4-5. If bytes 4-5 are not present, use the default static value.

a. This is the well-known TFTP port number as per RFC 1340.

- Restart the Mediatrix 4102 so that the changes may take effect.

Management Server

The *ipAddressConfigMs* group provides the configuration necessary for contacting a SNMP management server such as the Media5 Unit Manager Network.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Unit Manager Server*.

► To select the Management Server configuration source:

- In the *ipAddressConfig* folder, locate the *msSelectConfigSource* variable (under the *ipAddressConfigMs* group).
- Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 43: Management Server Source

Variable	Default Static Value	DHCP Source
msHost	N/A	Use option specified in variable <i>msDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 200, bytes 0-3.
msStaticHost	"192.168.0.10"	N/A
msTrapPort	N/A	Use option specified in variable <i>msDhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 200, bytes 4-5. If bytes 4-5 are not present, use the default static value.
msStaticPort	162	N/A
msStaticTrapPort	162	N/A



Note: If you change the value of the *msStaticTrapPort* variable, change the port used in the management server. Not doing so will prevent you from viewing the received traps from the unit.

- Restart the Mediatrix 4102 so that the changes may take effect.

Configuration File Fetching

The *ipAddressConfigFileFetching* group provides the configuration necessary to contact the configuration file server when fetching a configuration file.

► **To select the configuration file fetching server configuration source:**

1. In the *ipAddressConfig* folder, locate the *configFileFetchingSelectConfigSource* variable (under the *ipAddressConfigFileFetching* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 44: Configuration File Fetching Source

Variable	Default Static Value	DHCP Source
configFileFetching Host	N/A	Use option specified in variable <i>configFileFetchingDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 201, bytes 0-3.
configFileFetching Port	N/A	Use option specified in variable <i>configFileFetchingDhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 201, bytes 4-5. If bytes 4-5 are not present, use the default static value.
configFileFetching StaticHost	"192.168.0.10"	N/A
configFileFetching Static Port	69	N/A

3. Restart the Mediatrix 4102 so that the changes may take effect.

Syslog

The *ipAddressConfigSyslog* group provides the configuration necessary for contacting a Syslog server.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Syslog Daemon*.

► **To select the Syslog configuration source:**

1. In the *ipAddressConfig* folder, locate the *syslogSelectConfigSource* variable (under the *ipAddressConfigSyslog* group).
2. Set this variable to either **static** or **dhcp**.

Table 45: Syslog Source

Variable	Default Static Value	DHCP Source
syslogHost	"192.168.0.10"	Use option specified in variable <i>syslogDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 110, bytes 0-3.
syslogPort	514 ^a	Not provided by the DHCP, use the default static value.

a. The port number is as per RFC 1340.

3. Restart the Mediatrix 4102 so that the changes may take effect.

MGCP Call Agent

The *ipAddressConfigMgcpCallAgent* group provides the configuration necessary for contacting a MGCP call agent.

► **To select the MGCP Call Agent configuration source:**

1. In the *ipAddressConfig* folder, locate the *mgcpCSelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 46: MGCP Call Agent Source

Variable	Default Static Value	DHCP Source
mgcpCAHost	"192.168.0.10"	Use option specified in variable <i>mgcpCADhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 207, bytes 0-3.
mgcpCAPort	2727	Use option specified in variable <i>mgcpCADhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 207, bytes 4-5. If bytes 4-5 are not present, use the default static value.

3. Restart the Mediatrix 4102 so that the changes may take effect.

NCS Call Agent

The *ipAddressConfigNcsCallAgent* group provides the configuration necessary for contacting a NCS call agent.

► **To select the NCS Call Agent configuration source:**

1. In the *ipAddressConfig* folder, locate the *ncsCSelectConfigSource* variable (under the *ipAddressConfigNcsCallAgent* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 47: NCS Call Agent Source

Variable	Default Static Value	DHCP Source
ncsCAHost	"192.168.0.10"	Use option specified in variable <i>ncsCADhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 210, bytes 0-3.
ncsCAPort	2727	Use option specified in variable <i>ncsCADhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 210, bytes 4-5. If bytes 4-5 are not present, use the default static value.

3. Restart the Mediatrix 4102 so that the changes may take effect.

SNTP

The *ipAddressConfigSntp* group provides the configuration necessary for contacting a NTP/SNTP server. If you are using a NTP or SNTP server (see [“Chapter 16 - SNTP Settings” on page 189](#) for more details), the DHCP server already has options that can be set to provide time server addresses, and the order in which clients use them to attempt to discover servers.

The Mediatrix 4102 uses *Option 42* to specify the IP address corresponding to the server that provides NTP/SNTP (RFC 1769).



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *SNTP*.

► **To select the SNTP configuration source:**

1. In the *ipAddressConfig* folder, locate the *sntpSelectConfigSource* variable (under the *ipAddressConfigSntp* group).
2. Set this variable to either **static** or **dhcp**.

Table 48: SNTP Source

Variable	Default Static Value	DHCP Source
sntpHost	"192.168.0.10"	Option 42 (first of the list).
sntpPort	123	Not provided by the DHCP, use the default static value.

LAN Connector Static IP Address

You can use the *LAN* connector of the Mediatrix 4102 with the network card of a computer. You could then use this computer to directly access the unit via its LAN interface.

This section describes how to set the static IP address of the *LAN* connector and use this LAN static IP address according to the VLAN substitution or always enabled configuration.

See also [“LAN and WAN with VLAN substitution” on page 199](#) for information on the *LAN* connector behaviour when forwarding network traffic between the WAN and the LAN interfaces of the Mediatrix 4102.

► **To set the LAN connector static IP address:**

1. In the *ipRoutingMIB*, set the *lanStaticAddressActivation* variable to one of the following values:

Table 49: LAN Connector Static IP Address

Parameter	Description
ipRouting	To set the <i>lanStaticAddress</i> variable as the Local Area Network (LAN) IP address used by the Mediatrix 4102's <i>LAN</i> interface, set the variable <i>ipRoutingEnable</i> to enable as described in “Enabling TAS” on page 122 .
vlanSubstitution	To set the <i>lanStaticAddress</i> as the Local Area Network (LAN) IP address used by the Mediatrix 4102's <i>LAN</i> interface, set the variable <i>qosVlanleee8021qSubstitutionEnable</i> to enable . Also set the VLAN Substitution feature as described in “VLAN Substitution” on page 198 . See also “LAN and WAN with VLAN substitution” on page 199 for information on the <i>LAN</i> connector behaviour when forwarding network traffic between the WAN and the LAN interfaces of the Mediatrix 4102.
always	Sets the <i>lanStaticAddress</i> as the Local Area Network (LAN) IP address used by the Mediatrix 4102's <i>LAN</i> interface.

2. In the *ipAddressConfig* folder, set the static LAN connector information as follows:

Table 50: LAN Interface Source

Variable	Default Static Value	Description
lanStaticAddress	192.168.10.1	LAN IP address used by the unit's LAN interface.
lanStaticNetworkMask	255.255.255.0	LAN subnet mask used by the unit's LAN interface.



Note: Do not set the *lanStaticAddress* variable to 0.0.0.0. This could prevent the unit from properly sending a DHCP discover request.



Note: Media5 recommends not to set the *lanStaticNetworkMask* variable to 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host addresses. Since a subnet must have a network (all bits 0) and a broadcast address (all bits 1), this leaves no room for hosts.

3. Restart the Mediatrix 4102 so that the changes may take effect.

DHCP Server Configuration

Standards Supported

- RFC 2131 – Dynamic Host Configuration Protocol, section 2
- RFC 2132 – DHCP Options and BOOTP Vendor Extensions



Note: This section applies only if you are using the DHCP connection type.

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 4102 unique identifier is its media access control (MAC) address.



Note: Media5 recommends to use a Windows 2000- or Unix-based DHCP server. If you run Windows NT 4.0 and use the built-in Microsoft DHCP Server, use the Site Specific instead of Vendor Specific information.

You can locate the MAC address as follows:

- ▶ on the label located on the bottom side of the unit.
- ▶ in the *sysMgmtMIB* under the *sysMacAddress* variable.

Media5 recommends to reserve an IP address with an infinite lease for each Mediatrix 4102 on the network.

Connection to the DHCP Behaviour

When the Mediatrix 4102 restarts, it requests a DHCP offer to get its IP addresses and network information. The Mediatrix 4102 waits four seconds before sending another request. The delay between each request is increased exponentially after each request up to a maximum delay of 64 seconds, and then restarts at a 4 seconds delay.

- ▶ first request: 4 seconds delay
- ▶ second request: 8 seconds delay
- ▶ third request: 16 seconds delay
- ▶ fourth request: 32 seconds delay
- ▶ fifth request: 64 seconds delay
- ▶ sixth request: 4 seconds delay
- ▶ seventh request: 8 seconds delay

► etc.

The Mediatrix 4102 stops broadcasting as soon as it receives at least one reply. If the offer is valid, the Mediatrix 4102 takes it and continues its initialization procedure.



Note: If the *localHostSelectConfigSource* variable is set to **static** and any other *xxSelectConfigSource* variable is set to **dhcp**, the Mediatrix 4102 makes its DHCP request that will be released immediately.

Network Configuration

[Table 51](#) lists some of the network options to configure in the DHCP server:

Table 51: Network Configuration

Information	Description	Option	Data Format	Example
Subnet Mask	Specifies subnet configuration	001	xxx.xxx.xxx.xxx	255.255.255.0
Routers	List of routers on your network	003	Array of IP Addresses	192.168.10.1 192.168.10.2
DNS Servers	List of DNS servers on your network	006	Array of IP Addresses	192.168.10.11 192.168.10.12

Vendor and Site Specific DHCP Options



Note: This section applies only if you are using the DHCP connection type.

This section briefly describes vendor and site specific DHCP options.

Most of the MIB variables described in [“Services” on page 56](#) require that you define their IP address and, if required, port number. When defining these variables, you can do so in two ways: via vendor specific options or site specific options.

The default value is to use the vendor specific codes. In this case, the *xxSiteSpecificCode* MIB variables are set to 0.

If you want to use site specific codes instead, change the value of the *xxSiteSpecificCode* MIB variables from the default value (0) to the value you select in the DHCP server. See [“Site specific code definition” on page 71](#) for an example of vendor specific and site specific settings.

Vendor Specific Options

Standards Supported

RFC 2132 – DHCP Options and BOOTP Vendor Extensions, section 8.4 (“Vendor-specific options”)

The vendor specific DHCP option is a standard DHCP option used to store information specific to the vendor of the DHCP client. The vendor specific option code is 43. Because there are different information elements that can be stored in this option, each element has been allocated a “sub-option” number. See [Table 52 on page 69](#) for the complete list.

Like all other options, the vendor specific information field (option 43) first contains a code (43), a length (in byte) and some data that spans the number of bytes specified in the length.

The data is organized as a series of sub-options, each of them laid-out like a regular option (code, length, data). The codes can be anything between 1 and 254, and the vendor, Media5, chooses these codes. See [Table 52 on page 69](#) for actual codes.

The following figures show the general and encapsulated layout of the vendor specific information option.

Figure 21: General Layout of a Vendor Specific Information Option

43	Len	Data	Data	Data	Data	...
----	-----	------	------	------	------	-----

Figure 22: Layout for Encapsulated Vendor Specific Options

43	Len	Code1	Len1	Data1	Data1	...	Code2	Len2	Data2	Data2	...
----	-----	-------	------	-------	-------	-----	-------	------	-------	-------	-----

[Figure 23](#) is an example of a vendor specific option containing an *msHost* IP address (192.168.1.2).

Figure 23: Example of Encapsulated Vendor Specific Option

43	6	200	4	192	168	1	2
----	---	-----	---	-----	-----	---	---

Mediatrrix units store two types of information in vendor specific options: IP addresses with optional port number and FQDNs with optional port number. The layout for storing IP addresses is explained in section [“Entering IP Addresses” on page 69](#). The layout for storing FQDNs is explained in section [“Entering FQDNs” on page 70](#).

Vendor Class ID

When using the vendor specific option, first define a Vendor Class ID for the Mediatrrix 4102 (not supported in Windows NT servers). A Vendor Class ID can be used by DHCP clients to identify their vendor type and configuration. When using this option, vendors can define their own specific identifier values to convey a particular hardware or operating system configuration or other identifying information.

Where vendor classes are used, the DHCP server responds to identifying clients by using option code 43, the reserved option type for returning vendor specific information to the client.

DHCP servers that do not interpret this option type are expected to ignore it when it is specified by clients.

Please refer to your DHCP server's documentation to learn how to create a new vendor class.



Note: The class to add is *Mediatrrix 4102*.

Creating Vendor Specific Information

Once the Vendor ID Class is created, place the proper values in the 43 option of the DHCP server. The 43 option contains sub-options that are encapsulated (according to the format described in RFC 2132).

If the option is not in the DHCP server, the Mediatrrix 4102 uses an invalid value (0.0.0.0:0).

Please refer to your DHCP server's documentation to learn how to create vendor specific information. See [“Entering IP Addresses” on page 69](#) for more details on the syntax to use.

Site Specific Options

Standards Supported

RFC 2132 – DHCP Options and BOOTP Vendor Extensions, section 2 (“BOOTP Extension/DHCP Option Field Format”).

Site specific options are non-standard DHCP options specific to the network where the Mediatrrix 4102 is used. You are responsible to allocate an option number (between 128 and 254) for each information element to be stored.

Mediatrrix units store two types of information in site specific options: IP addresses with optional port number and FQDNs with optional port number. The layout for storing IP addresses is explained in section [“Entering IP Addresses” on page 69](#). The layout for storing FQDNs is explained in section [“Entering FQDNs” on page 70](#).

[Figure 24](#) is an example of site specific option #146, containing address 192.168.0.1.

Figure 24: Site Specific Option Example

146	4	192	168	0	1
-----	---	-----	-----	---	---

When using the site specific option, you can place the values in the site specific options of your choice in the DHCP server. You must then enter the values in the proper MIB variables.

Please refer to your DHCP server's documentation to learn how to create site specific information. See ["Entering IP Addresses" on page 69](#) for more details on the syntax to use.

Option Codes

This table lists all vendor specific sub-option codes.

Table 52: Sub-Option Codes

Code		Description
Decimal	Hexadec.	
110	0x6E	Syslog Server address and port.
117	0x75	Image Primary Server host address and port. The default port number is 69 if you are using TFTP as protocol. The default port number is 80 if you are using HTTP as protocol.
118	0x76	Image Secondary Server host address and port. The default port number is 69 if you are using TFTP as protocol. The default port number is 80 if you are using HTTP as protocol.
200	0xC8	Management Server SNMP Trap host address and port.
201	0xC9	Configuration file fetching host address and port. The default port number is 69 if you are using TFTP as protocol. The default port number is 80 if you are using HTTP as protocol.
207	0xCF	MGCP Call Agent host address and port.
210	0xD2	NCS Call Agent host address and port.

Entering IP Addresses

In the DHCP server, IP addresses can be entered in decimal, hexadecimal or octal format. See ["IP Addresses" on page 55](#) for more details.

There are two formats of address string:

- ▶ Long: Has a size of 6 bytes (12 hexadecimal characters) and includes the IP address and port.
- ▶ Short: Has a size of 4 bytes (8 hexadecimal characters) and includes only the IP address. In this case, the default port is used.

Numeric values are stored in network byte order (Big-Endian).

Table 53: Address String Formats

Variable	Valid Range	Typical Value	Note
IP Address	Any valid IP address	192.168.0.2 (hex. 0xC0.0xA8.0x0.0x2)	N/A
Port	1 - 32,768	162 (hex. 0xA2)	Not present in the format with dimension 4.

When entering IP addresses in the DHCP server, there is a difference between the vendor specific option and the site specific option.

The vendor specific options must be encapsulated because more than one information can be stored in this option:

```
[code][length][4-6 bytes address][another code][another length][another address]...
```

The site specific options can have only one information per option:
[4-6 bytes address]
The DHCP server adds the proper code and length in the packet it sends out.

Example

The following example shows how to enter the Syslog (code 110) IP address 192.168.0.10 (with the default port used) and the same address at port 2545 in hexadecimal format.

Figure 25: Example – Short Address String

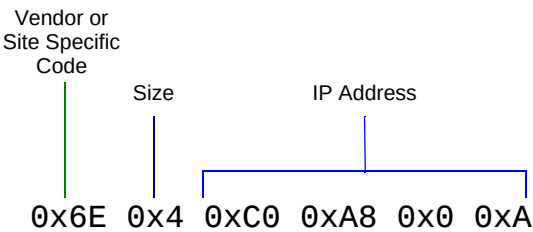
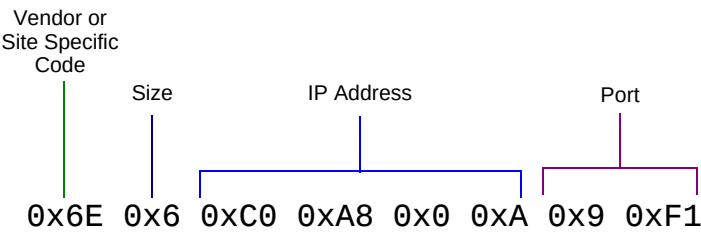


Figure 26: Example – Long Address String



Entering FQDNs

The FQDN address layout is a Media5 proprietary extension to the IP address layout. This format allows the configuration of an IP address in binary format (with or without port) or a FQDN in string format (with or without port) in the same option. The method to decode the information is based on the length of the option: a length of 4 or 6 is decoded as an IP address in binary format and a length higher than 6 is decoded as a FQDN in string format.

The IP address in binary format (with and without port) is explained in section [“Entering IP Addresses” on page 69](#).

The FQDN in string format consists of an array of characters representing the FQDN address.

Figure 27: FQDN String Format (without a port number)

Code	Len (7 to n)	FQDN char 1	FQDN char 1	...	FQDN char n
------	--------------	-------------	-------------	-----	-------------

You can specify a port by adding the port number in string format after a ':' at the end or the FQDN.

Figure 28: FQDN String Format (without a port number)

Code	Len (7 to n)	FQDN char 1	FQDN char 1	...	FQDN char n	":" (0x3A)	Port char 1	...	Port char y
------	--------------	-------------	-------------	-----	-------------	------------	-------------	-----	-------------

The space or null (ASCII code 0) character can be used as padding at the end of the string to have a length higher than 6, since all spaces and nulls are ignored. Note that an IP address can be defined in string format.

Examples

The following are some examples of the DHCP server configuration (based on linux dhcpd).

Vendor specific options – option vendor-encapsulated-options

- ▶ Syslog Server (IP address "192.168.0.1" in binary format).
6e:04:c0:a8:00:01:
- ▶ Primary Image Server (IP address and port "192.168.0.10:6000" in binary format).
75:06:c0:a8:00:01:17:70:
- ▶ Secondary Image Server (IP address "192.168.0.1" in string format).
76:0b:31:39:32:2e:31:36:38:2e:30:2e:31:
- ▶ Management Server (IP address and port "192.168.0.1:6000" in string format).
c8:10:31:39:32:2e:31:36:38:2e:30:2e:31:3a:36:30:30:30:
- ▶ Configuration File Fetching (FQDN "server.com").
c9:0a:73:65:72:76:65:72:2e:63:6f:6d:

Site specific options

- ▶ Syslog Server (IP address "192.168.0.1" in binary format). The IP-address or string format of dhcpd can be used.
option mx-syslog-ip 192.168.0.1;
Or "option mx-syslog-str c0:a8:00:01;"
- ▶ Primary Image Server (IP address and port "192.168.0.10:6000" in binary format).
option mx-primary-image-str c0:a8:00:01:17:70;
- ▶ Secondary Image Server (IP address "192.168.0.1" in string format).
option mx-secondary-image-str "192.168.0.1";
- ▶ Management Server (IP address and port "192.168.0.1:6000" in #string format).
option mx-ms-str "192.168.0.1:6000";
- ▶ Configuration File Fetching (FQDN "server.com").
option mx-filefetching-str "server.com";

Site specific code definition

```
option mx-syslog-ip code 129 = ip-address;
option mx-syslog-str code 129 = string;
option mx-primary-image-ip code 130 = ip-address;
option mx-primary-image-str code 130 = string;
option mx-secondary-image-ip code 131 = ip-address;
option mx-secondary-image-str code 131 = string;
option mx-ms-ip code 132 = ip-address;
option mx-ms-str code 132 = string;
option mx-filefetching-ip code 133 = ip-address;
option mx-filefetching-str code 133 = string;
```

Settings Example

Let's say for instance you want:

- ▶ the Image server at 10.3.2.154 (static)
- ▶ the Management Server via DHCP in the vendor specific options
- ▶ the Syslog server via DHCP in the site specific option #250

The following are the corresponding MIB values:

- ▶ imageSelectConfigSource = static
- ▶ imageStaticPrimaryHost = 10.3.2.154
- ▶ msSelectConfigSource = dhcp
- ▶ msDhcpSiteSpecificCode = 0
- ▶ syslogSelectConfigSource = dhcp
- ▶ syslogDhcpSiteSpecificCode = 250

The following is the corresponding DHCP setup, assuming the Management server is located at 10.3.2.201 and the Syslog server is located at 10.3.2.200 (port 1024):

- ▶ Option 43 (vendor specific option) contains the hexadecimal sequence 0xC80x40xA0x30x20xC9 **inserted among other sequences**.

Table 54: Hexadecimal Sequence - Option 43

Hexadecimal Part	Corresponding Information
0xC8	code 200 (management server)
0x4	size of 4 bytes
0xA0x30x20xC9	IP address 10.3.2.201

- ▶ Option 250 (site specific option) contains the hexadecimal sequence 0xA0x30x20xC80x400.

Table 55: Hexadecimal Sequence - Option 250

Hexadecimal Part	Corresponding Information
0xA0x30x20xC8	IP address 10.3.2.200
0x400	port 1024

Error Handling

In the event of a network or server failure, this section describes the application behaviour and/or replacement values to use.

Table 56: Replacement Values for Error Recovery

Type	Variable	Replacement value
IP address	(All variables of that type)	0.0.0.0
String	(All variables of that type)	""

DHCP Server Failures

If the Mediatrix 4102 cannot contact the DHCP server, it performs one of the following actions:

1. Retries contacting the DHCP server until it answers. The Mediatrix 4102 does not restart.
2. Uses the replacement value from [Table 56](#) for all variables that depend on the DHCP.

This assumes that the Mediatrix 4102 is set to get its IP information via a DHCP server.

Vendor/Site Specific Option Missing

If a vendor specific or site specific option is missing from the DHCP server answer, the Mediatrix 4102 uses the replacement value from [Table 56](#) for each variable that depends on missing vendor/site specific options.

DNS Failures

If the DNS cannot be contacted, the Mediatrix 4102 performs the following steps:

1. The Mediatrix 4102 sends a first request to the primary DNS server.

2. If the DNS server cannot be contacted within two seconds, the Mediatrix 4102 sends a request to the secondary DNS server.
3. If the secondary DNS server cannot be contacted, the Mediatrix 4102 uses the replacement value from [Table 56](#) for all variables that depend on the DNS.

Ethernet Connection Speed

You can set the speed of the Ethernet connection of the Mediatrix 4102.

You can also set these parameters via the web interface, as described in [“Ethernet Connection Speed” on page 58](#).

► To set the Ethernet connection speed:

1. In the *sysConfigMIB*, set the Ethernet connection speed of the:
 - WAN connector in the *sysConfigNetworkEthernetSpeed* variable
 - LAN connector in the *sysConfigComputerEthernetSpeed* variable.

The following values are available:

- Auto detect
- 10Mbs-HalfDuplex
- 100Mbs-HalfDuplex
- 10Mbs-FullDuplex
- 100Mbs-FullDuplex

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 detect** so that the Mediatrix 4102 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 73](#) for more details.

2. Restart the Mediatrix 4102 so that the changes may take effect.

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 4102 has the possibility to force the desired Ethernet link speed and duplex mode by disabling the auto-negotiation and selecting the proper setting (*sysConfigNetworkEthernetSpeed* or *sysConfigComputerEthernetSpeed* variable). 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.

MGCP Protocol Features

This chapter describes how to set information exclusive to the Media Gateway Control Protocol (MGCP). It assumes that the Mediatrix 4102 unit currently runs the MGCP protocol or that you will switch the unit to this protocol.

The MGCP signalling programs and information are defined in a MGCP stack. This includes Call Agent information and addresses, media package settings, etc.

Introduction

When the Mediatrix 4102 runs the MGCP protocol, it uses the *mgcpMIB*. This MIB is located in the Media5 MIB architecture.

► **To use the MGCP MIB:**

1. In the *telephonyMIB*, locate the *telephonyIpSignalingProtocolSelection* variable.
This variable allows you to switch from one protocol to another.
2. Set the *telephonyIpSignalingProtocolSelection* variable to **mgcp**.
3. Restart the Mediatrix 4102.
After the unit restarts, it uses the selected protocol.

MGCP Information

The Mediatrix 4102 uses IETF RFC 3435 - Media Gateway Control Protocol (MGCP) Version 1.0. F. Andreassen, B. Foster. January 2003. MGCP is a protocol for controlling Voice over IP (VoIP) Gateways from intelligent external call control elements. MGCP uses the Master/Slave concept, where external call control elements are the Masters, while the devices connected to them (such as the Mediatrix 4102), are the Slaves and only obey orders given by the Master.

The Mediatrix 4102 is used with any MGCP Call Agent (also known as Connection Manager), which manages calls from and to the Mediatrix 4102.

Services Provided

The Mediatrix 4102 uses the services provided by the Call Agent. See your Call Agent documentation for more information.

Call Agent Information

The Call Agent is the server that sends the proper information to the Mediatrix 4102 unit and manages calls from and to the unit.



Note: You can set the domain name of the gateway that manages the endpoints in the *localHostFqdnSelectConfigSource* variable. If the FQDN is not present or is blank, the FQDN is blank. See [“FQDN Configuration Source” on page 59](#) for more details.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *MGCP Configuration Window*.

Configuration Source

The Mediatrix 4102 must know the IP address or FQDN and port number of the Call Agent. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *mgcpCSelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).
This variable defines whether the Mediatrix 4102 must ask for its Call Agent settings through a DHCP server or not.
2. Set the *mgcpCSelectConfigSource* variable to **dhcp**.
You can query the Call Agent's IP address and port number assigned by the DHCP server in the following variables (under the *ipAddressStatusMgcpCallAgent* group of the *ipAddressStatus* folder):
 - *mgcpCAHost*
 - *mgcpCAPort*
3. Set how you want to define the MGCP Call Agent information in the DHCP server.

Table 57: MGCP Call Agent DHCP Information

To use a...	Set...
vendor specific code	The <i>mgcpCADhcpSiteSpecificCode</i> variable to 0 . Set the MGCP call agent IP address in the DHCP server inside the vendor specific sub-option 207 (hexadecimal 0xCF).
site specific code	The <i>mgcpCADhcpSiteSpecificCode</i> variable to any value between 128 and 254. Set the MGCP call agent IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>mgcpCADhcpSiteSpecificCode</i> variable in the unit's configuration).

See [“Vendor and Site Specific DHCP Options” on page 67](#) for more details.

4. Restart the Mediatrix 4102 so that the changes may take effect.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *mgcpCSelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).
This variable defines whether the Mediatrix 4102 must ask for its Call Agent settings through a DHCP server or not.
2. Set the *mgcpCSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 58: MGCP Call Agent Static Address

Variable	Description
mgcpCStaticHost	Static MGCP Call Agent IP address or domain name. Default Value: 192.168.0.10
mgcpCStaticPort	Static MGCP Call Agent IP port number. Default Value: 2727

4. Restart the Mediatrix 4102 so that the changes may take effect.

Establishing a MGCP Session

The following is an example describing how to establish a MGCP session

Figure 29: Layout Example

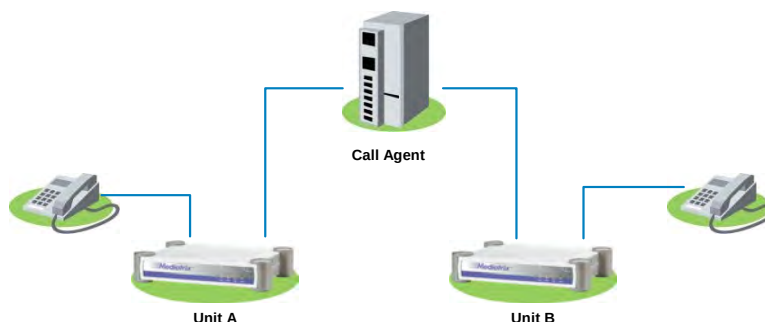
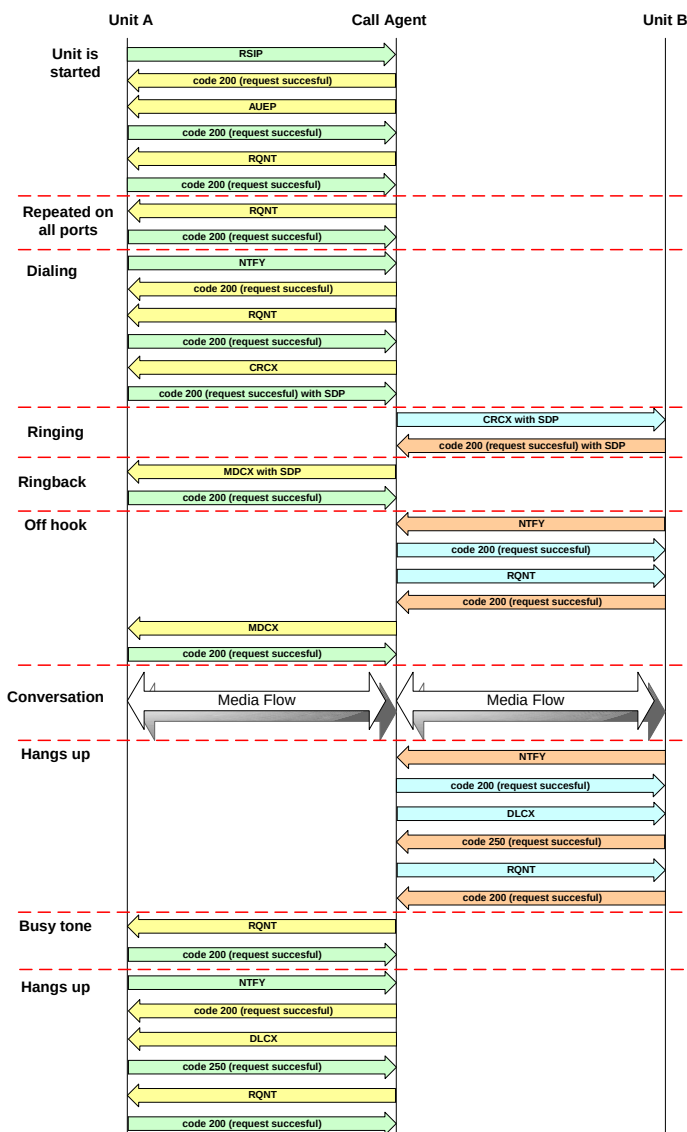


Figure 30: MGCP CALL Flow



MGCP Commands

The following commands are supported.

Table 59: MGCP Commands

Command	Description
Commands Sent by the Call Agent	
AUCX – Audit Connection	Can be used by the Call Agent to retrieve the parameters attached to a connection.
AUEP – Audit Endpoint	Can be used by the Call Agent to find out the status of a given endpoint.
CRCX – Create Connection	Used to create a connection between two endpoints.
MDCX – Modify Connection	Used to modify the characteristics of a gateway's "view" of a connection. This "view" of the call includes both the local connection descriptors as well as the remote connection descriptor.
DLCX – Delete Connection	Used to terminate a connection. As a side effect, it collects statistics on the execution of the connection.
RQNT – Request Notification	Used to request the gateway to send notifications upon the occurrence of specified events in an endpoint.
Commands Sent by the Gateway	
NTFY –Notify	Sent when the observed events occur.
RSIP – Restart In Progress - forced - disconnect	Notifies the Call Agent that the gateway, or a group of endpoints managed by the gateway, is being taken out of service or is being placed back in service.

MGCP Responses

All MGCP commands are acknowledged. The acknowledgment carries a return code, which indicates the status of the command. The return code is an integer number, for which four ranges of values have been defined:

- ▶ values between 200 and 299 indicate a successful completion
- ▶ values between 400 and 499 indicate a transient error
- ▶ values between 500 and 599 indicate a permanent error

Basic Information

You can set general MGCP information pertaining to the Mediatix 4102. This information is located in the *mgcpMIBObjects* group of the *mgcpMIB*.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *MGCP Configuration Window*.

► **To set basic MGCP information:**

1. Set the UDP port number on which the Mediatix 4102 is listening for any MGCP request in the *mgcpPort* variable.
The default value is **2427**.
2. Set the default digit map for all the endpoints in the *mgcpDefaultDigitMap* variable.
This digit map is used if no digit map is sent by the Call Agent. The default value is **x.T**.
3. Define the level of restart for initial RSIP (Restart in Progress) in the *mgcpRestartLevel* variable.
The RSIP command is used by the gateway to signal that an endpoint, or a group of endpoints, is put in-service or out-of-service.

Table 60: RSIP Level

Level	Example
gateway(0)	RSIP 45531023 *@[192.168.13.60]
group(1)	RSIP 45531023 aaln/*@[192.168.13.60] RSIP 45531023 aalg/*@[192.168.13.60]
endpoint(2)	RSIP 45531023 aaln/1@[192.168.13.60] RSIP 45531023 aaln/2@[192.168.13.60] RSIP 45531023 aalg/3@[192.168.13.60] RSIP 45531023 aalg/4@[192.168.13.60]

The default value is **gateway**.

4. Indicate if the EndpointIdList returned by a wildcarded AUEP (audited endpoint) will include or not endpoints that are not started in the *mgcpEndpointIdListIncludeNotStarted* variable.
The following values are available:
 - excludeNotStarted(0)
 - includeNotStarted(1)
 The default value is **excludeNotStarted**.
5. Indicate if piggy-backing can be used to send several MGCP messages in the same UDP packet in the *mgcpPiggyBackingEnable* variable.
The following values are available:
 - disable(0)
 - enable(1)
 The default value is **enable**.
6. Specify if the ptime is included in the SDP packets in the *mgcpAddPtimeIfPresentInLCO* variable.
The following values are available:
 - excludePtime(0)
 - includePtime(1)

If you select *includePtime*, the ptime is included in the SDP packets whenever the ptime is provided in the *LocalConnectionOptions(LCO)* parameters. Otherwise the ptime is never provided in SDP. The ptime indicates the desired packetization interval that the offerer would like to receive.

The default value is **excludePtime**.

7. Restart the Mediatrix 4102 so that the changes may take effect.

Endpoints

Endpoints are originating or terminating devices such as telephones or faxes. This table contains the local endpoint name. The endpoint name is created as follows: *term2/term1@localHostFqdn*.

These endpoint names are case insensitive. They can be made up of letters, digits or other printable characters, with the exception of "/", "@", "*", "\$" and white space.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *MGCP Configuration Window*.

► To set endpoints information:

1. In the *mgcpMIB*, locate the *mgcpEndpointIfTable* group.
This table contains the endpoint information to set.
2. Set the following variables:

Table 61: MGCP Endpoint Information

Variable	Description
mgcpEndpointIdTerm1	The rightmost term of the local endpoint name. E.g.: RSIP 725581549 aaln/3@[192.168.13.60]
mgcpEndpointIdTerm2	Second term from the right of the local endpoint name. E.g.: RSIP 725581549 aaln/3@[192.168.13.60] Default Value: aaln

3. Restart the Mediatrix 4102 so that the changes may take effect.

Retransmission Parameters

Retransmission is a method of error control in which hosts receiving messages acknowledge the receipt of correct messages and do not acknowledge the receipt of incorrect messages. The lack of acknowledgement indicates to the sending host that it should transmit the failed message again.

► **To set Retransmission information:**

1. In the *mgcpMIB*, locate the *mgcpRetransmission* group.
2. Set the Retransmission algorithm used in the *mgcpRetransmissionAlgorithm* variable.
The following values are available.

Table 62: Retransmission Algorithm Parameters

Parameter	Description
static(0)	The retransmission period stays the same. Ex.: Period of 500 ms. The following retransmissions will be at 500 ms, 1000 ms, 1500 ms, etc.
exponential(1)	The retransmission period is doubled at each period. Ex.: Initial period of 500 ms. The retransmissions will be at 500 ms, 1000 ms, 2000 ms, 4000 ms, etc.
exponentialWithJitter(2)	The retransmission period is exponentially calculated with a random weighting factor varying from 88% to 112% of the calculated period. Ex.: Initial period of 500 ms. $\text{Period} = (\text{Period} \times 2) * (\text{Random value (0 to 24)} + 88) / 100$ $\text{Period2} = (\text{Initial period} \times 2) * (\text{Random value (0 to 24)} + 88) / 100$ etc.

The default value is **exponentialWithJitter**.

3. Set the following variables:

Table 63: MGCP Retransmission Information

Variable	Description
mgcpRetransmissionInitialPeriod	Retransmission initial period in ms. Default Value: 200
mgcpRetransmissionMaxPeriod	Retransmission maximum period in ms. Must be greater than or equal to the retransmission initial period. Default Value: 30000
mgcpRetransmissionDisconnect Timeout	Time elapsed (in ms) at which an endpoint becomes disconnected. Default Value: 20000
mgcpRetransmissionSuspicion Threshold	Number of retransmissions at which an endpoint may actively query the name server to detect the possible change of the Call Agent's interfaces. Default Value: 7

Table 63: MGCP Retransmission Information (Continued)

Variable	Description
mgcpRetransmissionSuspicionThresholdDnsQuery	Indicates whether a DNS query is performed or not when the number of retransmissions is equal to the suspicion threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
mgcpRetransmissionDisconnectThreshold	Number of retransmissions at which an endpoint should contact the DNS one more time to see if any other interfaces have become available. When the number of retransmissions is greater than this value, the endpoint becomes disconnected. Default Value: 7
mgcpRetransmissionDisconnectThresholdDnsQuery	Indicates whether a DNS query is performed or not when the number of retransmissions is equal to the disconnect threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
mgcpRetransmissionHistoryTimeout	Number of milliseconds for which the responses to old transactions must be kept. Default Value: 20000
mgcpRetransmissionMaxWaitingDelay	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP (Restart in Progress). Default Value: 600000
mgcpRetransmissionDisconnectInitialWaitingPeriod	Initial waiting delay (in ms) an endpoint must wait before starting the disconnect procedure. Default Value: 15000
mgcpRetransmissionDisconnectMinWaitingPeriod	Minimum waiting delay (in ms) that must have elapsed since the gateway became initially disconnected, and before reinitiating the disconnect procedure. If the endpoint remains disconnected after the "disconnected" procedure, the minimum waiting delay is doubled up to a maximum value. Default Value: 15000
mgcpRetransmissionDisconnectMaxWaitingPeriod	Disconnected maximum waiting delay (in ms) since the gateway became disconnected that an endpoint can wait before starting the disconnect procedure. Default Value: 600000

4. Restart the Mediatrix 4102 so that the changes may take effect.

Packages

The *mgcpMIB* supports five packages:

- ▶ Generic Media Package
- ▶ DTMF Package
- ▶ Line Package
- ▶ Extended Analog Line (XL) Package
- ▶ X-P Package

Setting the Default Package

You can set the default MGCP package of the Mediatix 4102.

▶ **To select the default package:**

1. In the *mgcpMIB*, locate the *mgcpDefaultPackage* variable (in the *mgcpMIBObjects* group). This variable defines the default package to use for all the endpoints. You have the choice between:
 - Line Package
 - DTMF Package
 - Generic Media Package
 The default value is **Line Package**.
2. Restart the Mediatix 4102 so that the changes may take effect.

Dynamic Timeout Values

Although all the timeouts are provisioned in the MIB and currently set to the Basic MGCP Packages suggestions (as defined in the following sections), the gateway controller may want to alter the timeout value for some features. In this case, the timeout period (in milliseconds) is provided as a parameter to the signal (RFC 2705bis-00).

Generic Media Package

The Generic Media package groups the events and signals that can be observed on several types of endpoints, such as trunking gateways, access gateways or residential gateways.



Note: Currently, the Mediatix 4102 does not NACK the modem tone request, but the modem tone request is not yet supported.

▶ **To set Generic Media package information:**

1. In the *mgcpMIB*, locate the *mgcpGenericMediaPackage* group.
2. Set the ringback tone information.
The ringback tone (also referred to as ringing tone) advises the caller that a connection has been made and that a calling signal is being applied to the called party or service point. See ["Appendix D - Country-Specific Parameters" on page 239](#) for more details on country-specific ringback tones.

Table 64: MGCP Generic Media Package Information

Variable	Description
mgcpGenericMediaPackageRtDuration	Ringback tone timeout value in ms. Values range from 0 ms to 4294967295 ms. Default Value: 180000

Table 64: MGCP Generic Media Package Information (Continued)

Variable	Description
mgcpGenericMediaPackageRbkDuration	Ringback on connection tone timeout value in ms. Values range from 0 ms to 4294967295 ms. Default Value: 180000

- Restart the Mediatrix 4102 so that the changes may take effect.

DTMF Package

The DTMF package groups variables pertaining to the DTMFs.

► To set DTMF package information:

- In the *mgcpMIB*, locate the *mgcpDtmfPackage* group.
- Set the following variables:

Table 65: MGCP DTMF Package Information

Variable	Description
mgcpDtmfPackageLDuration	DTMF long duration timeout value in ms. Values range from 0 ms to 4294967295 ms. Default Value: 2000
mgcpDtmfPackageTCriticalDuration	Interdigit timeout value in ms when a timer is all that is required for the digit string to match a pattern in the digit map. Values range from 0 ms to 4294967295 ms. Default Value: 4000
mgcpDtmfPackageTPartialDuration	Interdigit timeout value in ms when at least one more digit is required for the digit string to match any of the patterns in the digit map. Values range from 0 ms to 4294967295 ms. Default Value: 16000

- Restart the Mediatrix 4102 so that the changes may take effect.

Line Package

The Line package groups variables that determine tone timeouts of the MGCP protocol Line Package.

► To set Line package information:

- In the *mgcpMIB*, locate the *mgcpLinePackage* group.
- Set the following variables:

Table 66: MGCP Line Package Information

Variable	Description
mgcpLinePackageBzDuration	Busy tone timeout value in ms. It indicates the line or equipment is in use, engaged or occupied. Values range from 0 ms to 4294967295 ms. Default Value: 30000

Table 66: MGCP Line Package Information (Continued)

Variable	Description
mgcpLinePackageDIDuration	Dial tone timeout value in ms. It indicates the line is ready to receive dialling. Values range from 0 ms to 4294967295 ms. Default Value: 16000
mgcpLinePackageMwiDuration	Message waiting indicator tone timeout value in ms. It indicates there is a message waiting somewhere for the owner of the telephone. Values range from 0 ms to 4294967295 ms. Default Value: 16000
mgcpLinePackageOtDuration	Off hook warning tone timeout value in ms. It indicates that the telephone is not hung up correctly. Values range from 0 ms to 4294967295 ms. Default Value: 65535000
mgcpLinePackageRgDuration	Ring tone timeout value in ms. It indicates the called line is ringing out. Values range from 0 ms to 4294967295 ms. Default Value: 180000
mgcpLinePackageRoDuration	Reorder tone (also called fast busy) timeout value in ms. It indicates that all switching paths are busy, all toll trunks are busy, there are equipment blockages, the caller dialled an unassigned code, or the digits dialled got messed up along the way. Values range from 0 ms to 4294967295 ms. Default Value: 30000
mgcpLinePackageSIDuration	Stutter dial tone timeout value in ms. It notifies the user that a voice mail message is available when the telephone does not or cannot have a message-waiting light. Values range from 0 ms to 4294967295 ms. Default Value: 16000
mgcpLinePackageWtDuration	Call waiting tone timeout value in ms. It indicates someone is trying to call. Values range from 0 ms to 4294967295 ms. Default Value: 30000
mgcpLinePackageOsiDuration	Network disconnect timeout value in ms. It indicates that the far-end party has disconnected. Values range from 0 ms to 4294967295 ms. Default Value: 900
mgcpLinePackageHdPersistent	Indicates whether the off-hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event is detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable

Table 66: MGCP Line Package Information (Continued)

Variable	Description
mgcpLinePackageHfPersistent	Indicates whether the flash hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event is detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable
mgcpLinePackageHuPersistent	Indicates whether the on hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event is detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable

3. Restart the Mediatix 4102 so that the changes may take effect.

Extended Analog Line (XL) Package

The XL package meets the needs of the Line Reversal feature. Line Reversal is used by the call agent on one or more endpoints (lines) of the Mediatix 4102.

What is Line Reversal?

Line reversal consists of reversing the polarity of the tip/ring leads (GND becomes -48V and -48V switches to GND). There are two ways in which line reversal is often used:

- ▶ Line reversal on seizure – This is used to prevent that a call originates from a line at the same time that a call terminates to the line. The line reversal signal is applied on seizure to the terminating/called party followed by ringing and maintained until the line is answered. Once reversal has been applied, the line cannot attempt a simultaneous origination.
- ▶ Line reversal on answer – In this case, line reversal is applied to the originating party to control electronic equipment such as coin phones or answering machines. The line reversal signal acts as a stimulus to the equipment to perform specific actions such as dropping coins or activating the answering machine.

A specific line reversal signal is needed for the call agent to have full control of the line polarity states. This enables the call agent to control both line reversal on answer and line reversal on seizure by using one MGCP signal. This approach maps well to the legacy method of setting/resetting a data flag to indicate line reversal state.

XL Package Settings

There are no settings related to the XL package in the Mediatix 4102 MIB structure.

Limitations to Using Line Reversal

Do not use the XL package in the following situations:

- ▶ When an endpoint of the Mediatix 4102 rings
- ▶ When an endpoint of the Mediatix 4102 uses caller ID
- ▶ When an endpoint of the Mediatix 4102 uses the caller ID on Call Waiting

If the XL package is used in these cases, the ring is cancelled.

X-P Package

The X-P package is a special package that deals with tones.

▶ To set X-P package information:

1. In the *mgcpMIB*, locate the *mgcpXPPackage* group.
2. Set the *mgcpXPPackageIrDuration* variable.
This variable defines the initial ring timeout value in ms.
3. Restart the Mediatix 4102 so that the changes may take effect.

The X-P package offers the following tone definitions:

Table 67: X-P Package Tones

Symbol	Definition	Duration
mp (pc=xx)	Meter pulse ^a and pulse counts	BR (Brief)
ir	Initial ring ^b	Timeout duration configurable
oc	Report on completion ^c	N/A
of	Report on failure	N/A
pt1	Project specific tone 1	Timeout infinite
pt2	Project specific tone 2	Timeout infinite
pt3	Project specific tone 3	Timeout infinite
pt4	Project specific tone 4	Timeout infinite
pt5	Project specific tone 5	Timeout infinite
pt6	Project specific tone 6	Timeout infinite
pt7	Project specific tone 7	Timeout infinite
pt8	Project specific tone 8	Timeout infinite
pt9	Project specific tone 9	Timeout infinite
pt10	Project specific tone 10	Timeout infinite

a. A meter pulse is sent from the media gateway controller to the Mediatix 4102 to indicate the charge display has to be incremented.

b. Initial ring is sent from the media gateway controller to the Mediatix 4102.

c. The event is triggered when the timeout signal completes successfully, e.g. initial ring.

Redirecting to a Different Call Agent

The Mediatix 4102 is provisioned with information for the initial registration sequence to a call agent – either by the unit's own provisioning tool or DHCP. However, the call agent may change the registration request during the registration sequence to another call agent.

Upon receipt of a message that specifies a change in the registration request, the Mediatix 4102 overwrites its provisioned value with the new value and begins sending messages to the new call agent until a new "NotifiedEntity" parameter is received OR until the Mediatix 4102 is reprovisioned due to a restart.

Meter Pulse

A meter pulse allows to calculate call charges by providing a series of charging "pulses" on a customer's line. Typically, all pulses cost the same. However, the farther you call, the quicker the pulses come. This enables customers to track the cost of their calls or to charge a call to a third party.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See ["MIB Structure" on page 47](#) for more details.

In the case of some private pay phones, the pulses enable customers to set the frequency at which the pay phone user must insert cash to pay for a call.

The meter pulse feature is sent at 2.5 volts. The actual number of pulses sent is call agent-driven.

► **To set the meter pulse feature:**

1. In the *fxsMeterPulseMIB*, locate the *fxsMeterPulseMIBObjects* group.
2. Set the meter pulse frequency in the *fxsMeterPulseFreq* variable.
The meter pulse may use one of the following frequencies:
 - *freq_12_kHz*(1)
 - *freq_16_kHz*(2)The selected frequency applies to **all** FXS lines.
3. Set the meter pulse duration in the *fxsMeterPulseDuration* variable.
This is the pulse duration (voltage is ON) in ms. The clock precision is 10 ms, i.e. you can request 213 ms, but the system will play each pulse 213 +/- 10 ms. Available values are from 120 ms to 220 ms.
Since this variable is located in a table, you can set its value on a per-line basis.
4. Set the meter pause duration in the *fxsMeterPauseDuration* variable.
This is the pause duration (voltage is OFF) in ms. The clock precision is 10 ms, i.e. you can request 327 ms, but the system will pause for 327 +/- 10 ms. Available values are from 100 ms to 600 ms.
Since this variable is located in a table, you can set its value on a per-line basis.
5. Restart the Mediatix 4102 so that the changes may take effect.

MGCP Conference Mode

This mode enables the mixing of two RTP streams on a given endpoint, resulting in a conference call. The conference is in the G.711, codec and it is initiated by a flash hook.

In conference mode, audio signals received in data packets through connections are replicated to all the other connections whose mode is "conference."

There are many possible ways to setup a conference. However, you must follow one simple rule: at any point in time, there must be a maximum of two connections on the same endpoint. Only one of these two connections can be active and the other one must be set to inactive.



Note: The PCMU or PCMA codec must be enabled to use the Conference mode. See [“Enabling Individual Codecs” on page 169](#) for more details.

The following is a call flow of a conference.

Figure 31: Conference Message Flow – Part 1

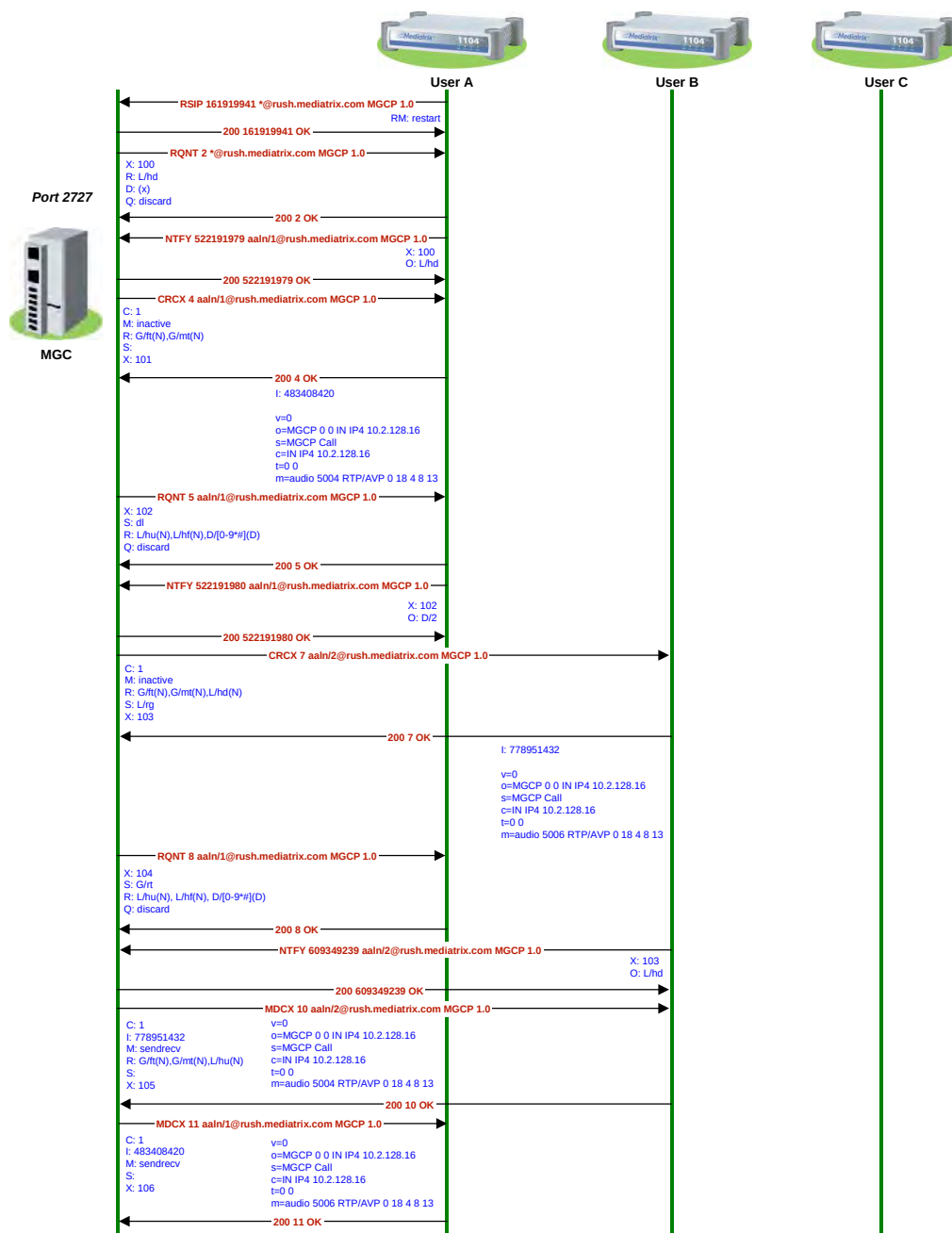


Figure 32: Conference Message Flow – Part 2

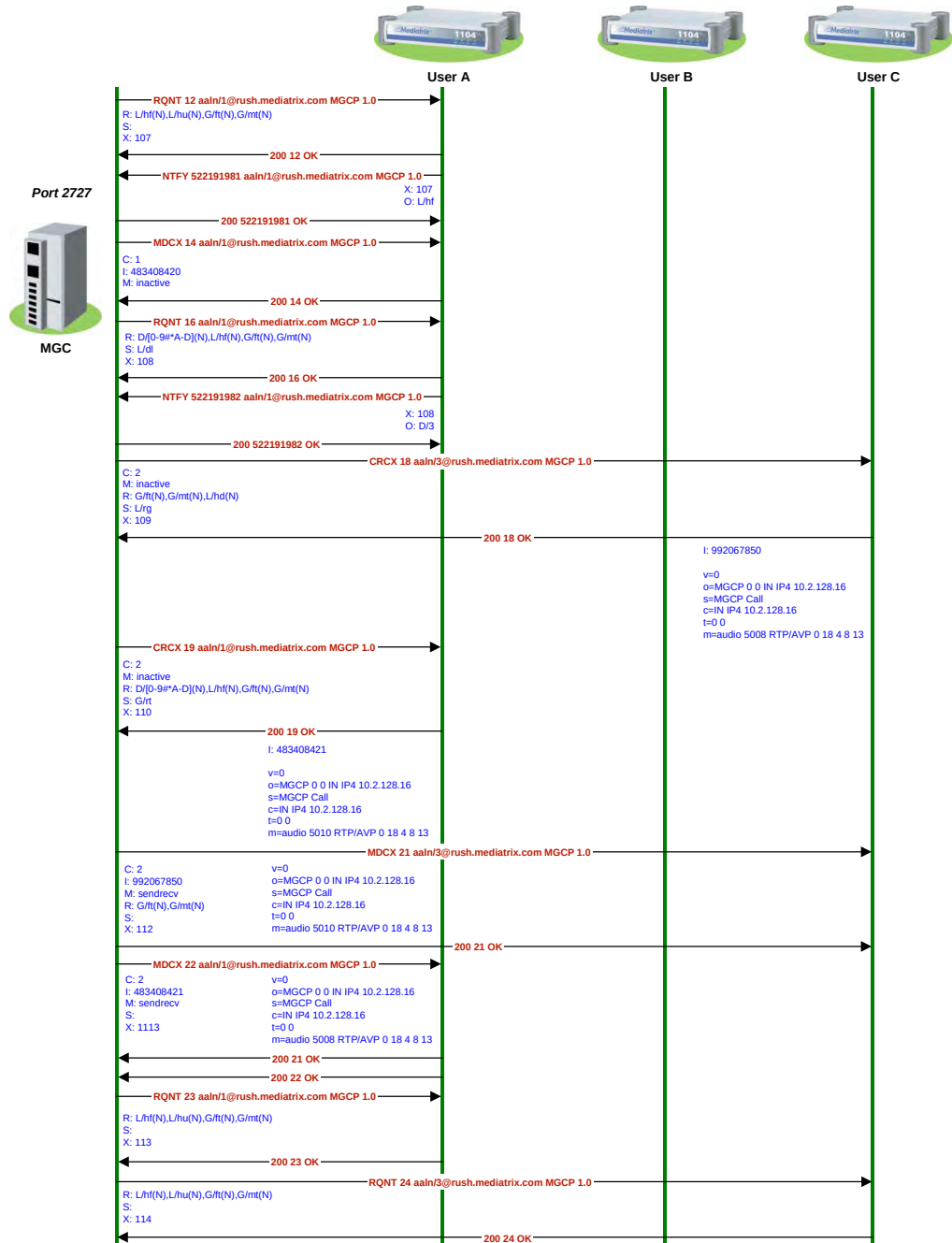
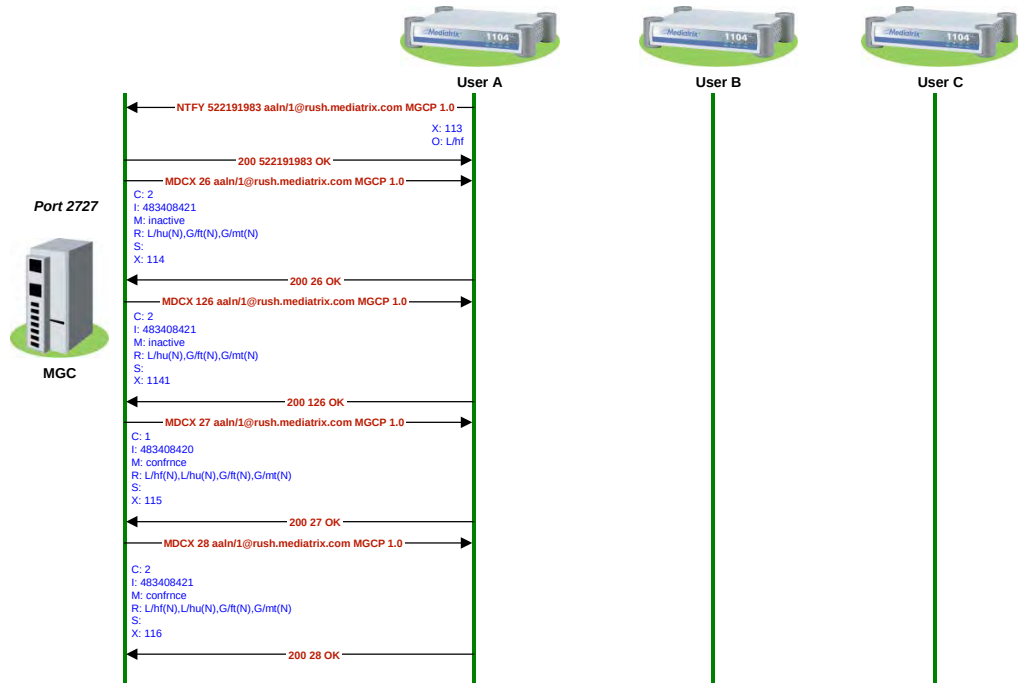


Figure 33: Conference Message Flow – Part 3



Firewall Traversal

The Mediatrax 4102 may be used in a private domain that is not directly connected to the IP network. For instance, this may be the case for ITSP (Internet Telephony Service Provider) clients that have a small private network. This private network is connected to the public IP network through a firewall.

When a Mediatrax 4102 controlled with the MGCP protocol is deployed behind a firewall, the Media Gateway Controller (MGC) should be allowed to control the unit. To keep the firewall connection alive, signalling packets must be exchanged between the Mediatrax 4102 and MGC within a specified period of time called the keep-alive timeout. If no packets are exchanged for the specified period, then the connection will be closed.

To keep the connection alive, the Mediatrax 4102 uses the RSIP *RM : x-keepalive* command to indicate that its inactivity timer has timed-out. The RSIP keep-alive command is sent at the gateway level.

The RSIP keep-alive command does not require any 200 OK from the MGC. It is launched immediately after the activation of the MGCP stack. It is then possible to see a RSIP keep-alive command preceding the initial RSIP restart if the registration initial delay period is larger than the inactivity timer. Furthermore, the RSIP keep-alive is not submitted to the disconnection procedure.

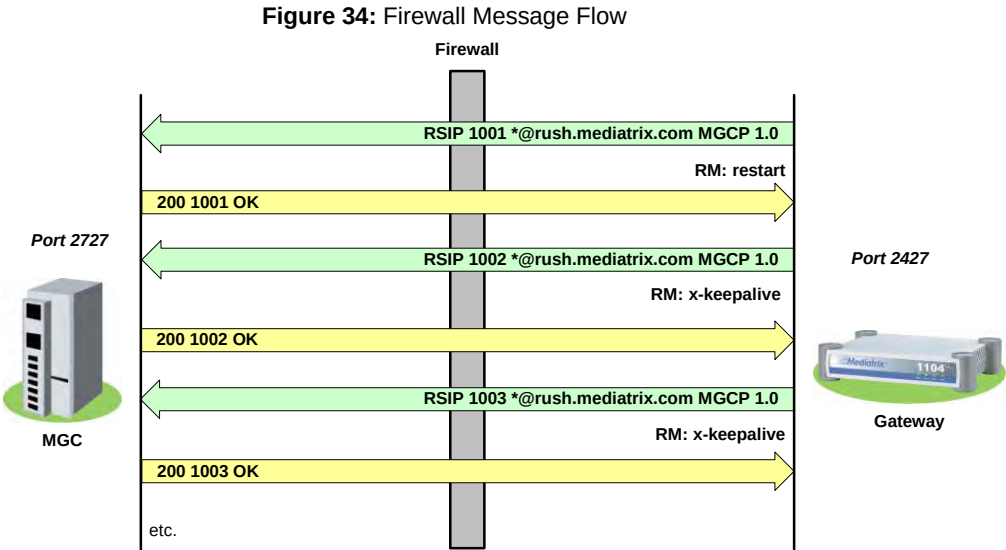
Note that voice packets cannot be used to keep the connection opened because they are transmitted on another channel.

► To enable the firewall keep-alive timeout mechanism:

1. In the *mgcpMIB*, define the keep-alive timeout value (in seconds) in the *mgcpFwKeepAliveTimeout* variable.
The default value is 300 seconds.
2. Set the *mgcpFwKeepAliveEnable* variable to **enable**.
This enables the firewall keep-alive timeout mechanism. The RSIP keep-alive is sent every time the timeout is reached.

The following illustrates the message flow when using the firewall keep-alive feature.

 **Note:** The RSIP RM: x-keepalive command does not require any 200 OK from the MGC. In this case, the 200 OK is optional.



Interoperability Configuration

The following sections describe a few interoperability parameters you can use to improve the way the Mediatrix 4102 interops with other products.

 **Note:** The following parameters also apply if the unit is running the NCS signalling protocol.

Offer/Answer Model

Standards Supported	• RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)
----------------------------	--

You can define whether the Mediatrix 4102 requires strict adherence to RFC 3264 from the peer when negotiating capabilities for the establishment of a media session.

- **To define how to process the Offer/Answer model:**
1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsValidateOfferAnswerModel* variable to the proper value.

The following values are available:

Table 68: Offer/Answer Model Parameters

Parameter	Description
disable	The peer can freely: - Send back a brand new list of codecs or add new ones to the offered list. - Add media lines AFTER the ones found in the offer. As long as at least one codec sent back is supported by the Mediatix 4102, the call is allowed to go on. Any media lines added by the peer is simply ignored.
enable	The following guidelines from the Offer-Answer Model must be strictly followed. An answer must: - Include at least one codec from the list that the Mediatix 4102 sent in the offer. - Avoid adding extra codecs that were not present 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.

Offered Stream Format

RFC 3264 stipulates that to reject an offered stream, the port number in the corresponding stream in the answer must be set to zero. However, some gateways prefer to remove the unwanted stream from the answer.

The answer to an offered session description is based on the offered session description.

► To define the stream format:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsAnswerStreamFormat* variable to the proper value.

Table 69: Offered Stream Format Parameters

Parameter	Description
zeroAnswerStream	The port number is set to zero if the corresponding stream in the answer is unwanted. This behaviour follows the RFC 3264 best practice. This is the default value.
removeAnswerStream	The unwanted stream is removed from the answer and returned to the offerer. This behaviour is kept for backward compatibility issue.

Session ID and Session Version

You can define the maximum length of the session ID and session version number in the origin line (o=) of the SDP.

► To define the session ID and session number:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsOriginLineSessionIDAndVersionMaxLength* variable to the proper value.

Table 70: Session ID/Version Parameters

Parameter	Description
none	The session ID and the session version number are represented by the 0 value. This is the default value.

Table 70: Session ID/Version Parameters (Continued)

Parameter	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.

Multiple Fax Tone Detection

You can control whether the Mediatrix 4102 reports more than one occurrence of the fax tone during the negotiation phase. This is used when event notification requests can be received after the fax tone.

► To enable multiple fax tone detection:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsMultipleFaxToneDetection* variable to **enable**. The Mediatrix 4102 will report every occurrence of the fax tone event.
If you set the variable to **disable**, when establishing a fax call, the Mediatrix 4102 only reports the first occurrence of the fax tone event.

Connected RTP Sockets

You can define whether the endpoints will listen to RTP sources other than the one with which they established a RTP session.

► To use connected RTP sockets:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsConnectRtpSockets* variable to **enable**. The endpoints will only play packets coming from the address established in the RTP session.
If you set the variable to **disable**, the Mediatrix 4102 uses unconnected sockets and the endpoints will play any RTP packets addressed to them.
2. Restart the Mediatrix 4102 so that the changes may take effect.

UDP Checksum

You can enable the UDP checksum in the RTP stack.

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

UDP checksumming is disabled by default to gain performance. In this case, the UDP checksum is not calculated. The value 0 is written in the *checksum* field of each RTP packet header.

► To enable UDP checksum:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsRtpUdpChecksumEnable* variable to **enable**. The UDP checksum is calculated for each RTP packet. Note that this may affect performance. The parameter takes effect on the next connection.

T.38 Capabilities Using Audio Codec 98

You can enable or disable the parsing of remote SDP in order to extract remote T.38 capabilities from an audio stream. This is useful when a call agent is re-using the audio stream to advertise the remote T.38 capabilities instead of creating a new image stream.

► **To enable T.38 capabilities using audio codec 98:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsT38CapabilitiesUsingAudioCodec98* variable to **enable**.

The Mediatrix 4102 verifies the remote SDP audio stream for the T.38 port number. The remote SDP must meet the following conditions in order to detect T.38 capabilities from the audio stream:

- Single audio stream
- Single media format 98
- No rtpmaps

If the variable is set to **disable**, the call agent never uses the audio stream to advertise the remote T.38 port number.

Immediate Modem Tone Reporting

You can control whether the early detection of a modem tone by the Mediatrix 4102 is immediately reported to the call agent (when requested) or delayed until the exact nature of the transmission has been determined. Some fax transmissions begin by exchanging modem tones in their setup stage; therefore, a little time is needed before the Mediatrix 4102 is able to discriminate between a fax or a modem transmission.

► **To enable immediate modem tone reporting:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsImmediateModemToneReporting* variable as required.

Table 71: Modem Tone Reporting Parameters

Parameter	Description
enable	The Mediatrix 4102 will report a modem tone to the call agent (assuming the call agent has requested it) as soon as it detects one.
disable	The Mediatrix 4102 will wait until it has determined the exact nature of a data transmission and then report either a fax or a modem tone to the call agent (always assuming the call agent has requested it).

Brief OSI Signal

For legacy reasons, you can change the behaviour of the Network Disconnect signal (L/osi) by changing its type from time-out to brief (see RFC 3435 for a description of the various signal types).

► **To make the OSI signal brief:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsMakeOsiSignalBrief* variable as required.

Table 72: Brief OSI Signal Parameters

Parameter	Description
enable	The L/osi signal will behave like a brief signal.
disable	The L/osi signal conforms to its standard definition and behaves like a time-out signal.

Fake RFC 3407 Recognition

You can allow the recognition of a remote endpoint's T.38 capabilities when they are advertised using the notation recommended in RFC 3407. More precisely, when enabled, the Mediatrix 4102 will recognize the line '**a=cdsc: 1 image udptl t38**' in the following SDP:

```
v=0
c=IN IP4 47.47.47.47
a=sqn: 0
a=cdsc: 1 image udptl t38
m=audio 1234 RTP/AVP 18
a=ptime:20
```

as valid T.38 support advertisement.



Note: No other part of the RFC is supported and the unit itself never uses this syntax.

► **To fake the RFC 3407 recognition:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsFakeRfc3407Recognition* variable as required.

Table 73: Modem Tone Reporting Parameters

Parameter	Description
enable	T.38 advertisement as described above is recognized
disable	RFC 3407 syntax is ignored.

T.38 Negotiation Syntax

Standards Supported

- ITU-T Recommendation T.38, section D.2.3

You can define the format used, in the SDP portion of SIP packets, to advertise the unit's T.38 capabilities.

► **To set the T.38 negotiation syntax to use:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsUseIuT38Format* variable with the proper behaviour.

Table 74: T.38 Negotiation Syntax Usage

Parameter	Description
disable	Support for the boolean T.38 parameters T38FaxFillBitRemoval, T38FaxTranscodingMMR, and T38FaxTranscodingJBIG is advertised by associating a value of 0 (unsupported) or 1 (supported) with the parameter in the following manner: a=T38FaxFillBitRemoval:0 a=T38FaxTranscodingMMR:0 a=T38FaxTranscodingJBIG:0 This is the default value.
enable	Support for the above T.38 parameters is advertised in conformance with ITU-T Recommendation T.38, section D.2.3. The presence of the parameter in the SDP indicates support for it (without the need for an associated value), while its absence means that it is not supported.

Brackets Around IP Address in Domain Name

When the configured domain name is an IP address, you can define whether or not to add brackets around the endpoint's domain name.

► **To add brackets around the IP address:**

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsBracketsAroundIpAddressInDomainNameEnable* variable with the proper behaviour.

Table 75: Brackets around the IP Address

Parameter	Description
disable	Brackets are not added around the IP address, e.g.: aaln/1@192.168.0.1.
enable	Brackets are added around the IP address, e.g.: aaln/1@[192.168.0.1]. This is the default value.

Polarity Reversal on Calling Card Service Tone

You can define whether or not a polarity reversal must be performed before playing the calling card service tone when receiving the S:L/z signal request.

► **To enable polarity reversal on calling car service tone:**

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsPolarityReversalOnCallingCardServiceToneEnable* variable with the proper behaviour.

Table 76: Polarity Reversal on Calling Card Service Tone

Parameter	Description
disable	Calling card service tone signal request is handled normally.
enable	A polarity reversal is performed before handling the calling card service tone signal request.

NCS Protocol Features

This chapter describes how to set information exclusive to the Network-based Call Signalling (NCS) protocol. It assumes that the Mediatrix 4102 unit currently runs the NCS protocol or that you will switch the unit to this protocol.

The NCS signalling programs and information are defined in a NCS stack. This includes Call Agent information and addresses, media package settings, etc.

Introduction

When the Mediatrix 4102 runs the NCS protocol, it uses the *ncsMIB*. This MIB is located in the Media5 MIB architecture.

► **To use the NCS MIB**

1. In the *telephonyMIB*, locate the *telephonyIpSignalingProtocolSelection* variable.
This variable allows you to switch from one protocol to another.
2. Set the *telephonyIpSignalingProtocolSelection* variable to **NCS**.
The default value is **MGCP**.
3. Restart the Mediatrix 4102.
After the unit restarts, it uses the selected protocol.

NCS Information

The Mediatrix 4102 uses the PacketCable™ network-based call signaling (NCS) protocol specification (March 12, 1999). NCS is a profile of the Media Gateway Control Protocol (MGCP). The Mediatrix 4102 is used with any NCS Call Agent (also known as Connection Manager), which manages calls from and to the Mediatrix 4102.

Services Provided

The Mediatrix 4102 uses the services provided by the Call Agent. See your Call Agent documentation for more information.

Call Agent Information

The Call Agent is the server that sends the proper information to the Mediatrix 4102 unit and manages calls from and to the unit.



Note: You can set the domain name of the gateway that manages the endpoints in the `localHostFqdnSelectConfigSource` variable. If the FQDN is not present or is blank, the IP address of the Mediatrix 4102 inserted within angle brackets is used instead. See [“FQDN Configuration Source” on page 59](#) for more details.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *NCS Configuration Window*.

Configuration Source

The Mediatrix 4102 must know the IP address and port number of the Call Agent. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the `ipAddressConfig` folder, locate the `ncsCAsSelectConfigSource` variable (under the `ipAddressConfigNcsCallAgent` group).
This variable defines whether the Mediatrix 4102 shall ask for its Call Agent settings through a DHCP server or not.
2. Set the `ncsCAsSelectConfigSource` variable to **dhcp**.
You can query the Call Agent's IP address and port number assigned by the DHCP server in the following variables (under the `ipAddressStatusNcsCallAgent` group of the `ipAddressStatus` folder):
 - `ncsCaHost`
 - `ncsCAPort`
3. Set how you want to define the NCS Call Agent information in the DHCP server:

Table 77: NCS Call Agent DHCP Information

To use a...	Set...
vendor specific code	The <code>ncsCADhcpSiteSpecificCode</code> variable (under the <code>ipAddressConfigNcsCADhcp</code> group) to 0 . Set the NCS call agent IP address in the DHCP server inside the vendor specific sub-option 210 (hexadecimal 0xD2).
site specific code	The <code>ncsCADhcpSiteSpecificCode</code> variable (under the <code>ipAddressConfigNcsCADhcp</code> group) to any value between 128 and 254. Set the NCS call agent IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <code>ncsCADhcpSiteSpecificCode</code> variable in the unit's configuration).

See [“Vendor and Site Specific DHCP Options” on page 67](#) for more details.

4. Restart the Mediatrix 4102 so that the changes may take effect.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► To use static information:

1. In the *ipAddressConfig* folder, locate the *ncsCSelectConfig Source* variable (under the *ipAddressConfigNcsCallAgent* group).
This variable defines whether the Mediatrix 4102 shall ask for its Call Agent settings through a DHCP server or not.
2. Set the *ncsCSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 78: NCS Call Agent Static Address

Variable	Description
ncsCAStaticHost	Static NCS Call Agent IP address or domain name. Default Value: 192.168.0.10
ncsCAStaticPort	Static NCS Call Agent IP port number. Default Value: 2727

4. Restart the Mediatrix 4102 so that the changes may take effect.

Basic Information

You can set general NCS information pertaining to the Mediatrix 4102. This information is located in the *ncsMIBObjects* group of the *ncsMIB*.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *NCS Configuration Window*.

► To set basic NCS information:

1. Set the UDP port number on which the Mediatrix 4102 is listening for any NCS request in the *ncsPort* variable.
The default value is **2427**.
2. Set the default digit map for all the endpoints in the *ncsDefaultDigitMap* variable.
This digit map is used if no digit map is sent by the Call Agent. The default value is **x.T**.
3. Define the level of restart for initial RSIP (Restart in Progress) in the *ncsRestartLevel* variable.
The RSIP command is used by the gateway to signal that an endpoint, or a group of endpoints, is put in-service or out-of-service.

Table 79: RSIP Level

Level	Example
gateway(0)	RSIP 45531023 *@[192.168.13.60]
group(1)	RSIP 45531023 aaln/*@[192.168.13.60] RSIP 45531023 aalg/*@[192.168.13.60]

Table 79: RSIP Level (Continued)

Level	Example
endpoint(2)	RSIP 45531023 aaln/1@[192.168.13.60] RSIP 45531023 aaln/2@[192.168.13.60] RSIP 45531023 aalg/3@[192.168.13.60] RSIP 45531023 aalg/4@[192.168.13.60]

The default value is **gateway**.

4. Indicate if the EndpointIdList returned by a wildcarded AUEP (audited endpoint) will include or not endpoints that are not started in the *ncsEndpointIdListIncludeNotStarted* variable.

The following values are available:

- excludeNotStarted(0)
- includeNotStarted(1)

The default value is **excludeNotStarted**.

5. Indicate if piggy-backing can be used to send several NCS messages in the same UDP packet in the *ncsPiggyBackingEnable* variable.

The following values are available:

- disable(0)
- enable(1)

The default value is **enable**.

6. Restart the Mediatrix 4102 so that the changes may take effect.

Endpoints

Endpoints are originating or terminating devices such as phones or faxes. This table contains the local endpoint name. The endpoint name is created as follows: *term2/term1@localHostFqdn*.



In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *NCS Configuration Window*.

► To set endpoints information:

1. In the *ncsMIB*, locate the *ncsEndpointIfTable* group.
This group contains the endpoint information to set.
2. Set the following variables:

Table 80: NCS Endpoint Information

Variable	Description
ncsEndpointIdTerm1	The rightmost term of the local endpoint name.
ncsEndpointIdTerm2	Second term from the right of the local endpoint name. Default Value: aaln

3. Restart the Mediatrix 4102 so that the changes may take effect.

Retransmission Parameters

Retransmission is a method of error control in which hosts receiving messages acknowledge the receipt of correct messages and do not acknowledge the receipt of incorrect messages. The lack of acknowledgement is an indication to the sending host that it should transmit the failed message again.

► **To set Retransmission information:**

1. In the *ncsMIB*, locate the *ncsRetransmission* group.
This group contains the retransmission information to set.
2. Set the following variables:

Table 81: NCS Retransmission Information

Variable	Description
ncsRetransmissionAlgorithm	Retransmission algorithm used. • static(0) The retransmission period stays the same. Ex.: Period of 500 ms. The following retransmissions will be at 500 ms, 1000 ms, 1500 ms, etc. • exponential(1) The retransmission period is doubled at each period. Ex.: Initial period of 500 ms. The retransmissions will be at 500 ms, 1000 ms, 2000 ms, 4000 ms, etc. • exponentialWithJitter(2) The retransmission period is exponentially calculated with a random weighting factor varying from 88% to 112% of the calculated period. Ex.: Initial period of 500 ms. $\text{Period} = (\text{Period} \times 2) * (\text{Random value (0 to 24)} + 88) / 100$ $\text{Period2} = (\text{Initial period} \times 2) * (\text{Random value (0 to 24)} + 88) / 100$ etc. Default Value: exponentialWithJitter
ncsRetransmissionInitialPeriod	Retransmission initial period in ms. Default Value: 200
ncsRetransmissionMaxPeriod	Retransmission maximum period in ms. Shall be greater than or equal to the retransmission initial period. Default Value: 30000
ncsRetransmissionDisconnect Timeout	Time elapsed (in ms) at which an endpoint becomes disconnected. Default Value: 20000
ncsRetransmissionSuspicion Threshold	Number of retransmissions at which an endpoint may actively query the name server to detect the possible change of the Call Agent's interfaces. Default Value: 7

Table 81: NCS Retransmission Information (Continued)

Variable	Description
ncsRetransmissionSuspicionThresholdDnsQuery	Indicates whether a DNS query is performed or not when the number of retransmissions is equal to the suspicion threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
ncsRetransmissionDisconnectThreshold	Number of retransmissions at which an endpoint should contact the DNS one more time to see if any other interfaces have become available. When the number of retransmissions is greater than this value, the endpoint becomes disconnected. Default Value: 7
ncsRetransmissionDisconnectThresholdDnsQuery	Indicates whether a DNS query is performed or not when the number of retransmissions is equal to the disconnect threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
ncsRetransmissionHistoryTimeout	Number of milliseconds for which the responses to old transactions shall be kept. Default Value: 20000
ncsRetransmissionMaxWaitingDelay	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP (Restart in Progress). Default Value: 600000
ncsRetransmissionDisconnectInitialWaitingPeriod	Initial waiting delay (in ms) an endpoint shall wait before starting the disconnect procedure. Default Value: 15000
ncsRetransmissionDisconnectMinWaitingPeriod	Disconnected minimum waiting delay (in ms) that shall have elapsed since the gateway became disconnected before entering the disconnect procedure. Default Value: 15000
ncsRetransmissionDisconnectMaxWaitingPeriod	Disconnected maximum waiting delay (in ms) since the gateway became disconnected that an endpoint can wait before starting the disconnect procedure. Default Value: 600000

- Restart the Mediatrix 4102 so that the changes may take effect.

Line Package

The Line package groups variables that determine tone timeouts of the NCS protocol Line Package.

► **To set Line package information:**

1. In the *ncsMIB*, locate the *ncsLinePackage* group.
This group contains the information to set.
2. Set the following variables:

Table 82: NCS Line Package Information

Variable	Description
<i>ncsLinePackageBzDuration</i>	Busy tone timeout value in ms. It indicates the line or equipment is in use, engaged or occupied. Default Value: 30000
<i>ncsLinePackageDIDuration</i>	Dial tone timeout value in ms. It indicates the line is ready to receive dialing. Default Value: 16000
<i>ncsLinePackageLDuration</i>	DTMF long duration timeout value in ms. It is observed when a DTMF signal is produced for a duration longer than two seconds. In this case, the Mediatrix 4102 will detect two successive events: first, when the signal has been recognized, the DTMF signal, and then, 2 seconds later, the long duration signal. Default Value: 2000
<i>ncsLinePackageMwiDuration</i>	Message waiting indicator tone timeout value in ms. It indicates there is a message waiting somewhere for the owner of the phone. Default Value: 16000
<i>ncsLinePackageOtDuration</i>	Off hook warning tone timeout value in ms. It indicates that the telephone is not hung up correctly. Default Value: 65535000
<i>ncsLinePackageRbkDuration</i>	Ring back on connection tone timeout value in ms. It is the sound one hears when calling someone else's phone. Default Value: 180000
<i>ncsLinePackageRgDuration</i>	Ring tone timeout value in ms. It indicates the called line is ringing out. Default Value: 180000
<i>ncsLinePackageRoDuration</i>	Reorder tone (also called fast busy) timeout value in ms. It indicates that all switching paths are busy, all toll trunks are busy, there are equipment blockages, the caller dialed an unassigned code, or the digits dialed got messed up along the way. Default Value: 30000
<i>ncsLinePackageRtDuration</i>	Ring back tone timeout value in ms. Default Value: 180000

Table 82: NCS Line Package Information (Continued)

Variable	Description
ncsLinePackageSIDuration	Stutter dial tone timeout value in ms. It notifies the user that they have a voice mail message when the phone does not or cannot have a message-waiting light. Default Value: 16000
ncsLinePackageTCritical Duration	Interdigit timeout value in ms when a timer is all that is required for the digit string to match a pattern in the digit map. Default Value: 4000
ncsLinePackageTPartial Duration	Interdigit timeout value in ms when at least one more digit is required for the digit string to match any of the patterns in the digit map. Default Value: 16000

- Restart the Mediatrix 4102 so that the changes may take effect.

Encoding Name of the Payload Type 18

For NCS compatibility, the Mediatrix 4102 allows you to choose the literal name of the compression algorithm defined by the RTP Payload Type 18. If the Call Agent and the Mediatrix 4102 do not use the same encoding name, this may result in no voice being transmitted.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See ["MIB Structure" on page 47](#) for more details.

► To set the encoding name of the RTP Payload Type 18:

- In the *ncsCompatibilityMIB*, under *mediatrixExperimental*, locate the *ncsCompatibilityMIBObjects* group.
- Set the *ncsCompatibilityRtpPayloadType18EncodingName* variable.
This variable defines the literal name of the compression algorithm corresponding to the RTP payload type 18. You have the following choices:
 - g729
 - g729A
- Restart the Mediatrix 4102 so that the changes may take effect.

RTP Payload Type 18

The payload type "18" identifies the codec G729 (or G729A) in RTP packets. This number is defined by the IANA (Internet Assigned Numbers Authority).

Impacts of Encoding Name

In NCS, the encoding name used for the RTP payload type 18 has an impact on the following :

- The literal name of the compression algorithm in the "Local Connection Options" sent in a NCS command.

Example of local connection options is:

L: a:**G729**, e:on

- The literal name of the compressions algorithm in the "Capabilities" send in a NCS answer.

Example of the capabilities is:

A: a:**G729**, p:10-40, t:0, v:L, m:sendonly;recvonly;sendrecv;inactive

Compatibility Version

You can define the content of the Protocol header in a packet.

► **To set the compatibility version:**

1. In the *ncsCompatibilityMIB*, under *mediatrixExperimental*, locate the *ncsCompatibilityMIBObjects* group.
2. Set the *ncsCompatibilityVersion* variable.

Table 83: NCS Compatibility Version Parameters

Parameter	Description
mgcp01Ncs10	The Protocol header is set to 'MGCP 0.1 NCS 1.0'. This protocol is fully supported.
fakeMgcp10Ncs10	The Protocol header is set to 'MGCP 1.0 NCS 1.0'. This protocol is not supported and the behavior of the unit is the same as for MGCP 0.1 NCS 1.0. This is a fake support to allow communication with a call agent that supports it. This configuration only has an effect if the <i>telephonyIpSignalingProtocolSelection</i> variable is set to ncs ("Introduction" on page 99).

Interoperability Configuration

Please refer to ["Interoperability Configuration" on page 93](#) for a few interoperability parameters you can use to improve the way the Mediatix 4102 interops with other products.



Note: The interoperability parameters apply to units that are either running the MGCP or NCS signalling protocol.

Country-Specific Configuration

This chapter describes how to set the Mediatrix 4102 with the proper country settings.

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
- ▶ Reason for Absence of Calling Line Identity
- ▶ Calling Party Name
- ▶ Reason for Absence of 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)

Both methods can be used on different lines at the same time.

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 line configuration. The Mediatrix 4102 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.
- ▶ Brazil: STD 220-250-713 Issue 01. November 1993: General specification "identification of the calling party for SPC with DTMF".



Note: For units in Brazil, set the *analogScnGwInterDigitDialDelay* and *analogScnGwDtmfDuration* value to 70 ms (in the *analogScnGwMIB*). This will ensure that the caller ID displays properly.

- ▶ Denmark: TDK-TS 900 301-1 January 2003: Public Switched Telephone Network (PSTN)

Calling Line Identification presentation (CLIP) supplementary service Specification of the NTP.

FSK Generation

Different countries use different standards to send caller ID information. The Mediatrix 4102 is compatible with the following widely used standards:

- ▶ Bellcore GR-30-CORE
- ▶ British Telecom (BT) SIN227, SIN242
- ▶ UK Cable Communications Association (CCA) specification TW/P&E/312
- ▶ ETSI 300 659-1



Note: The compatibility of the Mediatrix 4102 is not limited to the above caller ID standards.

Continuous phase binary FSK modulation is used for coding which is compatible with:

- ▶ BELL 202
- ▶ ITU-T V.23, the most common standard

ADSI

ADSI (Analog Display Service Interface) is a telecommunications protocol standard that enables alternate voice and data capability over the existing analog telephone network. It is an extension to basic caller ID. To use ADSI, you would need an ADSI capable device.

ADSI can display the basic caller ID parameters and the following additional parameters:

- ▶ Call Type
- ▶ First Called Line Identity
- ▶ Number of Messages (MWI)
- ▶ Type of Forwarded Call
- ▶ Type of Calling User
- ▶ Redirecting Number
- ▶ Charge
- ▶ Duration of the Call
- ▶ Network Provider Identity



Note: Currently, very few ADSI-capable devices support these additional information.

Setting the Location (Country)

It is very important to set variables according to the country in which the Mediatrix 4102 is used because a number of parameter values are set according to this choice. These parameters are:

- ▶ Tones
- ▶ Rings
- ▶ Impedances
- ▶ Line Attenuations

See [“Appendix D - Country-Specific Parameters” on page 239](#) for more information on these country-specific settings.



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

► **To set a country location:**

1. In the *telephonyMIB*, locate the *telephonyCountrySelection* variable.
This variable indicates the current country used by the Mediatrix 4102. It can also be used to select a caller ID standard in countries that support more than one caller ID standard.
2. Set the variable with one of the following parameters:

North America 1	Sweden	Russia
North America 2	Australia 1	Netherlands
Austria 1	Australia 2	Brazil
Austria 2	Australia 3	New Zealand
France	Japan	UAE 2 (United Arab Emirates)
Germany 1	Israel	uk-bellcore
Germany 2	Thailand	uk-cca
UK	Indonesia	uk-etsi-fsk
Italy	China	france-etsi-fsk
Spain	Hong Kong	france-etsi-dtmf
Switzerland	Malaysia	austria2-etsi-fsk
3. Restart the Mediatrix 4102 so that the changes may take effect.

Caller ID Selection

In countries that support more than one caller ID standard, this standard can be selected with the *telephonyCountrySelection* variable. Be careful to properly select the option corresponding to your caller ID.

Table 84: Caller ID Mappings

Country	Caller ID	<i>telephonyCountrySelection</i> variable Mapping
UK	British Telecom	uk
	Bellcore	uk-bellcore
	CCA	uk-cca
	ETSI-FSK	uk-etsi-fsk
France	Bellcore	france
	ETSI-FSK	france-etsi-fsk
	ETSI-DTMF	france-etsi-dtmf
Austria 1	Bellcore	austria1
	ETSI-FSK	austria-etsi-fsk
Austria 2	Bellcore	austria2
	ETSI-FSK	austria2-etsi-fsk

See ["Caller ID Information" on page 109](#) for more details.

Transparent Address Sharing

This chapter explains how to properly configure the Transparent Address Sharing service for a cable or DSL modem.

Standards Supported

- RFC 1027 – Using ARP to Implement Transparent Subnet Gateways (section 2.14.3.3.8 Processing of ARP messages).

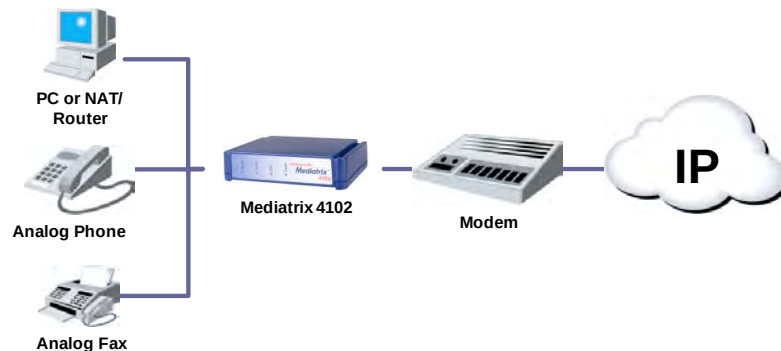
What is Transparent Address Sharing?

When in Transparent Address Sharing (TAS) mode, the Mediatrix 4102 shares a Wide Area Network (WAN) connection with a single PC or a network of IP equipment. The unit routes IP packets between the LAN and the network providing the public address (WAN).

The Media5 patent on transparent IP address sharing allows both WAN and LAN interfaces to be used with a single IP address from the service provider in a user-friendly way, without the configuration complexities of an integrated NAT.

The Mediatrix 4102 thus connects up to two analog phones or fax machines to a broadband access equipment, allowing Service Providers to offer IP telephony services to residential users.

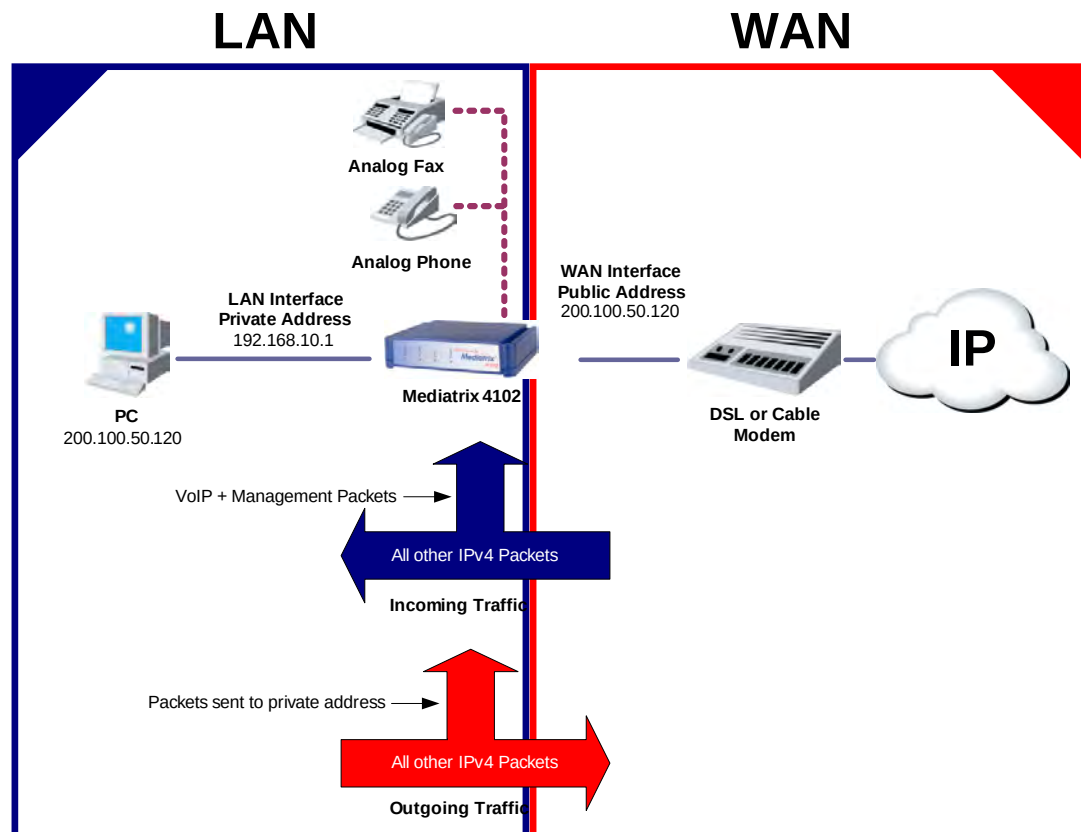
Figure 35: Mediatrix 4102 Residential Application Scenario



In a residential VoIP deployment, the WAN interface of the Mediatrix 4102 gets assigned a public IPv4 address by the ISP, either by a DHCP negotiation, by establishing a point-to-point link (PPPoE), or by some other mechanism depending on the type of link.

The device on the LAN (e.g., the PC) gets assigned the same public IPv4 address as the Mediatrix 4102. The subnet mask given is the same as the one assigned by the ISP, or if it is not available (such as for a PPPoE connection), it uses the predefined subnet classes.

Figure 36: Transparent Address Sharing



The LAN interface of the Mediatrix 4102 is configured with a private IPv4 address. This address allows the device on the LAN to communicate with the Mediatrix 4102 as this would be otherwise impossible because both devices share the same public IPv4 address. The Mediatrix 4102 performs transparent routing by forwarding to the WAN any packet sent to any IPv4 address that is included in the public subnet.

Each packet received from the WAN is forwarded directly to the device on the LAN, except if it belongs to the hosted application, in this case, VoIP. In the other direction, each IPv4 packet received from the LAN is forwarded to the WAN, except for packets sent explicitly to the private address assigned to the Mediatrix 4102. The Mediatrix 4102 itself can initiate a communication with the device on the LAN, by using its private IPv4 address as the source address.

Router Mode

The router mode separates the two external interfaces of the Mediatrix 4102 (the LAN and WAN connectors). The Mediatrix 4102 has two distinct network interfaces with one IP address for each of them. These interfaces are called LAN (LAN connector) and WAN (WAN connector). The Mediatrix 4102 performs IP routing both ways.

The router mode is a requirement for the TAS to properly work. When enabling TAS, you also enable the Mediatrix 4102 in router mode.

In non-router mode, the interfaces are switched and the Mediatrix 4102 only has one network interface. Both external network interfaces generally have the same behaviour.

Cable vs DSL Modem

Most of the Mediatrix 4102 settings are the same no matter what the modem you are using. However, there are a few differences.

Table 85: Cable vs DSL Modem

Cable Modem	DSL Modem
You must configure the Mediatrix 4102 to use a DHCP server to get its IP information as per “DHCP Server Configuration” on page 66. However, some locations may require to manually enter static IP information instead. The easiest way to do so is to use the web interface. See “Chapter 2 - Web Interface – Introduction” on page 25 for more details.	You must configure the PPPoE service as per “PPPoE Service” on page 116. However, some DSL modems may require that you configure the Mediatrix 4102 to use a DHCP server to get its IP information as per “DHCP Server Configuration” on page 66.

Multicast and IGMP

The Mediatrix 4102 does not support the Internet Group Management Protocol (IGMP), i.e., the PC connected to the LAN connector of the Mediatrix 4102 cannot register to IGMP services.

Multicast is communication between a single sender and multiple receivers on a network. IGMP is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content.

Configuration Steps

The following are the steps to follow to properly setup the TAS service.

► To setup the TAS service:

1. Define the PPPoE parameters as described in [“PPPoE Service” on page 116](#). **This only applies if you are using a DSL modem.**
2. Define the WAN IP address configuration source as described in [“WAN Information Configuration Source” on page 118](#).
3. Configure the TAS mechanism as described in [“Configuring TAS” on page 119](#).
4. Optionally, modify port allocation settings as described in [“Ports Settings” on page 123](#).
5. Restart the Mediatrix 4102 so that the changes may take effect.

PPPoE Service

Standards Supported

- RFC 1332 – IP Control Protocol (IPCP)
- RFC 1661 – Point to Point Protocol (PPP)
- RFC 1334 – Password Authentication Protocol (PAP)
- RFC 1994 – Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 – PPP over Ethernet (PPPoE)
- RFC 1471 – PPP Link control Protocol MIB (PPP-LCP-MIB) (with the exception of the LQR MIB)
- RFC 1472 – PPP Security Protocols MIB (PPP-SEC-MIB)
- RFC 1473 – PPP IP Network Control Protocol MIB (PPP-IP-NCP-MIB)
- RFC 1877 – PPP IPCP Extensions for Name Server Address – with the exception of sections 1.2 and 1.4

The Mediatrix 4102 uses the PPPoE protocol to interact with a DSL broadband modem. It can discover a PPP access concentrator (AC) and establish a PPP session with it.



Note: This section applies only if you are using a DSL modem. If you are using a cable modem, go directly to [“WAN Information Configuration Source” on page 118](#).

The PPPoE service is required to properly use the TAS service with DSL modems. You must perform the following tasks to configure the PPPoE service:

- ▶ Enable the PPPoE service.
- ▶ Set a user name and password.

Enabling the PPPoE Service

You must configure and enable the service to properly connect to an access concentrator.

You can also use the web interface to enable the PPPoE service. See [“WAN Page” on page 29](#) for more details.

▶ To configure the PPPoE service:

1. In the *ipAddressConfig* folder, set the *localHostSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group) to **static**.
This is required to avoid conflicts with the PPPoE interface. See [“Local Host” on page 57](#) for more details on the local host settings.
2. Set the *localHostStaticDefaultRouter* variable (under the *ipAddressConfigLocalHostStatic* group) to **0.0.0.0**.
3. In the *pppoeMIB*, set the *pppoeAcName* variable with the name of the access concentrator to which connect.
The variable may be set with any string of characters, with a maximum of 255 characters.

PPPoE

PPPoE (Point to Point Protocol over Ethernet) is a proposal specifying how a host personal computer interacts with a DSL broadband modem to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dialup Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

If you leave this variable empty, the Mediatrix 4102 accepts the first offer that it receives.

4. Set the *pppoeServiceName* variable with the name of the service requested to the access concentrator.
The variable may be set with any string of characters, with a maximum of 255 characters.
If you leave this variable empty, the Mediatrix 4102 looks for any access concentrator.
5. Enable the PPPoE service by setting the *pppoeEnable* variable to **enable**.



Note: When establishing a PPPoE connection, the default router IP address is automatically overridden by the PPP connection's peer IP address.

6. If you do not need to configure other parameters, restart the Mediatrix 4102 as per [“Restarting the Mediatrix 4102” on page 124](#).

Setting a User Name and Password

When connecting to an access concentrator, it usually requests that the Mediatrix 4102 identifies itself with a specific user name and password, also called ID and secret pair. This information is set in the standard *PPP-SEC-MIB* as described in RFC 1472.

You can also use the web interface to enter the PPPoE user name and password. See [“WAN Page” on page 29](#) for more details.

► To configure a user name and password:

1. In the *PPP-SEC-MIB*, locate the *pppSecuritySecretsTable*.
This table contains the ID (user name) and secret (password) pair that the Mediatrix 4102 advertises to the access concentrator.



Caution: When you are in a specific row and you set the *pppSecuritySecretStatus* variable of this row to **invalid**, the row is deleted and you cannot add it back. When the last remaining row is deleted, two rows are re-created with default passwords and user names.

2. Set the Identity (user name) of the ID/Secret pair in the *pppSecuritySecretsIdentity* variable.
You can set an identity for both security protocols (CHAP and PAP) supported. The table contains one row for each protocol. The CHAP security protocol is described in RFC 1994, while the PAP security protocol is described in RFC 1334. If you want to exclusively use one of the security protocols, you can disable the other row.
3. Set the secret (password) of the ID/Secret pair in the *pppSecuritySecretsSecret* variable.
You can set an identity for both security protocols (CHAP and PAP) supported. The table contains one row for each protocol. The CHAP security protocol is described in RFC 1994, while the PAP security protocol is described in RFC 1334. If you want to exclusively use one of the security protocols, you can disable the other row.
For other standard settings, please refer to the MIBs described in RFC 1471 (with the exception of the LQR MIB), RFC 1472, and RFC 1473.
4. If you do not need to configure other parameters, restart the Mediatrix 4102 as per [“Restarting the Mediatrix 4102” on page 124](#).

WAN Information Configuration Source

The WAN address is the public IP address attributed to the Mediatrix 4102. This address is used for incoming signalling, media and management traffic. You can assign this information to the Mediatrix 4102 through an access concentrator (DSL modem) or DHCP server (cable modem).

► **To set the WAN IP address configuration source:**

1. In the *ipAddressConfig* folder, locate the *localHostWanAddressSelectConfigSource* variable (under the *ipAddressConfigLocalHost* group).

This variable indicates the source to be used for the provisioning of the WAN address.

Table 86: WAN IP Address Source Settings

Option	Description
localAddress	The WAN address is the one that is set in the <i>localHostAddress</i> variable, whereas the <i>localHostStaticWanAddress</i> is ignored.
static	The Mediatrix 4102 has a static WAN address. The address is configured in the <i>localHostStaticWanAddress</i> variable. Note that this setting allows a limited NAT traversal scheme.
pppoe	The Mediatrix 4102 uses PPP over Ethernet in order to obtain its WAN IP address. Note: The PPPoE service must be enabled for the WAN address to be configured.
automatic	If the PPPoE service is enabled, the Mediatrix 4102 uses <i>pppoe</i> as the configuration source. Otherwise it uses <i>localAddress</i> .

2. Set the *localHostWanAddressSelectConfigSource* variable to **automatic**.
You can query the actual configuration source used in the *localHostWanAddressConfigSource* read-only variable (in the *ipAddressStatus* folder).
You can query the actual WAN IP address attributed to the Mediatrix 4102 in the *localHostWanAddress* read-only variable (in the *ipAddressStatus* folder).
3. If you do not need to configure other parameters, restart the Mediatrix 4102 as per [“Restarting the Mediatrix 4102” on page 124](#).

Configuring TAS

The following steps describe how to properly setup and enable the Mediatrix 4102 in TAS mode. By enabling TAS, you also implicitly enable the Mediatrix 4102 in router mode (see [“Router Mode” on page 114](#) for more details).

When the TAS service is enabled, it adds a network interface to the Mediatrix 4102. This means that two IP addresses may be attributed to the unit – the *LAN* and *WAN* connectors of the Mediatrix 4102 each have an IP address.

The *LAN* and *WAN* connectors of the Mediatrix 4102 are allocated IP addresses differently depending on the scenario involved:

► **TAS disabled**

The *LAN* and *WAN* connectors use the same IP address as set in the *localHostAddress* variable. See [“Local Host” on page 57](#) for more details.

► **TAS enabled - cable modem (PPPoE disabled)**

The *WAN* connector receives an IP address to access the WAN. This IP address is coming from the DHCP server and is stored in the *localHostAddress* variable. See [“Local Host” on page 57](#) for more details.

The IP address of the *LAN* connector (LAN interface) is configured statically, as described in [“LAN Interface” on page 120](#).

Figure 37: Cable Modem IP Addresses



For example:

- The Mediatrix 4102 is set up to get a WAN address via DHCP.
- The local host address is set to the DHCP-derived address (let's say 10.40.40.53).
- The LAN side address is also 10.40.40.53. This is consistent with the TAS feature.

The *lanStaticAddress* variable is set by default to 192.168.10.1.

In summary:

a. WAN is good.

IP address 10.40.40.53 on both sides, WAN and LAN.

The web page of the Mediatrix 4102 is at 192.168.10.1.

b. WAN goes down.

The IP address 10.40.40.53 is not available on the WAN side.

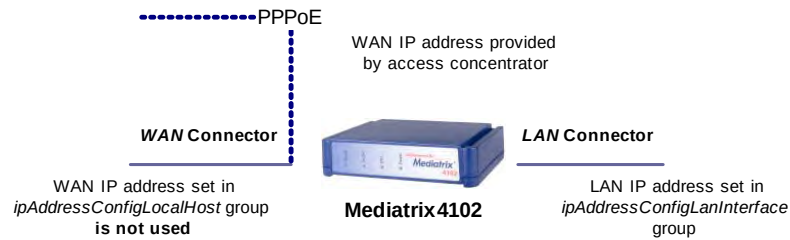
The web page of the Mediatrix 4102 is still at 192.168.10.1.

The IP address of the *LAN* connector is the IP address of the Mediatrix 4102 plus or minus 1, i.e., the IP address of the *LAN* connector is either 192.168.10.0 or 192.168.10.2.

► **TAS enabled - DSL modem (PPPoE enabled)**

The *WAN* connector receives an IP address to access the WAN. This IP address is coming from the access concentrator and is stored in the *localHostWanAddress* variable. In this case, the IP address in the *localHostAddress* variable is not used.

The IP address of the *LAN* connector (LAN interface) is configured statically, as described in [“LAN Interface” on page 120](#).

Figure 38: DSL Modem IP Addresses (PPPoE)

QoS Differentiated Services Fields

If you want to differentiate the packets sent by the PC from the packets sent by the Mediatrix 4102, you must substitute a configured value for the QoS Differentiated Services fields of the packets sent from the PC (routed from the LAN to the WAN interface).

The goal is to prioritize the Mediatrix 4102's packets over the PC's packets. This allows to offer a quicker response time for the voice, for instance. However, the ISP's network must support QoS routing. It must be configured accordingly and route according to the DiffServ it encounters.

See ["Differentiated Services \(DS\) Field" on page 195](#) for more details.

► To configure a substitution value:

1. In the *ipRoutingMIB*, set the substitution value in the *ipRoutingQosDiffServSubstitution* variable. This substitution value is used for the Differentiated Services fields of IP packets originating from the equipment connected to the LAN interface and routed to the WAN. It supersedes the TOS byte of the packets coming from the PC. The default value is **0**.
2. Set the *ipRoutingQosDiffServSubstitutionEnable* variable to **enable**. The *DiffServ* field of IP packets originating from the equipment connected to the LAN interface and routed to the WAN is modified.
3. If you do not need to configure other parameters, restart the Mediatrix 4102 as per ["Restarting the Mediatrix 4102" on page 124](#).

LAN Interface

The Mediatrix 4102's two Ethernet connectors are used as follows:

- **WAN connector:** WAN interface of the Mediatrix 4102 where you can connect your modem.
- **LAN connector:** LAN interface where you connect the PC or other IP equipment. The LAN interface is usually used to connect a PC that will have access to the WAN by sharing the Mediatrix 4102 WAN address.



Note: The LAN interface configuration settings are valid only when TAS is enabled.

You can also use the web interface to configure the LAN interface parameters. See ["LAN Page" on page 31](#) for more details.

► To configure the LAN interface settings:

1. In the *ipAddressConfig* folder, locate the *ipAddressConfigLanInterface* group.
2. Set the LAN IP address of the LAN connector in the *lanStaticAddress* variable. If TAS is disabled, the LAN connector rather uses the same address as the WAN connector as set in the *localHostAddress* variable. See ["Local Host" on page 57](#) for more details.



Note: Do not set the *lanStaticAddress* variable to 0.0.0.0. This could prevent the unit from properly sending a DHCP discover request.

- Set the LAN subnet mask of the *LAN* connector in the *lanStaticNetworkMask* variable.
If TAS is disabled, the *LAN* connector rather uses the same network mask as the *WAN* connector as set in the *localHostNetworkMask* variable. See [“Local Host” on page 57](#) for more details.



Note: Media5 recommends not to set the *lanStaticNetworkMask* variable to 255.255.255.254 because this would only create a subnet with two addresses. This only leaves one bit host address. Since a subnet must have a network (all bits 0) and a broadcast (all bits 1) address, this leaves no room for hosts.

- If you do not need to configure other parameters, restart the Mediatrix 4102 as per [“Restarting the Mediatrix 4102” on page 124](#).

MAC Address Spoofing

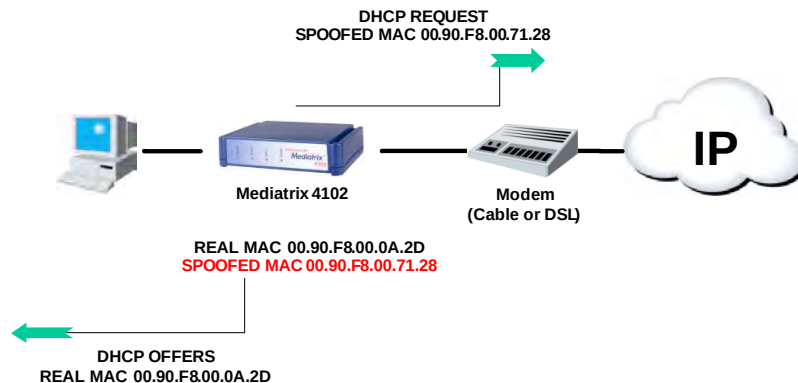
A number of ISPs control connections to their servers by monitoring the MAC address of the connecting device. If the MAC address does not match its database, it refuses the connection.

Consider the typical scenario in which a user of a Mediatrix 4102 is already subscribed to an ISP for a WAN access (i.e., the Internet). If the ISP monitors the MAC address, the user will not be able to connect to the WAN when using the Mediatrix 4102 in front of the usual device.

The workaround is to have the Mediatrix 4102 spoof its MAC address in messages destined to the WAN. The spoofed MAC address matches the ISP's database and the connection will be granted. However, the spoof is only performed on the WAN side of the Mediatrix 4102. The LAN (or private) side of the Mediatrix 4102 remains unchanged.

For example, DHCP requests sent by the Mediatrix 4102 on the WAN side would contain the spoofed MAC address, but DHCP offers returned by the Mediatrix 4102 to the device networked on the *LAN* connector will contain the real MAC address of the Mediatrix 4102.

Figure 39: MAC Address Spoofing



You can also use the web interface to enter the MAC address spoofing information. See [“LAN Page” on page 31](#) for more details.

► To spoof the MAC address:

- In the *ipRoutingMIB*, set the MAC address used to spoof the unit's actual MAC address in the *ipRoutingMacSpoofAddress* variable.
A valid MAC address is a continuous series of 12 hexadecimal digits (without colons). An empty character string means that the spoofing is considered disabled, even though the *ipRoutingMacSpoofEnable* variable is set to **enable**.



Note: The following MAC addresses are not allowed:

- 000000000000
- FFFFFFFFFFFF
- 01xxxxxxxxxx, where x can be any digit or letter

You can view the current MAC address of the online device in the *LAN* connector in the *ipRoutingMacAddress* variable (*ipRoutingMacSpoof* group of the *ipRoutingMIB*).

If you are using a router that is connected to the *LAN* connector of the Mediatrix 4102, you must disable the router's MAC address spoofing feature so that the Mediatrix 4102 properly spoofs the MAC address of the PC connected to the router. In this case, the *ipRoutingMacAddress* variable does not show the PC's MAC address, but rather the router's MAC address.

2. Enable the MAC address spoofing by setting the *ipRoutingMacSpoofEnable* variable to **enable**.
The unit's MAC address used on the WAN side is the configured MAC address.
If you set the variable to **disable**, the unit's MAC address used on the WAN side is the actual unit's MAC address.
3. If you do not need to configure other parameters, restart the Mediatrix 4102 as per ["Restarting the Mediatrix 4102" on page 124](#).

Enabling TAS

Enabling TAS is essential to use a broadband connection. By enabling TAS, you also implicitly enable the Mediatrix 4102 in router mode. See ["Router Mode" on page 114](#) for more details.

► To configure TAS:

1. In the *ipRoutingMIB*, set the duration, in seconds, of the lease offered by the DHCP server in the *ipRoutingDhcpServerLeaseTime* variable (in the *ipRoutingDhcp* group).
The TAS service of the Mediatrix 4102 contains a DHCP server. Enabling TAS also enables this DHCP server, which allocates an IP address to the PC or IP equipment located on the LAN. See ["DHCP Server" on page 125](#) for more details.



Note: The DHCP server embedded in the Mediatrix 4102 allocates only one address. To connect more PCs to the Mediatrix 4102, use a router.

The *ipRoutingDhcpServerLeaseTime* variable is the lease time given to the PC connected to the Mediatrix 4102.

- If the lease time is short, the PC will react faster to address changes, but it will have to renew its lease often.
 - If the lease time is long, the PC will react more slowly to address changes.
2. Enable TAS by setting the *ipRoutingEnable* variable to **enable**.
You may want to disable the factory reset procedure of the Mediatrix 4102, even if users depress the *Default Settings* switch. See ["Disabling the Factory Reset" on page 23](#) for more details.
 3. If you do not need to configure other parameters, restart the Mediatrix 4102 as per ["Restarting the Mediatrix 4102" on page 124](#).
Optionally, you may want to modify the port allocation settings.

Ports Settings

The Mediatrix 4102 allows you to define how to dynamically allocate the ports it uses. This allows for better NAT and firewall traversal capabilities.

UDP and TCP Ports

When needed, the TCP/IP implementation of the Mediatrix 4102 randomly selects a dynamic port amongst the free ports of the range.

Let's say for instance that the dynamic ports range is from 41000 to 42000. The Mediatrix 4102 needs to download a new version of its software. The TCP/IP implementation selects a local UDP port for the TFTP client. The port is selected in the dynamic ports range so the port has a value between 41000 and 42000.

► **To set the range of the UDP and TCP ports:**

1. In the *sysConfigMIB*, set the lower boundary for the range of dynamic UDP and TCP ports in the *sysConfigMinDynamicPort* variable.
The default lower boundary value is **31001**.
2. Set the upper boundary for the range of dynamic UDP and TCP ports in the *sysConfigMaxDynamicPort* variable.
The default upper boundary value is **32000**.
3. If you do not need to configure other parameters, restart the Mediatrix 4102 as per ["Restarting the Mediatrix 4102" on page 124](#).



Note: The smallest acceptable range – between the lower and upper boundaries – is 500.

T.38 Base Port Range

The T.38 ports are allocated starting from the base port. T.38 uses one port for each FXS interface.

► **To define a T.38 base port:**

1. In the *dataIffMIB*, set the *dataIffT38BasePort* variable with the port number you want to use as T.38 base port.
The default T.38 base port is **6004**. In the case of the base port defined on 6004:
 - If there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it uses the T.38 port 6004.
 - If there is currently a call on FXS connector 1 and FXS connector 2 has an incoming or outgoing call, then FXS connector 2 uses the T.38 port 6005.
2. If you do not need to configure other parameters, restart the Mediatrix 4102 as per ["Restarting the Mediatrix 4102" on page 124](#).

UDP and TCP Ports Ranges

The UDP and TCP ports are separated in three ranges: well-known ports (0 to 1023), registered ports (1024 to 49151) and dynamic ports (49152 to 65535). The IANA (Internet Assigned Numbers Authority, www.iana.org) assigns the well-known ports. The IANA also lists the registered ports. The dynamic ports are not under the authority of the IANA. Most TCP/IP implementations use the range 1025 to 65535 for dynamic ports instead of the range defined by the IANA.

RTP/RTCP Base Port Range

The RTP/RTCP ports are allocated starting from the base port. The Mediatrix 4102 may use two or four RTP/RTCP ports for each FXS interface:

- ▶ It uses two ports in case of a standard call.
- ▶ It uses four ports in other types of calls such as a conference call, a call transfer, etc.

▶ **To define a RTP/RTCP base port:**

1. In the *ntpMIB*, set the *ntpConfigBasePort* variable with the port number you want to use as RTP/RTCP base port.

The default RTP/RTCP base port is **5004**. In the case of the base port defined on 5004:

- If there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it uses the RTP/RTCP ports 5004 and 5005.
- If there is currently a standard call on FXS connector 1 and FXS connector 2 has a conference call, then FXS connector 2 uses the RTP/RTCP ports 5006, 5007, 5008, and 5009, which are the next available ports.

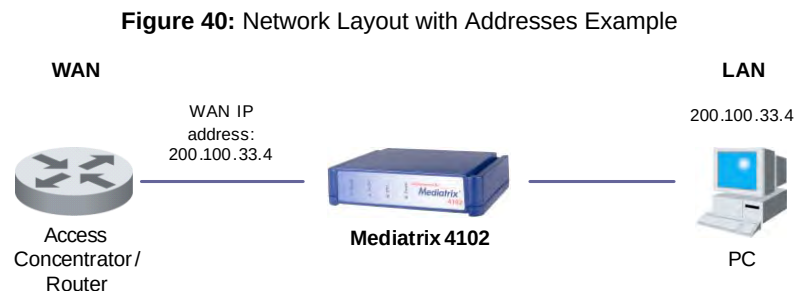
2. If you do not need to configure other parameters, restart the Mediatrix 4102 as per [“Restarting the Mediatrix 4102” on page 124](#).

Restarting the Mediatrix 4102

Once all the mandatory and optional changes are done, restart the Mediatrix 4102 so that the changes may take effect.

If you are using , the Mediatrix 4102 tries to establish a PPP connection to the access concentrator.

The IP address of the PC is set to be the exact same as the unit's WAN address. The embedded DHCP server provides the IP address to the PC.



DHCP Server

Enabling the TAS service also enables a DHCP server that allocates IP addresses to the PC located on the LAN.

DHCP Server Compliance

Standards Supported

- RFC 2131 – Dynamic Host Configuration Protocol, section 2
- RFC 2132 – DHCP Options and BOOTP Vendor Extensions

The DHCP server is compliant to RFC 2131 and RFC 2132 with the following limitations:

- ▶ The pool of assignable IP addresses contains only one address. This means that only one DHCP client at a time can lease an address. All other lease requests are ignored.
- ▶ The DHCP server never accepts the IP address requested by the client (option 50) unless by coincidence.
- ▶ The DHCP server never accepts the lease time that is proposed by the client (option 51) unless by coincidence.
- ▶ The DHCP server returns only the options specified in ["Supported DHCP Options" on page 125](#), all other parameter requests (as part of option 55) are ignored.

Supported DHCP Options

The DHCP server embedded in the Mediatrix 4102 supports the following options.

Table 87: Supported DHCP Option

Code	Description
1	Network Mask When the router state is public, returns a subnet mask that depends on the class of the WAN address. See RFC 791, section 3.2. When the router state is private, returns the network mask as configured in the MIB.
3	Router Option When the router state is public, returns the first address in the subnet. When the router state is private, does not return a router IP address.
6	Domain Name Server Option Returns the list of DNS addresses as configured in the MIB.
42	Network Time Server Option Returns the SNTP server address as configured in the MIB. If the MIB contains a FQDN, option 42 contains the resolved IP address.
51	Lease Time Returns 20 seconds.
52	Option Overload Always set to "3".
53	DHCP Message Type
53	Server Identifier Returns the unit's LAN IP address.

DSL Modem Specific Information

The following sections apply only if you are using a DSL modem.

Establishing a Connection

When the Mediatrix 4102 restarts, it establishes the connection to the access concentrator in conformance with the RFCs listed in [“PPPoE Service” on page 116](#).

When establishing a PPP connection, the Mediatrix 4102 goes through three distinct phases:

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

Discovery Phase

The Mediatrix 4102 broadcasts the value of the *pppoeServiceName* MIB variable (see [“Enabling the PPPoE Service” on page 116](#) for more details).

The access concentrator with a matching service name answers the Mediatrix 4102.

- ▶ If no access concentrator answers, this creates a “PPPoE failure” error. The Mediatrix 4102 handles it as described in [Table 88 on page 127](#).
- ▶ If more than one access concentrators respond to the discovery, the Mediatrix 4102 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 4102 sends the ID/secret pair configured in the *pppSecuritySecretsTable* (see [“Setting a User Name and Password” on page 117](#) for details). If the access concentrator rejects the authentication, this creates an “authentication failure” error. The Mediatrix 4102 handles it as described in [Table 88 on page 127](#).

Network-Layer Protocol Phase

The Mediatrix 4102 negotiates an IP address. The requested IP address is the one from the last successful PPPoE connection. If the Mediatrix 4102 never connected by using PPPoE (or after a factory reset), it does not request any specific IP address.

When the PPP connection is established, the access concentrator assigns an IP address to the Mediatrix 4102. This IP address may be used as the WAN IP address. See [“WAN Information Configuration Source” on page 118](#) for details.

Primary and secondary DNS servers may be supplied by the access concentrator. If this is the case, the new DNS servers supersede the servers defined locally.

Configuration of DNS Servers

When the PPP connection is active, the DNS servers supplied by the access concentrator supersede the locally defined servers as follows:

- ▶ If the *localHostDnsOverrideEnable* variable is set to **enable**, the servers supplied by the access concentrator do not replace the *localHostPrimaryDns* or *localHostSecondaryDns* variables. See [“Static DNS” on page 60](#) for more details.
- ▶ If the *localHostDnsOverrideEnable* variable is set to **disable**:
 - If no server is supplied by the access concentrator, the value of the *localHostPrimaryDns* and *localHostSecondaryDns* variables applies.
 - If one server is supplied by the access concentrator, it replaces the server defined in the *localHostPrimaryDns* variable.

- If two servers are supplied by the access concentrator, they replace both the *localHostPrimaryDns* and *localHostSecondaryDns* variables.



Note: If the DNS servers addresses sent by the access concentrator change while the Mediatrix 4102 is establishing the connection to the access concentrator, you must restart the unit so that it uses the new addresses.

Error Handling

The following describes the Mediatrix 4102 behaviour in case of error.

Table 88: Error Handling

On this error...	The Mediatrix 4102...
Authentication failure	1. Waits for 10 seconds. 2. Retries to establish the connection as in "Establishing a Connection" on page 126.
PPPoE failure	1. Waits for 10 seconds. 2. Retries to establish the connection as in "Establishing a Connection" on page 126.
Peer not responding	1. Retries to establish the connection as in "Establishing a Connection" on page 126.

Connection Unsuccessful

If the first PPP connection fails, the Mediatrix 4102 stops its initialization until the PPP connection is opened successfully. Until the PPP connection is successfully established, the unit cannot be reached by using SNMP. However, you can access the web page through the LAN port.

PPP Connection Loss

A network connection may abruptly shutdown for many reasons. One of the most common reasons is the maintenance of the network and its environment.

When the Mediatrix 4102 detects it has lost the PPP connection, it tries to re-establish the connection as in ["Establishing a Connection" on page 126.](#)

It is possible that the IP address assigned by the access concentrator changes after re-establishing a connection. In this case, the Mediatrix 4102 restarts because it does not support dynamic IP address change.

Routing Mechanism

Usually, the packets go through the Mediatrix 4102.

If the PC wants to directly contact the Mediatrix 4102, it must use the unit's LAN address (*localHostAddress* variable if TAS is disabled or *lanStaticAddress* if TAS is enabled).

Blocked Ports

The Mediatrix 4102 uses some ports for signalling, media transport and management purposes. Packets sent to these ports are blocked. Most of the ports can be configured by using a MIB variable.

Table 89: Blocked Ports

Port Description	Port Number	Configurable
SNMP	161 UDP	Yes
DHCP offer listening	68 UDP	No
TFTP server for configuration downloads. Note: This port is used only if the configuration download service is enabled, and only for the time it is required.	69 UDP	No
MGCP/NCS	2427	Yes
RTP/RTCP Note: The Mediatrix 4102 uses up to four UDP ports per FXS interface. See "RTP/RTCP Base Port Range" on page 124 for details.	5004+ UDP	Yes
T.38 Note: The Mediatrix 4102 uses one UDP port per FXS interface. See "T.38 Base Port Range" on page 123 for details.	6001+ UDP	Yes

Using the Mediatrix 4102 with a Low Bandwidth Connection

You can use the Mediatrix 4102 with a low bandwidth connection without any visible performance issues. This is true for both DHCP and PPPoE connections, with either a DSL or cable modem. However, you must configure the Mediatrix 4102 accordingly.

What is Considered a Low Bandwidth Connection?

Media5 considers that the process is not optimal when the transmission of one or more large Ethernet packet takes more time than the time it takes for packetization. For instance, a 1518 bytes packet takes the following transmission time according to the bandwidth:

Table 90: Transmission Time vs. Bandwidth

Bandwidth (kbps)	Transmission Time (ms)
64	190
128	95
256	47
512	24
1024	12
2048	6

Table 90: Transmission Time vs. Bandwidth

Bandwidth (kbps)	Transmission Time (ms)
4096	3

One can see that from 128 kbps or less, the delay becomes significant, considering this is for one packet only. Media5 thus recommends to follow the configuration in the next section for a bandwidth lower than 4096 kbps. This will ensure the best voice quality possible.

Configuration for a Low Bandwidth Connection

The following steps should allow you to use a low bandwidth connection.

► To use the Mediatrix 4102 with a low bandwidth connection:

1. Configure the Mediatrix 4102 in TAS mode as described in this chapter. Enable the TAS mode by setting the *ipRoutingEnable* variable to **enable**. See ["Enabling TAS" on page 122](#) for more details.
2. In the *qosleee8021q* group of the *qosMIB*, define a 802.1q priority for the voice and fax packets in the following variables.

- *qosVoiceleee8021qUserPriority* for voice priority
- *qosT38Faxleee8021qUserPriority* for fax priority

The Mediatrix 4102 uses 9 output queues with increasing priorities. The lowest priority queue is always used for the traffic coming from the LAN port and routed to the WAN port. You cannot change this priority level. The 8 other queues are used for the traffic the Mediatrix 4102 sends. By default, the lowest priority queue (of these 8 queues) is used for all traffic, and the other 7 are unused.

However, you can assign certain types of traffic to other queues of higher priority by configuring a 802.1q priority. It is not required to activate the packet tagging feature, only provide a priority to the protocol.

A good practice would be to always have a priority other than "0" for the voice and the fax. The signalling could also receive a higher priority. Thus, the SNMP and HTTP accesses performed from the WAN would be answered in lower priority.

See ["IEEE 802.1q" on page 196](#) for more details on 802.1q priorities.

3. Set the value of the following variables to **enable**:
 - *qosVoiceleee8021qEnable*
 - *qosT38Faxleee8021qEnable*

The corresponding user priority configuration is enabled.

4. Restart the Mediatrix 4102 so that the changes may take effect.

Configuration File Download

The configuration file download feature allows to update the Mediatrix 4102 configuration by transferring a configuration file via TFTP or HTTP. The configuration file can either be transferred from the management server or from the configuration file download server. The main difference is the session initiator, which is respectively the management server and the Mediatrix 4102. The advantage of having the Mediatrix 4102 as the session initiator is to allow NAT traversal.

You can also manually upload a configuration file to the Mediatrix 4102 by using the web interface. See [“Configuration File Upload Page” on page 33](#) for more details.

Configuration File Download Server

The service allows to download a unique file for each Mediatrix 4102, and/or a file shared among many units. These configuration files may be encrypted or not.

You have the choice to perform the configuration file download by using the TFTP protocol or the HTTP protocol. You can also configure the Mediatrix 4102 to automatically update its configuration.

To download a configuration file, you may need to setup the following applications on your computer:

- ▶ TFTP server with proper root path
- ▶ SNTP server properly configured
- ▶ HTTP server with proper root path
- ▶ Configuration source
- ▶ Configuration file name and location

Configuring the TFTP Server

If you are to perform a configuration file download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

If you are to use the automatic configuration file update feature (see [“Automatic Configuration Update” on page 139](#) for more details), you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to [“Chapter 16 - SNTP Settings” on page 189](#) for more details on how to configure the Mediatrix 4102 for a SNTP server.

Configuring the HTTP Server

If you are to perform a configuration 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.

Configuration File Server Settings

The Mediatrix 4102 must know the IP address and port number of its configuration file server. This server contains the configuration file the Mediatrix 4102 will download. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself in static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *configFileFetchingSelectConfigSource* variable (under the *ipAddressConfigFileFetching* group).
This variable defines whether the Mediatrix 4102 must ask for its configuration file server settings through a DHCP server or not.
2. Set the *configFileFetchingConfigSource* variable to **dhcp**.
You can query the configuration file server's IP address and port number assigned by the DHCP server in the following read-only variables (in the *ipAddressStatus* folder):
 - *configFileFetchingHost*
 - *configFileFetchingPort*
3. Set how you want to define the configuration server information in the DHCP server:

Table 91: Configuration File Server DHCP Information

To use a...	Set...
vendor specific code	The <i>configFileFetchingDhcpSiteSpecificCode</i> variable to 0 . Set the configuration file server IP address in the DHCP server inside the vendor specific sub-option 201 (hexadecimal 0xC9).
site specific code	The <i>configFileFetchingDhcpSiteSpecificCode</i> variable to any value between 128 and 254. Set the configuration file server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>configFileFetchingDhcpSiteSpecificCode</i> variable in the unit's configuration).

See [“Vendor and Site Specific DHCP Options” on page 67](#) for more details.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► To use static information:

1. In the *ipAddressConfig* folder, locate the *configFileFetchingSelectConfigSource* variable.
This variable defines whether the Mediatrix 4102 must ask for its configuration file server settings through a DHCP server or not.
2. Set the *configFileFetchingSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 92: Configuration File Server Static Information

Variable	Description
<i>configFileFetchingStaticHost</i>	Static configuration file server IP address or domain name to use when downloading a configuration file. This is the current address of the PC that hosts the configuration files. Default Value: 192.168.0.10
<i>configFileFetchingStaticPort</i>	Static configuration file server IP port number to use when downloading a configuration file. Default Value: 69

The default port value complies to RFC 1340 on the well-known ports (assigned numbers). This value applies to a TFTP server. It may be different for other servers. If you are using an HTTP server to perform the configuration file download, you must change the port value to 80.

Setting up the Configuration File Download

When performing a configuration file download, you can download two different files:

- ▶ A generic configuration file that should be used to update a large number of units with the same configuration.
- ▶ A specific configuration file that contains the configuration for a single unit, for instance the telephone numbers of its lines.

When both the generic and specific configuration files are downloaded, settings from the specific configuration file always override the settings from the generic configuration file. These files must be located in the same directory.

▶ To setup the configuration file download:

1. In the *configFileFetchingMIB*, set the *configFileFetchingFileLocation* variable with the path, on the remote server, of the directory where the configuration files are located.

The path is case sensitive hence it must be entered properly.

The path is relative to the root path of the transfer server (*configFileFetchingHost*). Use the "/" character when defining the path to indicate sub-directories.

Let's consider the following example:

- The directory that contains the configuration file is called: **Config_File**.
- This directory is under **C:/Root/Download**.

Table 93: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	Config_File
c:/	root/download/Config_File
c:/root	download/Config_File

The following are some tips to help your download process:

- Use the "/" character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the "/" character and produce an error. In this case, use the "\" character.
- Use basic directory names, without spaces or special characters such as "~", "@", etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the configuration file path of the Mediatrix 4102 (you may have to convert "\" into "/") to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

2. Set the *configFileFetchingFileName* variable with the name of the generic configuration file to download.



Caution: The generic configuration file must be in XML format, no matter what its file extension.

The file name is case sensitive hence it must be entered properly.

This file should be used to update a large number of units with the same configuration.

If you leave the variable empty, the Mediatrix 4102 does not download the generic configuration file.

3. Set the *configFileFetchingSpecificFileName* variable with the name of the specific configuration file to download.



Caution: The specific configuration file must be in XML format, no matter what its file extension.

The file name is case sensitive hence it must be entered properly.

This file should be used to update the configuration of a single unit.

This variable may contain macros that are substituted by actual values when downloading the configuration file. Supported macros are:

- %mac%: the MAC address of the unit
- %product%: the product name of the unit
- %%: the character “%”

For instance:

- The “%mac%.xml” value for a Mediatrix 4102 with MAC address “0090F12345AB” will be “0090F12345AB.xml”.
- The value “Hello%%Hi” will result in “Hello%Hi”.
- The value “%%mac%%mac%.xml” will result in “%0090F12345AB%mac%.xml”.

From left to right: the first macro encountered is first substituted, the second macro encountered is then substituted, etc.

When the character “%” is not part of a macro, it is not replaced. The following are examples:

- The value “%mac.xml” stays “%mac.xml”
- The value “Hello%Hi” stays “Hello%Hi”
- The value “%moc%.xml” stays “%moc%.xml”

If the variable is empty (after macro substitution), the Mediatrix 4102 does not download the specific configuration file.

Configuration Update Status

If valid configuration files are successfully downloaded, then the Mediatrix 4102 automatically restarts to apply all the new settings. If the Mediatrix 4102 does not restart, this could mean the download failed or that the configuration in the file is the same as the configuration in the unit.

You can validate the status of the configuration update in various ways.

MIB Variable

You can query the status of the last configuration file download in the *sysAdminDownloadConfigFileStatus* variable:

- ▶ idle: No configuration file download has been performed yet.
- ▶ fail: The last configuration file download failed.
- ▶ success: The last configuration file download succeeded.
- ▶ inProgress: A configuration file download is in progress.
- ▶ listening: The unit is listening and waiting for a configuration file to be sent by the management server.

Syslog Messages

A lot of information is transmitted as system log (syslog) messages. The following are some of the syslog messages sent by the unit:

Table 94: Configuration File Download Syslog Messages

Level	Message	Event
Informational	The specific configuration update succeeded.	The configuration update with the specific configuration file has been successful.
Error	The specific configuration update failed.	The configuration update with the specific configuration file experienced an error and has not been completed.
Informational	The configuration file "XXX" was successfully fetched.	A configuration file was successfully fetched.
Informational	The unit configuration is not updated. The parameter values defined in the fetched configuration files are identical to the actual unit configuration.	The parameter values defined in the fetched configuration files are identical to the actual unit configuration.
Informational	The generic file \"%s\" parameter values are not applied. They are either identical to the unit configuration or overwritten by the specific file.	The generic configuration file parameter values are either identical to the unit configuration or overwritten by the specific configuration file.
Warning	None of the parameter values defined in the configuration file \"%s\" was successfully applied.	No parameter value from a fetched configuration file was successfully applied (e.g., because of bad OIDs).
Informational	Parameter values defined in the configuration file \"%s\" were successfully applied.	A fetched configuration file was successfully applied.
Informational	The unit is restarting to complete the configuration update.	All necessary fetched configuration files were successfully applied.

You can view these messages in the web interface. See ["System Log Page" on page 36](#) for more details.

Configuration Files Encryption

You can secure the exchange of configuration files between the server and the Mediatrix 4102. A privacy key allows the unit to decrypt a previously encrypted configuration file. This applies to files downloaded via TFTP or HTTP, but NOT on updates performed from the web interface.

To encrypt a configuration file (generic or specific), you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts files before sending them to the Mediatrix 4102 unit. Contact your sales representative for more details.

Configuration File Decryption on the Mediatrix 4102

The following describes how to decrypt a previously encrypted generic or specific configuration file. You must have one key for the generic configuration file and another key for the specific configuration file.

► **To decrypt a configuration file:**

1. In the *configFileFetchingMIB*, set the proper decryption variable with the secret key used to decrypt the configuration file.

Table 95: Decryption Variables

Configuration File	Variable
Generic	configFilePrivacyGenericSecret
Specific	configFilePrivacySpecificSecret

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F. All other characters are not supported.

Each character encodes 4 bits of the key. For instance, a 32-bit key requires 8 characters.

- If you enter too many bits, the key is truncated to the first 448 bits.
- If you do not enter enough bits, the key is padded with zeros.

For instance, a 32-bit key could look like the following: A36CB299.

This key must match the key used for the encryption of the relevant configuration file.

If the variable is empty, the configuration file is not decrypted.

2. Set the *configFilePrivacyEnable* variable to **enable**.
The Mediatrix 4102 will be able to decrypt the next encrypted generic or specific configuration file. If this variable is set to **disable**, the configuration file is not decrypted by the unit and the configuration update fails.

Configuration Download via TFTP

The following steps explain how to download configuration files by using the TFTP protocol.



Note: The configuration download via TFTP can only traverse NATs of types “Full Cone” or “Restricted Cone”. If the NAT you are using is of type “Port Restricted Cone” or “Symmetric”, the file transfer will not work.

► To download configuration files via TFTP:

1. Set the configuration file server host and port as defined in [“Configuration File Server Settings” on page 131](#).
2. Place the configuration files to download on the computer hosting the TFTP server. These files must be in a directory under the TFTP root path.
3. If not already done, set the configuration file path as described in [“Setting up the Configuration File Download” on page 133](#).
4. In the *configFileFetchingMIB*, set the *configFileTransferProtocol* variable to **tftp**.
5. In the *groupAdminMIB*, set the *groupSetAdmin* variable to **ForceLock**.
All activities in progress on the Mediatix 4102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is “locked”). The configuration file download may take place.
6. In the *sysAdminMIB*, initiate the configuration file download via TFTP by setting the *sysConfigCommand* variable to **updateConfiguration**.
The Mediatix 4102 immediately downloads the configuration files. It is the initiator of the TFTP sessions.

NAT Variations

NAT treatment of UDP varies among implementations. The four treatments are:

- Full Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.
- Restricted Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.
- Port Restricted Cone: Similar to a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.
- Symmetric: All requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

For more details on NAT treatments, refer to RFC 3489.

Configuration Download via HTTP

The following steps explain how to download the configuration files by using the HTTP protocol.

► **To download the configuration files via HTTP:**

1. Set the configuration file server host and port as defined in ["Configuration File Server Settings" on page 131](#).



Caution: When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *configFileFetchingPort* read-only variable (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See ["Configuration File Server Settings" on page 131](#) for more details.

2. Place the configuration files to download on the computer hosting the HTTP server.
These files must be in a directory under the root path.
3. If not already done, set the configuration file path as described in ["Setting up the Configuration File Download" on page 133](#).
4. In the *configFileFetchingMIB*, set the *configFileTransferProtocol* variable to **http**.
Your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.
5. If your HTTP server requires authentication when downloading the configuration file, set the following:
 - The user name in the *configFileTransferUsername* variable.
 - The password in the *configFileTransferPassword* variable.
6. In the *groupAdminMIB*, set the *groupSetAdmin* variable to **ForceLock**.
All activities in progress on the Mediatrix 4102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is "locked"). The configuration file download may take place.
7. In the *sysAdminMIB*, initiate the configuration file download via HTTP by setting the *sysConfigCommand* variable to **updateConfiguration**.
The Mediatrix 4102 immediately downloads the configuration files. It is the initiator of the HTTP sessions.

Automatic Configuration Update

You can configure the Mediatrix 4102 to automatically update its configuration. This update can be done:

- ▶ Every time the Mediatrix 4102 restarts.
- ▶ At a specific time interval you can define.

Automatic Update on Restart

The Mediatrix 4102 may download new configuration files each time it restarts.

▶ **To set the automatic update every time the Mediatrix 4102 restarts:**

1. Set the configuration file server host and port as defined in ["Configuration File Server Settings" on page 131](#).



Caution: When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See ["Configuration File Server Settings" on page 131](#) for more details.

2. Place the configuration files to download on the computer hosting the HTTP or TFTP server. These files must be in a directory under the root path.
3. If not already done, set the configuration file path as described in ["Setting up the Configuration File Download" on page 133](#).
4. In the *configFileFetchingMIB*, set the *configFileTransferProtocol* variable to either **http** or **tftp**.
If you are using the HTTP protocol to download the configuration, be aware that your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.
5. If you are using the HTTP protocol to download the configuration and your HTTP server requires authentication, set the following:
 - The user name in the *configFileTransferUsername* variable.
 - The password in the *configFileTransferPassword* variable.

The Mediatrix 4102 supports basic and digest HTTP authentication, as described in RFC 2617.
6. Set the *configFileAutoUpdateOnRestartEnable* variable to **enable** (in the *configFileAutomaticUpdate* group).
7. In the *sysConfigMIB*, set the *sysConfigDownloadConfigFile* variable to **automaticInitiateFileDownload**.

The automatic configuration update will be performed each time the Mediatrix 4102 restarts.

The unit configuration is only updated if at least one parameter value defined in the downloaded configuration files is different from the actual unit configuration.

Automatic Update at a Specific Time Interval

You can configure the Mediatrix 4102 to download new configuration files at a specific day and/or time.

► To set the automatic update at a specific time interval:

1. Set the configuration file server host and port as defined in ["Configuration File Server Settings" on page 131](#).



Caution: When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See ["Configuration File Server Settings" on page 131](#) for more details.

2. Place the configuration files to download on the computer hosting the HTTP or TFTP server. These files must be in a directory under the root path.
3. If not already done, set the configuration file path as described in ["Setting up the Configuration File Download" on page 133](#).
4. In the *configFileFetchingMIB*, set the *configFileTransferProtocol* variable to either **http** or **tftp**.
If you are using the HTTP protocol to download the configuration, be aware that your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.
5. If you are using the HTTP protocol to download the configuration and your HTTP server requires authentication, set the following:
 - The user name in the *configFileTransferUsername* variable.
 - The password in the *configFileTransferPassword* variable.

The Mediatrix 4102 supports basic and digest HTTP authentication, as described in RFC 2617.
6. Define the time base for automatic configuration updates in the *configFileAutoUpdateTimeUnit* variable (in the *configFileAutomaticUpdate* group).

You have the following choices:

Table 96: Time Unit Parameters

Parameter	Description
minutes	Updates the unit's configuration every x minutes. You can specify the x value in the variable <i>configFileAutoUpdatePeriod</i> (see Step 7).
hours	Updates the unit's configuration every x hours. You can specify the x value in the variable <i>configFileAutoUpdatePeriod</i> (see Step 7).
days	Updates the unit's configuration every x days. You can specify the x value in the variable <i>configFileAutoUpdatePeriod</i> (see Step 7). You can also define the time of day when to perform the update in the <i>configFileAutoUpdateTimeOfDay</i> variable (see Step 8).

7. Set the waiting period between each configuration update in the *configFileAutoUpdatePeriod* variable.
The time unit for the period is specified by the *configFileAutoUpdateTimeUnit* variable (see Step 6). Available values are from 1 to 48.
8. If you have selected **days** in Step 6, set the time of the day when to initiate a configuration update in the *configFileAutoUpdateTimeRange* variable.
The time of the day is based on the *sntpTimeZoneString* variable setting (see ["Chapter 16 - SNTP Settings" on page 189](#) for more details).

You must have a time server SNTP that is accessible and properly configured, or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to [“Chapter 16 - SNTP Settings” on page 189](#) for more details on how to configure the Mediatrix 4102 for a SNTP server.

If a time range is specified, the unit will download the configuration files at a random time within the interval specified.

The format should be one of the following:

```
hh[:mm[:ss]]
hh[:mm[:ss]] - hh[:mm[:ss]]
```

Where:

hh: Hours.
mm: Minutes.
ss: Seconds.

The configuration files are downloaded at the first occurrence of this value and thereafter with a period defined by the *configFileAutoUpdatePeriod* variable. Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the time range is set to '14:00 - 15:00' and the automatic unit configuration update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day.

9. Set the *configFileAutoUpdatePeriodicEnable* variable to **enable**.
10. In the *sysConfigMIB*, set the *sysConfigDownloadConfigFile* variable to **automaticInitiateFileDownload**.

The unit configuration is only updated if at least one parameter value defined in the downloaded configuration files is different from the actual unit configuration.

If one of the telephones/faxes is off-hook, the Mediatrix 4102 will perform the update 5 minutes after both ports are detected on-hook.

Error Handling

The following configuration file fetching service error sources are divided in three types depending on the transfer protocol: common errors (Table 35), TFTP errors (Table 36) and HTTP errors (Table 37). The error cause and the unit behaviour are also described.

Table 97: Configuration File Fetching Error Handling

Error Type	Cause	Behaviour
Common Error Handling		
Invalid file format	The file format is not valid.	Send a syslog warning message including the file location/name with the transfer server address: The fetched configuration file “XXX”, from server “XXX”, has an invalid format. No recorded settings applied.
Empty file	Committing an empty file.	Send a syslog warning message including the file location/name with the transfer server address: The fetched configuration file “XXX”, from server “XXX”, is empty.

Table 97: Configuration File Fetching Error Handling (Continued)

Error Type	Cause	Behaviour
Invalid file content	The file contains invalid characters. Allowed characters are ASCII codes 10 (LF), 13(CR), and 32 to 126.	Send a syslog warning message including the file location/name, the transfer server address and the invalid character (ASCII code): The fetched configuration file "XXX", from server "XXX", has an invalid character "ASCII code XXX". No recorded settings applied.
Invalid transfer server address	The server address is not valid.	Send a syslog warning message including the transfer server address: No configuration file is fetched because the server host "XXX" is invalid. Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> .
File size too big	Downloading a file with a size exceeding 512000 bytes.	Send a syslog warning message including the file location/name, the transfer server address, the file size and the maximum allowed size: The fetched configuration file "XXX", from server "XXX", has a size "XXX bytes" that exceeds the maximum allowed size "XXX bytes". Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> .
Invalid encryption	The configuration file cannot be decrypted. A badly encrypted file is detected if the header or the padding is invalid.	Send a syslog warning message including the file location/name and the transfer server address: The fetched configuration file \"%s\", from server \"%s\", can not be decrypted.
TFTP-Specific Error Handling		
File not found	Received error code 1 (file not found) from the TFTP server.	Send a syslog warning message including the file name and location with the TFTP server address: The configuration file "XXX" was not found on the TFTP server "XXX". Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> .
Access violation	Received error code 2 (access violation) from the TFTP server.	Send a syslog warning message including the file name and location with the TFTP server address: The configuration file "XXX" was not fetched. There was a TFTP access violation with server "XXX". Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> .
Connection timeout	No answer from the TFTP server. The time elapsed since the TFTP request was sent exceeds 32 seconds.	Send a syslog warning message including the file name and location with the TFTP server address: The configuration file "XXX" was not fetched. The TFTP connection with server "XXX" timed out. Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> .

Table 97: Configuration File Fetching Error Handling (Continued)

Error Type	Cause	Behaviour
Transfer error	Received a TFTP error (other than error code 1 and 2) from the TFTP server.	Send a syslog warning message including the file name and location with the TFTP server address: Error in the TFTP transfer of the configuration file "XXX" from host "XXX" and port number XXX. Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .
File size too big	Downloading a file with a size exceeding 512000 bytes.	Abort the transfer by sending error code 3 (disk full or allocation exceeded) to the TFTP client.
HTTP-Specific Error Handling		
Access unauthorized	Received a 401 Unauthorized from the HTTP server.	Send a syslog warning message including the file location/name with the HTTP server address: The access to configuration file "XXX" is unauthorized on HTTP server "XXX". Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .
File not found	Received a 404 Not Found from the HTTP server.	Send a syslog warning message including the file location/name with the HTTP server address: The configuration file "XXX" was not found on the HTTP server "XXX". Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .
Session timeout	No answer from the HTTP server. The time elapsed since the HTTP request was sent exceeds 15 seconds.	Send a syslog warning message including the file location/name with the HTTP server address: The configuration file "XXX" was not fetched. The HTTP session with server "XXX" timed out. Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .
Session closed by peer	The HTTP server closed the session.	Send a syslog warning message including the file location/name with the HTTP server address: The configuration file "XXX" HTTP transfer session was closed by peer: host "XXX". Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .
Transfer error	Received an HTTP error (other than 401 and 404) from the HTTP server.	Send a syslog warning message including the file location/name with the HTTP server address and port: Error in the HTTP transfer of the configuration file "XXX" from host "XXX" and port number XXX. Set <i>sysAdminDownloadConfigFileStatus</i> to <i>fail</i> .

Management Server

You can set the Mediatrix 4102 so that it asks the management server to send it a configuration file.



Note: Downloading a configuration file from the management server can only be performed through the TFTP protocol.

Management Server Configuration

To download a configuration file from the management server, you must setup the management server information as per ["Chapter 17 - Management Server Configuration" on page 193](#).

Downloading from the Management Server

Once the management server has been properly set up, you can define the configuration file download.



In the *Unit Manager Network Administration Manual*, refer to chapter *Performing Actions on Mediatrix Units*, section *Downloading a Configuration File*.

► To download the configuration file from the management server:

1. Place the configuration file on the computer hosting the management server.
2. In the *sysConfigMIB*, request a configuration file download by setting the *sysConfigDownloadConfigFile* variable to **requestFileDownload**.
3. Set the *sysConfigDownloadConfigMode* variable to **request**.

The Mediatrix 4102 sends a notification, *msTrapConfigInformation*, to the management server, via SNMP traps, to request the configuration file.

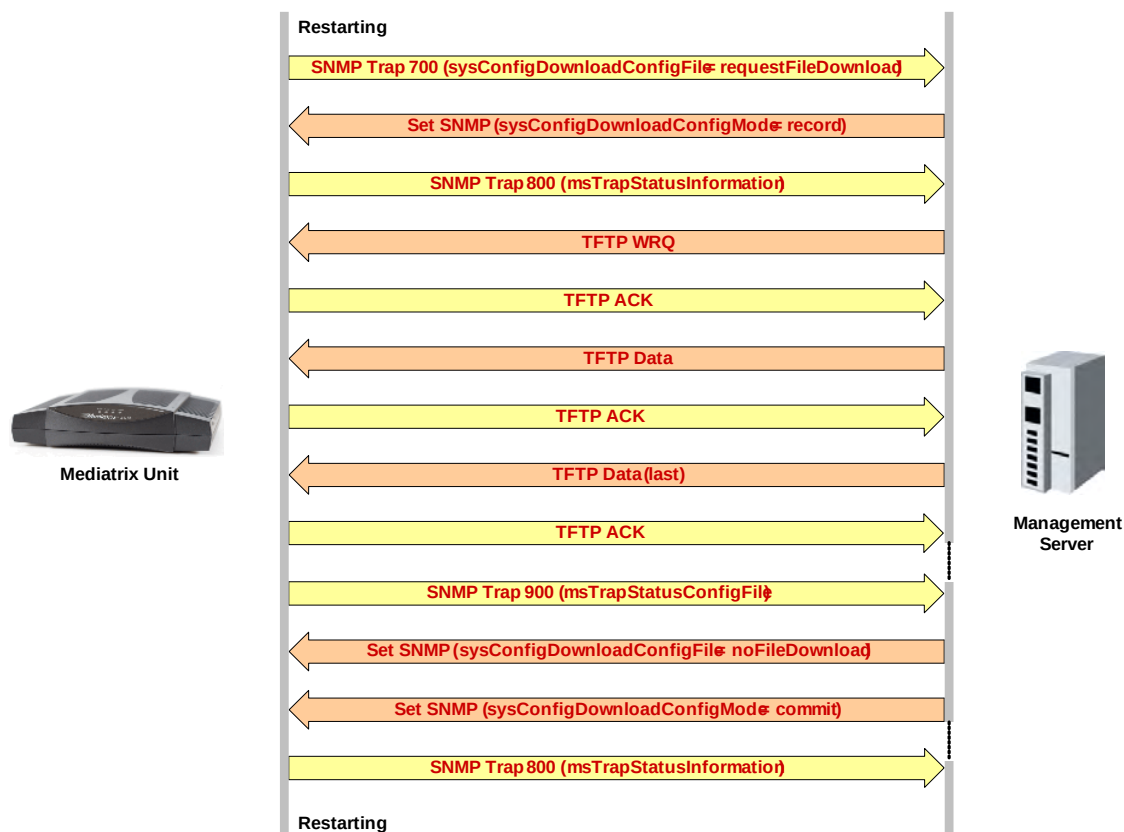
The management server then initiates the TFTP session and pushes the file into the unit.

If the management server is the Unit Manager Network from Media5, the following steps are automatically performed. If you are using another management server, you may have to perform them manually.

- a. The Unit Manager Network sets the *sysConfigDownloadConfigMode* variable to **record**.
- b. The Unit Manager Network sends the configuration file to the Mediatrix 4102.
- c. Once the configuration file has been sent, the Unit Manager Network sets the *sysConfigDownloadConfigFile* variable to **noFileDownload**.
- d. The Unit Manager Network sets the *sysConfigDownloadConfigMode* variable to **commit**.

If a valid configuration file is successfully downloaded, then the Mediatrix 4102 automatically restarts to apply all the new settings. If the Mediatrix 4102 does not restart, this could mean the download failed. In this case, you can query the status of the last configuration file download in the *sysAdminDownloadConfigFileStatus* variable:

- idle: No configuration file download has been performed yet.
- fail: The last configuration file download failed.
- success: The last configuration file download succeeded.
- inProgress: A configuration file download is in progress.
- listening: The unit is listening and waiting for a configuration file to be sent by the management server.

Figure 41: Configuration Sequence Update Using the Management Server

Error Handling

The following are possible error sources when updating the unit configuration using the management server. The error cause and the unit behaviour are also described.

Table 98: Configuration File Error Handling with the Management Server

Error Type	Cause	Behaviour
Empty file	Committing an empty file.	Send a syslog warning message including the file name and the TFTP client address: The configuration file "XXX" pushed to the unit by the TFTP client "XXX" is empty.
Invalid file content	Committing a file that contains invalid characters. Allowed characters are ASCII codes 10 (LF), 13(CR), and 32 to 126.	Send a syslog warning message including the file name, the TFTP client address and the invalid character (ASCII code): The configuration file "XXX" pushed to the unit by the TFTP client "XXX" has an invalid character "ASCII code XXX". No recorded settings applied.
Invalid file format	Committing a file with an invalid format.	Send a syslog warning message including the file name and the TFTP client address: The configuration file "XXX" pushed to the unit by the TFTP client "XXX" has an invalid format. No recorded settings applied.

Table 98: Configuration File Error Handling with the Management Server (Continued)

Error Type	Cause	Behaviour
File size too big	Downloading a file with a size exceeding 512000 bytes.	Send a syslog warning message including the file name, the TFTP client address, the file size and the maximum allowed size: The configuration file "XXX" from the TFTP client "XXX" is not downloaded because its size "XXX bytes" exceeds the maximum allowed size "XXX bytes". Send error code 3 (disk full or allocation exceeded) to the TFTP client. Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> and send <code>msTrapStatusConfigFile</code> .
TFTP transfer error	Received a TFTP error from the TFTP client.	Send a syslog warning message including the file name and the TFTP client address: Error in the TFTP transfer of the configuration file "XXX" from the TFTP client "XXX". Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> and send <code>msTrapStatusConfigFile</code> .
TFTP transfer aborted	The transfer was aborted while in progress by changing the value of <code>sysConfigDownloadConfigMode</code> or <code>sysConfigDownloadConfigFile</code> .	Send a syslog warning message including the file name and the TFTP client address: The TFTP transfer of the configuration file "XXX" from the TFTP client "XXX" was aborted. Set <code>sysAdminDownloadConfigFileStatus</code> to <i>fail</i> and send <code>msTrapStatusConfigFile</code> .
File pulling not allowed	A TFTP client is trying to read a file from the unit.	Send a syslog informational message including the file name and the TFTP client address: The TFTP client "XXX" is trying to pull the file "XXX" from the unit. This is not allowed. Send error code 2 (access violation) to the TFTP client.

Syslog Messages

A syslog message is sent whenever it is impossible for the management server to download a configuration file or when it is impossible to apply the new settings to the unit.

Table 99: Syslog Messages Using the Management Server

Level	Message	Event
Warning	The notification "XXX" could not be sent to <code>msHost</code> "XXX" and <code>msTrapPort</code> XXX.	A SNMP trap could not be sent to the management server. The syslog warning message includes the SNMP trap number, the management server address and port.
Informational	Parameter values defined in the configuration file were successfully committed. Restarting the unit...	A downloaded configuration file was successfully committed.
Warning	None of the parameter values defined in the configuration file was successfully committed.	No parameter value from the downloaded configuration file was successfully applied (e.g., because of bad OIDs).

Configuration File Example

The configuration file format uses XML (eXtensible Markup Language). The following is the accepted format:

```
<MX_Config_File FileId="MX_MIBFILE" MIBVersionNumber="" VersionNumber="1.0">
  <Object Prefix="" Suffix="" Value=""/>
  <Object Prefix="" Suffix="" Value=""/>
</MX_Config_File>
```

The following is an example of a configuration file:

```
<MX_Config_File FileId="MX_MIBFILE" MIBVersionNumber="1.0" VersionNumber="1.0">
  <Object Prefix="1.3.6.1.4.1.4935.15.1.8.1" Suffix="0" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.1.10.1" Suffix="0" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.1.10.10.1" Suffix="0" Value="192.168.0.10"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.1.20.1" Suffix="0" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.3.1.30.1" Suffix="0" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.3.1.30.3" Suffix="0" Value="ConfigFile.xml"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.15.1.5" Suffix="0" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.35.1.20.1.1" Suffix="3" Value="0"/>
  <Object Prefix="1.3.6.1.4.1.4935.15.35.1.20.1.1" Suffix="4" Value="0"/>
</MX_Config_File>
```

Supported Characters

When creating and/or editing a configuration file, the following ASCII codes are supported:

10 LF, line feed	62 >, greater than	94 ^, caret
13 CR, carriage return	63 ?, question mark	95 _, underscore
32 space	64 @, commercial at	96 `, back quote
33 !, exclamation mark	65 A	97 a
34 ", double quote	66 B	98 b
35 #, hash	67 C	99 c
36 \$, dollar	68 D	100 d
37 %, percent	69 E	101 e
38 &, ampersand	70 F	102 f
39 ', quote	71 G	103 g
40 (, open parenthesis	72 H	104 h
41), close parenthesis	73 I	105 i
42 *, asterisk	74 J	106 j
43 +, plus	75 K	107 k
44 ,, comma	76 L	108 l
45 -, minus	77 M	109 m
46 ., full stop	78 N	110 n
47 /, oblique stroke	79 O	111 o
48 0, zero	80 P	112 p
49 1	81 Q	113 q
50 2	82 R	114 r
51 3	83 S	115 s
52 4	84 T	116 t
53 5	85 U	117 u
54 6	86 V	118 v
55 7	87 W	119 w
56 8	88 X	120 x
57 9	89 Y	121 y
58 :, colon	90 Z	122 z
59 ;, semicolon	91 [, open square bracket	123 {, open curly bracket
60 <, less than	92 \, backslash	124 , vertical bar
61 =, equals	93], close square bracket	125 }, close curly bracket
		126 ~, tilde

All other ASCII codes will result in an invalid configuration file.

Software Download

This chapter describes how to download a software version available on the designated software server into the Mediatrix 4102.

You have the choice to perform the software download by using the TFTP or HTTP protocol. You can also configure the Mediatrix 4102 to automatically update its software version.



Note: You can only perform a software download from the WAN interface of the Mediatrix 4102. Software downloads from the LAN side are not supported.

Before Downloading

To download a software, you may need to setup the following applications on your computer:

- ▶ TFTP server with proper root path
- ▶ MIB browser (with the current Mediatrix 4102 MIB tree)
You can use the MIB browser built in the Media5's Unit Manager Network. See ["Unit Manager Network – Element Management System" on page xvii](#) for more details.
- ▶ Software upgrade zip file
- ▶ SNTP server properly configured
- ▶ HTTP server with proper root path
- ▶ Syslog daemon (optional)

Configuring the TFTP Server

If you are to perform a software download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server. This PC must not have a firewall running. Media5 also recommends to place the PC and the Mediatrix 4102 in the same subnet.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

If you are to use the automatic software update feature (see ["Automatic Software Update" on page 158](#) for more details), you must have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to ["Chapter 16 - SNTP Settings" on page 189](#) for more details on how to configure the Mediatrix 4102 for a SNTP server.

Configuring the HTTP Server

If you are to perform a software download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. This PC must not have a firewall running. Media5 also recommends to place the PC and the Mediatrix 4102 in the same subnet.

It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Software Servers Configuration

The Mediatrix 4102 must know the IP address and port number of its Primary and Secondary software servers. These servers contain the files required for the software update. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself in static variables.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Software and Emergency Download*.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable (under the *ipAddressConfigImage* group).
This variable defines whether the Mediatrix 4102 must ask for its Image server settings through a DHCP server or not.
2. Set the *imageSelectConfigSource* variable to **dhcp**.
You can query the Image server's IP address and port number assigned by the DHCP server in the following read-only variables (in the *ipAddressStatus* folder):
 - *imagePrimaryHost*
 - *imagePrimaryPort*
 - *imageSecondaryHost*
 - *imageSecondaryPort*
3. Set how you want to define the Primary Image server information in the DHCP server.

Table 100: Primary Image Server DHCP Information

To use a...	Set...
vendor specific code	The <i>imageDhcpPrimarySiteSpecificCode</i> variable to 0 . Set the Primary image server IP address in the DHCP server inside the vendor specific sub-option 117 (hexadecimal 0x75).
site specific code	The <i>imageDhcpPrimarySiteSpecificCode</i> variable to any value between 128 and 254. Set the Primary image server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>imageDhcpPrimarySiteSpecificCode</i> variable in the unit's configuration).

See [“Vendor and Site Specific DHCP Options” on page 67](#) for more details.

4. Set how you want to define the Secondary Image server information in the DHCP server.

Table 101: Secondary Image Server DHCP Information

To use a...	Set...
vendor specific code	The <i>imageDhcpSecondarySiteSpecificCode</i> variable to 0 . Set the Secondary image server IP address in the DHCP server inside the vendor specific sub-option 118 (hexadecimal 0x76).

Table 101: Secondary Image Server DHCP Information (Continued)

To use a...	Set...
site specific code	The <i>imageDhcpSecondarySiteSpecificCode</i> variable to any value between 128 and 254. Set the Secondary image server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>imageDhcpPrimarySiteSpecificCode</i> variable in the unit's configuration).

See ["Vendor and Site Specific DHCP Options" on page 67](#) for more details.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► To use static information:

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable.
This variable defines whether the Mediatrix 4102 must ask for its Image server settings through a DHCP server or not.
2. Set the *imageSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 102: Image Static Information

Variable	Description
imageStaticPrimaryHost	Static primary image server IP address or domain name. This is the current address of the PC that hosts the files required for the download (extracted from the zip file). Default Value: 192.168.0.10
imageStaticPrimaryPort	Static primary image server IP port number. Default Value: 69
imageStaticSecondary Host	Static secondary image server IP address or domain name. This is the current address of the PC that hosts the files required for the download (extracted from the zip file). Default Value: 192.168.0.10
imageStaticSecondaryPort	Static secondary image server IP port number. Default Value: 69

The default port value complies to RFC 1340 on the well-known ports (assigned numbers). This value (69) applies to a TFTP server. It may be different for other servers. If you are using an HTTP server, you must change the port value to 80.

Download Procedure

The following describes how to download a software version into the Mediatrix 4102.



Note: Configuration settings are not lost when upgrading the software to a newer version. However, configuration settings may be lost if you upload an older firmware to the device. See [“Software Downgrade” on page 160](#) for more details.

You have the choice to perform the software download by using the TFTP or HTTP protocol. You can also configure the Mediatrix 4102 to automatically update its software version.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Software and Emergency Download*.



Note: You can only perform a software download from the WAN interface of the Mediatrix 4102. Software downloads from the LAN side are not supported.

Extracting the Zip File

The zip file contains the software information required for the download.

Extract the contents of the zip file on the PC designated as the software file server. Be sure to use the defined folder name. This creates a directory that contains the files required for the Mediatrix 4102 to properly update its software.

The directory name must be the same as the name defined in the *imageLocation* or *imageSelectionFileLocation* variable of the *imageMIB*. See [“Setting up the Image Path” on page 152](#) for more details.

Media5 suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

This directory must be located under the root path as defined in the TFTP/HTTP server or the software download will not proceed.

Setting up the Image Path

When performing a software download, you must configure the path, on the remote image server, of the directory where you extracted the files required for the download. This applies to both the manual or automatic download procedure, using the HTTP or TFTP protocol.

The directory must be located under the root path, as defined in the TFTP or HTTP server, or the software download will not proceed. See [“Before Downloading” on page 149](#) for more details.

The Mediatrix 4102 first downloads a file called “setup.inf”. This file contains the list of all the other files to download, depending on the product. The “setup.inf” file and all the other files must be in the same directory. If any of the files is missing, the procedure will not work properly.

► To setup the Image path:

1. In the *imageMIB*, select where to get the image location in the *imageLocationProvisionSource* variable.

You have the following choices:

Table 103: Image Location Parameters

Parameter	Description
static	Uses the directory specified in the <i>imageLocation</i> variable (see Step 2).
remoteFile	The image location is defined in a file called “mediatrix4102targetimage.inf”. The location of this file is defined in the <i>imageSelectionFileLocation</i> variable. This is useful if you are using automatic updates with multiple units (see Step 3).

2. If you have set the *imageLocationProvisionSource* variable to **static** (see Step 1), configure the path in the *imageLocation* variable.
This is the location of the “setup.inf” file that contains the list of the files to download into the Mediatrix 4102. The “setup.inf” file and all the other files must be in the same directory. In other words, this is the path from the root TFTP/HTTP folder down to the files extracted from the zip file. Note that the path must contain a maximum of 63 characters.
3. If you have set the *imageLocationProvisionSource* variable to **remoteFile** (see Step 1):
 - a. Create a text file and write the path and/or name of the directory that contains the files required for download. Save this file as “mediatrix4102targetimage.inf” under the server root path.



Note: If you leave the file empty, the Mediatrix 4102 will look for the software download information in the root directory of the image server.

- b. Configure the path of the “mediatrix4102targetimage.inf” file in the *imageSelectionFileLocation* variable.

Note that the selection file name is in lower case. Some web servers are case sensitive. The path must contain a maximum of 63 characters.

This is useful if you are using automatic updates with multiple units. If you want the units to download a new version, you only have to change the path once in the “mediatrix4102targetimage.inf” file. If you were to use the *imageLocation* variable, you would have to change the path in every unit.

Let's consider the following example:

- ▶ The directory that contains the files required for download is called: **MGCP_v5.0.1.1_MX-M5001-01**.
- ▶ This directory is under **C:/Root/Download**.

Table 104: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	MGCP_v5.0.1.1_MX-M5001-01
c:/	root/download/MGCP_v5.0.1.1_MX-M5001-01
c:/root	download/MGCP_v5.0.1.1_MX-M5001-01

The following are some tips to help your download process:

- ▶ Use the “/” character when defining the path to indicate sub-directories. For instance, *root/download*.
If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, use the “\” character.
- ▶ Use basic directory names, without spaces or special characters such as “~”, “@”, etc., which may cause problems.
- ▶ Cut and paste the path and/or name of the directory that contains the extracted files into the image path of the Mediatrix 4102 (you may have to convert “\” into “/”) to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

Software Download Status

You can validate the status of the software download in various ways.

Syslog Messages

If you are using a Syslog daemon, you will receive messages that inform you of the software update status. The following are the syslog messages the Mediatrix 4102 sends:

Table 105: Software Update Syslog Messages

Level	Message	Event
General Messages		
Informational	The software update succeeded.	The software update has been successful.
Error	The software update failed.	The software update experienced an error and has not been completed.
Error	The software update failed (xxx).	An error occurs when updating the software, internal error code provided.
Warning	Primary image server not specified, cannot download file: xxx	This error occurs when an image download is initiated and no domain name or address is specified for the primary image server.
Warning	Secondary image server not specified, cannot download file: xxx.	When a request involving the primary server fails, the secondary server is tried. This error occurs when there is no address or domain name specified for the secondary image server.
Error	Cannot resolve address of image server: xxx.	A DNS request failed to resolve the domain name of the image server (primary or secondary).
Error	Target image at location: xxx from host: xxx is invalid or corrupted.	For periodic and automatic updates, the target image to download is first compared with the installed image. This error occurs when this comparison failed because of corruption in the target image files.
Informational	Image download transfer initiated.	When manual, periodic or "at restart" image download is initiated.
Warning	The file: xxx from host: xxx exceeds the size limit.	The selection file or "setup.inf" file received exceeds 10000 bytes.
Informational	Target image at location: xxx from host xxx is identical to currently installed image. Transfer aborted.	For periodic and automatic updates, the target image to download is first compared with the installed image. This message occurs when this comparison determined that the target image is identical to the installed image.
Error	Image does not support hardware (error %d)	The software download failed because the software image is not compatible with the hardware.
HTTP-Specific Messages		
Warning	HTTP image transfer of file: xxx from host: xxx was closed by peer.	The HTTP transfer was closed by the peer.

Table 105: Software Update Syslog Messages (Continued)

Level	Message	Event
Warning	HTTP image transfer of file: xxx from host: xxx was closed due to unsupported or malformed response from the host.	In the HTTP response, one of the following error occurred: - The protocol version is not 1.0 or 1.1. - Some field or line is not properly formatted. - The trailing <crLf> is not present at the end of the header. - Unsupported kind of response.
Warning	HTTP image transfer of file: xxx from host: xxx was refused because of a malformed or incompatible request.	When receiving HTTP response #400 or #403.
Warning	HTTP image transfer of file: xxx from host: xxx was refused because of a server error.	When receiving HTTP response #500 or #501.
Warning	HTTP image transfer of file: xxx from host: xxx was refused because service is unavailable.	When receiving HTTP response #503.
TFTP-Specific Messages		
Warning	Image transfer of file: xxx from host: xxx and port: xxx was closed due to unexpected error	Unexpected error, either internal or on a TFTP or HTTP connection.
Warning	Image transfer of file: xxx from host: xxx port: xxx was closed after timeout	When not receiving TFTP packets for 32 seconds or not receiving a HTTP packet for 15 seconds.
Warning	Image transfer. File: xxx not found on host: xxx	When receiving TFTP error "NOT FOUND" or HTTP response #404.
Warning	Image transfer. Access to file: xxx on host: xxx is unauthorized	When receiving TFTP error "ACCESS" or HTTP response #401.

If the local syslog messages are enabled (see ["Local Syslog" on page 204](#) for more details), you can view these messages on the web interface.

LED States

When the Mediatrix 4102 initiates a software download, the LEDs located on the front panel indicate the status of the process.

Table 106: LED States in Software Download

Event	LED State
Image downloading and writing	<i>Power, LAN, In Use and Ready</i> LEDs blink alternately at 1 Hz with 1/4 ON duty cycle. Warning: Do not turn the Mediatrix 4102 off while in this state.
Image download failed	<i>Power, LAN, In Use and Ready</i> LEDs blink at the same time at 2 Hz with 50% ON duty cycle for 4 seconds.

See ["LED Indicators" on page 16](#) for a detailed description of the LED patterns related to the software download process.

MIB Variable

You can validate the result of the last software update by checking the state of the `sysAdminLastDownloadSoftware` MIB variable.

Download via TFTP

The following steps explain how to download a software by using the TFTP protocol.



In the *Unit Manager Network Administration Manual*, refer to chapter *Performing Actions on Mediatrix Units*, section *Downloading a Software Version*.

► To download a software via TFTP:

1. If not already done, setup the Image server used to download the software (see [“Before Downloading” on page 149](#)).
2. Be sure that UDP ports 60000 to 60512 inclusively are opened in your firewall.
3. If not already done, configure the Image path as described in [“Setting up the Image Path” on page 152](#).
4. If not already done, configure the image hosts and ports as defined in [“Software Servers Configuration” on page 150](#).
5. Set the TFTP root path in your TFTP server.
It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.
6. Set the `imageTransferProtocol` variable to **tftp**.
7. Set the `groupSetAdmin` variable (in the `groupAdminMIB`) to **ForceLock**.
All activities in progress on the Mediatrix 4102 are terminated immediately and the unit enters the maintenance mode (the value of the `groupAdminState` variable is “locked”). The software upgrade may take place.
The Mediatrix 4102 lines will be unlocked after successfully downloading the software and restarting. If, for any reason, the software download is not successful, you must manually unlock the lines as per [“Lines Administrative State” on page 163](#).
8. Initiate the download by setting the `sysAdminCommand` variable (in the `sysAdminMIB`) to **downloadSoftware**.
This starts the download process.



Caution: Never shutdown the Mediatrix 4102 manually while in the download process, because the image may be partially written and the Mediatrix 4102 is unable to restart.

The software download may take several minutes, depending on your Internet connection, network conditions and servers conditions.

If Transparent Address Sharing is enabled during the software download, the PC connected to the Mediatrix 4102 may experience momentary loss of Internet connectivity.

9. Update the MIB browser with the MIB version coming with the software version.

Download via HTTP

The following steps explain how to download a software by using the HTTP protocol.

► **To download a software via HTTP:**

1. If not already done, setup the Image server used to download the software (see [“Before Downloading” on page 149](#)).
2. If not already done, configure the Image path as described in [“Setting up the Image Path” on page 152](#).
3. If not already done, configure the image hosts and ports as defined in [“Software Servers Configuration” on page 150](#).



Caution: When downloading via HTTP, the image server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See [“Software Servers Configuration” on page 150](#) for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to **http**.
Your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.
5. If your HTTP server requires authentication, set the following:
 - The user name in the *imageTransferUsername* variable.
 - The password in the *imageTransferPassword* variable.
6. Set the *groupSetAdmin* variable (in the *groupAdminMIB*) to **ForceLock**.
All activities in progress on the Mediatrix 4102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is “locked”). The software upgrade may take place.
The Mediatrix 4102 lines will be unlocked after successfully downloading the software and restarting.
If, for any reason, the software download is not successful, you must manually unlock the lines as per [“Lines Administrative State” on page 163](#).
7. Initiate the download by setting the *sysAdminCommand* variable (in the *sysAdminMIB*) to **downloadSoftware**.
This starts the download process.



Caution: Never shutdown the Mediatrix 4102 manually while in the download process, because the image may be partially written and the Mediatrix 4102 is unable to restart.

The software download may take several minutes, depending on your Internet connection, network conditions and servers conditions.

If Transparent Address Sharing is enabled during the software download, the PC connected to the Mediatrix 4102 may experience momentary loss of Internet connectivity.

8. Update the MIB browser with the MIB version coming with the software version.

Automatic Software Update

You can configure the Mediatix 4102 to automatically update its software version. This update can be done:

- ▶ Every time the Mediatix 4102 restarts.
- ▶ At a specific time interval you can define.

Automatic Update on Restart

The Mediatix 4102 may download a new software version each time it restarts.

▶ **To set the automatic update every time the Mediatix 4102 restarts:**

1. If not already done, setup the Image server used to download the software (see [“Before Downloading” on page 149](#)).
2. If not already done, configure the Image path as described in [“Setting up the Image Path” on page 152](#).
3. If not already done, configure the image hosts and ports as defined in [“Software Servers Configuration” on page 150](#).



Caution: When downloading via HTTP, the image server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See [“Software Servers Configuration” on page 150](#) for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to either **http** or **fttp**.
If you are using the HTTP protocol to download the software, be aware that your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.
5. If you are using the HTTP protocol and your HTTP server requires authentication, set the following:
 - The user name in the *imageTransferUsername* variable.
 - The password in the *imageTransferPassword* variable.
6. Set the *imageAutoUpdateOnRestartEnable* variable to **enable**.
7. Set the *imageAutoUpdateEnable* variable to **enable**.
The automatic software update will be performed each time the Mediatix 4102 restarts.

Automatic Update at a Specific Time Interval

You can configure the Mediatix 4102 to download a software version at a specific day and/or time.

▶ **To set the automatic update at a specific time interval:**

1. If not already done, setup the Image server used to download the software (see [“Before Downloading” on page 149](#)).
2. If not already done, configure the Image path as described in [“Setting up the Image Path” on page 152](#).

3. If not already done, configure the image hosts and ports as defined in [“Software Servers Configuration” on page 150](#).



Caution: When downloading via HTTP, the image server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See [“Software Servers Configuration” on page 150](#) for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to either **http** or **tftp**.
If you are using the HTTP protocol to download the software, be aware that your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.
5. If you are using the HTTP protocol and your HTTP server requires authentication, set the following:
 - The user name in the *imageTransferUsername* variable.
 - The password in the *imageTransferPassword* variable.
6. Define the time base for automatic software updates in the *imageAutoUpdateTimeUnit* variable (in the *imageAutomaticUpdate* group).
You have the following choices:

Table 107: Time Unit Parameters

Parameter	Description
minutes	Updates the software every x minutes. You can specify the x value in the variable <i>imageAutoUpdatePeriod</i> (see Step 7).
hours	Updates the software every x hours. You can specify the x value in the variable <i>imageAutoUpdatePeriod</i> (see Step 7).
days	Updates the software every x days. You can specify the x value in the variable <i>imageAutoUpdatePeriod</i> (see Step 7). You can also define the time of day when to perform the update in the <i>imageAutoUpdateTimeRange</i> variable (see Step 8).

7. Set the waiting period between each software update in the *imageAutoUpdatePeriod* variable.
The time unit for the period is specified by the *imageAutoUpdateTimeUnit* variable (see Step 6). Available values are from 1 to 48.
8. If you have selected **days** in Step 6, set the time of the day when to initiate a software update in the *imageAutoUpdateTimeRange* variable.
The time of the day is based on the *sntpTimeZoneString* variable setting (see [“Chapter 16 - SNTP Settings” on page 189](#) for more details).
You must have a time server SNTP that is accessible and properly configured, or the automatic software update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to [“Chapter 16 - SNTP Settings” on page 189](#) for more details on how to configure the Mediatrix 4102 for a SNTP server.
If a time range is specified, the unit will initiate the image software download at a random time within the interval specified.

The format should be one of the following:

```
hh[:mm[:ss]]
hh[:mm[:ss]] - hh[:mm[:ss]]
```

Where:

hh: Hours.
mm: Minutes.

ss: Seconds.

The image software download is initiated at the first occurrence of this value and thereafter with a period defined by *imageAutoUpdatePeriod*. Let's say for instance the automatic update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the time range is set to '14:00 - 15:00' and the automatic update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day.

9. Set the *imageAutoUpdateEnable* variable to **enable**.

If one of the telephones/faxes is off-hook, the Mediatrix 4102 will perform the download five minutes after both ports are detected on-hook.

Software Downgrade

It is possible to downgrade a Mediatrix 4102 from the current version (for instance, v5.0rx.x) to an older version (for instance, v4.4rx.x).



Note: If you perform a default reset on the Mediatrix 4102, you must download the current version into the unit before performing the software downgrade procedure.

► To perform a software downgrade:

1. Create, in a common folder under the TFTP root path, the current (for instance, v5.0) and older (for instance, v4.4) applications folders.
2. Re-update the Mediatrix 4102 with the current application.
The Mediatrix 4102 runs the current software version (v5.0rx.x).
3. Perform the software downgrade to the older application (v4.4rx.x) as described in ["Download Procedure" on page 152](#).

Emergency Software Procedure

If the software download is suddenly interrupted, it may not be complete. Without any protection against this situation, the Mediatrix 4102 is not functional.

A transfer may be interrupted for the following reasons:

- An electrical shortage.
- The user of the Mediatrix 4102 can accidentally power off the unit.

Depending on the moment when the software download has been interrupted, the emergency software procedure (also called rescue application) can automatically start a new software download to repair the software if it has been corrupted by the interruption. However, there is a small but critical time frame during which unrecoverable errors could happen. This is why it is very important that the unit is not turned off during software downloads.

Using the Emergency Software

When the emergency software procedure starts, the following steps apply:

1. The Mediatrix 4102 tries to initiate the software download with the primary software server.
2. If the software download fails with the primary software server, the Mediatrix 4102 tries to initiate the software download with the secondary software server.

3. If the primary and the secondary servers cannot be reached, the Mediatrix 4102 tries two default servers: 192.168.0.10 and then 192.168.0.2.
If, for some reason, it is impossible to rescue the unit by using the primary and secondary servers, setting up a server at one of these addresses within the correct subnet will provide an ultimate way to rescue the unit. However, if these addresses cannot be reached from the unit's subnet, the default gateway must provide appropriate routing to them.
4. If the software download also fails with the two default servers, the Mediatrix 4102 idles for one minute.
5. After this one minute, the Mediatrix 4102 tries to initiate the software download again.
6. If the software download fails again with the primary, secondary, and default software servers, the Mediatrix 4102 idles for two minutes before attempting to initiate the software download.
7. If the emergency software download still fails, the Mediatrix 4102 tries to initiate the software download again by doubling the delay between each attempt up to a maximum of 16 minutes:
 - first attempt: 1 minute delay
 - second attempt: 2 minutes delay
 - third attempt: 4 minutes delay
 - fourth attempt: 8 minutes delay
 - fifth attempt: 16 minutes delay
 - sixth attempt: 16 minutes delay
 - etc.

This procedure continues until the software download completes successfully. The software download can fail if the software server cannot be reached or if the software directory is not found on the software server.

This chapter describes the features available on the lines connected to the Mediatrix 4102.

For information on voice codecs, see [“Chapter 13 - Voice Transmissions” on page 167](#).

For information on data codecs, see [“Chapter 14 - Fax Transmission” on page 181](#).

Lines Administrative State

You can independently set the administrative state of each analog line of your Mediatrix 4102. This state determines how the Mediatrix 4102 processes calls.

For instance, you must properly unlock the two analog lines of the Mediatrix 4102 to properly make and receive calls on all of them.

The administrative states may be applied in two ways:

- ▶ **Temporary:** The administrative state is applied immediately, but it is not kept after the Mediatrix 4102 restarts.
- ▶ **Permanent:** When the Mediatrix 4102 restarts, it reads a MIB variable to determine the administrative state defined for each analog line.

Temporary Administrative State

You can set the administrative state of a line that will be kept until the Mediatrix 4102 restarts. Once the unit restarts, it uses the permanent state defined for each line. See [“Permanent Administrative State” on page 164](#) for more details.



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

▶ To set a temporary administrative state:

1. In the *ifAdminMIB*, locate the *ifAdminSetAdmin* variable.

This variable temporary locks/unlocks the selected line of the Mediatrix 4102. This state is kept until the unit restarts. It offers the following settings:

Table 108: Temporary Lock Settings

Setting	Description
unlock	Registers the line to the Call Agent.
lock	Cancels the line registration to the Call Agent. Active calls in progress remain established until normal call termination. No new calls may be initiated.
forcelock	Cancels the line registration to the Call Agent. All active calls in progress are terminated immediately. No new calls may be initiated.

Permanent Administrative State

The permanent administrative state is applied every time the Mediatix 4102 restarts.

► **To set a permanent administrative state:**

1. In the *ifAdminMIB*, locate the *ifAdminInitialAdminState* variable.
This variable indicates the administrative state the current analog line will have after the Mediatix 4102 restarts. It offers the following settings:

Table 109: Permanent Lock Settings

Setting	Description
unlocked	Registers the line to the Call Agent.
locked	The analog line is unavailable for normal operation. It cannot be used to make and/or receive calls.

Multiple Connections on Endpoints (Lines)

The Mediatix 4102 supports multiple connections on one endpoint. Under MGCP, it is now possible to create multiple connections on a single endpoint, as long as there is only one active connection at a time.

Flash Hook Detection

The 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.

The Mediatix 4102 allows you to set the minimum and maximum time within which pressing and releasing the plunger is actually considered a flash hook.

► **To set flash hook parameters:**

1. In the *fxsMIB*, set the following variables:

Table 110: Flash Hook Parameters

Variable	Description
<i>fxsFlashHookDetectionDelayMin</i>	Minimum time in ms the hook switch must remain pressed to perform a flash hook. Default Value: 100
<i>fxsFlashHookDetectionDelayMax</i>	Maximum time in ms the hook switch can remain pressed to perform a flash hook. Default Value: 1200

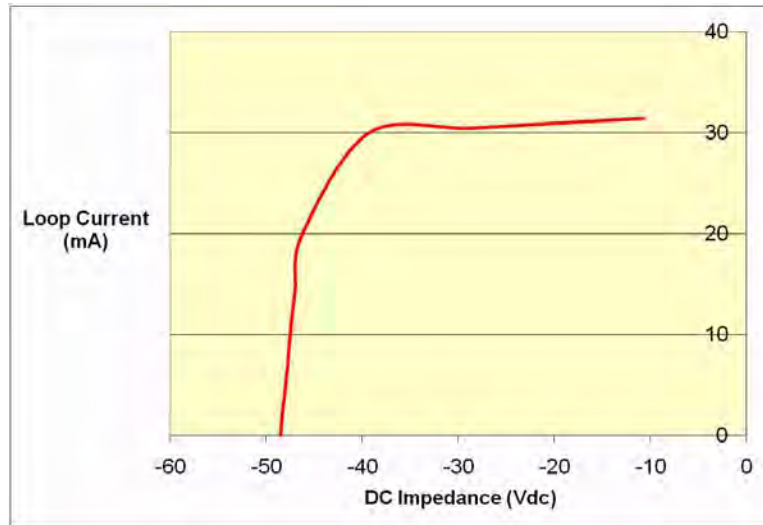
2. Restart the Mediatix 4102 so that the changes may take effect.

Loop Current

When one of its analog lines goes off-hook, the Mediatrix 4102 controls the line in a fixed loop current mode. The value of the loop current can be modified through the MIB.

Note that the actual measured current may be different than the value you set, because it varies depending on the DC impedance. This is illustrated in [Figure 42](#) for a loop current of 32 mA.

Figure 42: Loop Current vs Impedance – 32 mA



► **To set the loop current:**

1. In the *fxsMIB*, set the *fxsLoopCurrent* variable to the value you want to use. The loop current is in mA. The range of available values is from 20 mA to 32 mA. This value applies to all the endpoints of the Mediatrix 4102.
2. Restart the Mediatrix 4102 so that the changes may take effect.

When a remote end-user goes on-hook, the Mediatrix 4102 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 Mediatrix 4102 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.

This chapter describes the various codecs the Mediatrix 4102 supports for transmitting audio signals.

Codec Descriptions

The two lines of the Mediatrix 4102 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** line.

Table 111: Codecs Comparison

	Compression	Voice Quality
G.711	None	Excellent
G.726	Medium	Fair
G.729a/ab	High	Fair/Good

G.711 PCMA and PCMU

Specified in ITU-T Recommendation G.711. The audio data is encoded as 8 bits per sample, after logarithmic scaling. PCMU denotes μ -law scaling, PCMA A-law scaling.

Table 112: G.711 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. See “Packetization Time” on page 170 for more details.
Voice Activity Detection (VAD)	Can be enabled or disabled. When enabled, two levels of detection are available: transparent or conservative. See “G.711 and G.726 VAD” on page 176 for more details.
Comfort noise	Supports white and custom comfort noise as defined in <i>RFC 3389</i> . See “Comfort Noise” on page 178 for more details.

Analog Modem

The Mediatrix 4102 can send modem transmissions in clear channel (G.711). If configured adequately, modems with higher rate capabilities (for instance, V.90) will automatically fall back in the transmission range supported.

Currently, the Mediatrix 4102 does not NACK the modem tone request, but the modem tone request is not yet supported.

Quality of modem transmissions is dependent upon the system configuration, quality of the analog lines, as well as the number of analog-to-digital and digital-to-analog conversions. Modem performance may therefore be reduced below the optimum values stated above.

G.726

Specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec 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 113: G.726 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. The preferred is 20 ms. See "Packetization Time" on page 170 for more details.
Voice Activity Detection (VAD)	Uses the G.711 VAD settings. Can be enabled or disabled. When enabled, two levels of detection are available: transparent or conservative. See "G.711 and G.726 VAD" on page 176 for more details.
Comfort noise	Uses the G.711 comfort noise settings. Supports white and custom comfort noise as defined in RFC 3389. See "Comfort Noise" on page 178 for more details.

Analog Modem

The Mediatix 4102 can send modem transmissions in clear channel (G.726). If configured adequately, modems with higher rate capabilities (for instance, V.90) will automatically fall back in the transmission range supported

Currently, the Mediatix 4102 does not NACK the modem tone request, but the modem tone request is not yet supported.

Quality of modem transmissions is dependent upon the system configuration, quality of the analog lines, as well as the number of analog-to-digital and digital-to-analog conversions. Modem performance may therefore be reduced below the optimum values stated above.

G.729

Specified in ITU-T Recommendation G.729, coding of speech at 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP). For all data rates, the sampling frequency (and RTP timestamp clock rate) is 8000 Hz.

A voice activity detector (VAD) and comfort noise generator (CNG) algorithm in Annex B of G.729 is recommended for digital simultaneous voice and data applications; they can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B comfort noise frame occupies 2 octets.

The Mediatix 4102 supports G.729A and G.729AB for encoding and G.729, G.729A and G.729AB for decoding.

Table 114: G.729 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. See "Packetization Time" on page 170 for more details.
Voice Activity Detection (VAD)	The Mediatix 4102 supports the annex B. Annex B is the built-in support of VAD in G.729. See "G.729 VAD" on page 177 for more details.

Preferred Codec

The preferred codec is the codec you want to favour during negotiation.



Note: If the MGCP/NCS Call Agent provides a list of codecs (always in preference order), the preferred codec does not apply. In this case, the preferred codec of the Call Agent is used instead.



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

► To set a preferred codec:

1. In the *voicelfMIB*, locate the *voicelfCodecPreferred* variable (*voicelfCodecTable*). This variable sets the preferred codec for this line.
2. Choose the codec you want to use from one of the available configurations:
 - pcmu
 - pcma
 - g729
 - g726-16kbps
 - g726-24kbps
 - g726-32kbps
 - g726-40kbps

The default value is **pcmu**.

Enabling Individual Codecs

Enabling individual codecs allows you to define codecs that can be considered during negotiation. If codecs are disabled, they are not considered.

► To enable voice codecs:

1. In the *voicelfMIB*, choose the codec you want to use (*voicelfCodecTable*). You have the choice between the following codecs:

Table 115: Enabling Voice Codecs

Codec	Variable	Set to...
PCMU (G.711 u-Law)	voicelfCodecPcmuEnable	enable
PCMA (G.711 a-Law)	voicelfCodecPcmaEnable	enable
G.726 at 16 kbps	voicelfCodecG72616kbpsEnable	enable
G.726 at 24 kbps	voicelfCodecG72624kbpsEnable	enable
G.726 at 32 kbps	voicelfCodecG72632kbpsEnable	enable
G.726 at 40 kbps	voicelfCodecG72640kbpsEnable	enable
G.729.A	voicelfCodecG729Enable	enable

2. If you have enabled one or more of the G.726 codecs, set the G.726 actual RTP dynamic payload type used in an initial offer in one or more of the following variables:
 - voicelfCodecG72616kbpsPayloadType: The default value is 97.
 - voicelfCodecG72624kbpsPayloadType: The default value is 98.

- `voicelfCodecG72632kbpsPayloadType`: The default value is 99.
- `voicelfCodecG72640kbpsPayloadType`: The default value is 100.

The payload types available are as per RFC 3551. The values range from 96 to 127.



Note: When selecting the dynamic payload type, make sure that the value is not already used by another dynamic codec. If a value between 96 and 127 is refused, this means it is already used by another dynamic codec.



Note: If you set the `voicelfDtmfTransport` variable to `outOfBandUsingSignalingProtocol` ([“DTMF Transport Type” on page 172](#)), you cannot configure a dynamic payload type to 111 because it is already used by the DTMF out-of-band using signalling protocol.

3. Restart the Mediatrix 4102 so that the changes may take effect.

Packetization Time

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet.

► To set the packetization time:

1. In the `voicelfMIB`, set the packetization time of the codec(s) as required (`voicelfCodecTable`). Available values vary from one codec to another.

Table 116: Packetization Time Settings

Variable	Definition	Values (ms)
PCMU (G.711 u-Law)		
<code>voicelfCodecPcmuMinPTime</code>	Shortest packetization period allowed for the PCMU codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <code>voicelfCodecPcmuMaxPTime</code> variable. Default Value: 10	10-100, with increments of 10
<code>voicelfCodecPcmuMaxPTime</code>	Longest packetization period allowed for the PCMU codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <code>voicelfCodecPcmuMinPTime</code> variable. Default Value: 100	10-100, with increments of 10
PCMA (G.711 a-Law)		
<code>voicelfCodecPcmaMinPTime</code>	Shortest packetization period allowed for the PCMA codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <code>voicelfCodecPcmaMaxPTime</code> variable. Default Value: 10	10-100, with increments of 10
<code>voicelfCodecPcmaMaxPTime</code>	Longest packetization period allowed for the PCMA codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <code>voicelfCodecPcmaMinPTime</code> variable. Default Value: 100	10-100, with increments of 10

Table 116: Packetization Time Settings (Continued)

Variable	Definition	Values (ms)
G.726		
voicelfCodecG72616kbpsMinPTime	Shortest packetization period allowed for the G.726-16kbps codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <i>voicelfCodecG72616kbpsMaxPTime</i> variable. Default Value: 10	10-100, with increments of 10
voicelfCodecG72616kbpsMaxPTime	Longest packetization period allowed for the G.726-16kbps codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <i>voicelfCodecG72616kbpsMinPTime</i> variable. Default Value: 100	10-100, with increments of 10
voicelfCodecG72624kbpsMinPTime	Shortest packetization period allowed for the G.726-24kbps codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <i>voicelfCodecG72624kbpsMaxPTime</i> variable. Default Value: 10	10-100, with increments of 10
voicelfCodecG72624kbpsMaxPTime	Longest packetization period allowed for the G.726-24kbps codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <i>voicelfCodecG72624kbpsMinPTime</i> variable. Default Value: 100	10-100, with increments of 10
voicelfCodecG72632kbpsMinPTime	Shortest packetization period allowed for the G.726-32kbps codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <i>voicelfCodecG72632kbpsMaxPTime</i> variable. Default Value: 10	10-100, with increments of 10
voicelfCodecG72632kbpsMaxPTime	Longest packetization period allowed for the G.726-32kbps codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <i>voicelfCodecG72632kbpsMinPTime</i> variable. Default Value: 100	10-100, with increments of 10
voicelfCodecG72640kbpsMinPTime	Shortest packetization period allowed for the G.726-40kbps codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <i>voicelfCodecG72640kbpsMaxPTime</i> variable. Default Value: 10	10-100, with increments of 10
voicelfCodecG72640kbpsMaxPTime	Longest packetization period allowed for the G.726-40kbps codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <i>voicelfCodecG72640kbpsMinPTime</i> variable. Default Value: 100	10-100, with increments of 10

Table 116: Packetization Time Settings (Continued)

Variable	Definition	Values (ms)
G.729		
<code>voicelfCodecG729MinPTime</code>	Shortest packetization period allowed for the G.729 codec. Authorized values start at 10 ms and come in discrete steps of 10 ms up to the one specified by the <code>voicelfCodecG729MaxPTime</code> variable. Default Value: 10	10-100, with increments of 10
<code>voicelfCodecG729MaxPTime</code>	Longest packetization period allowed for the G.729 codec. Authorized values go up to 100 ms, in discrete steps of 10 ms, and start at the one specified by the <code>voicelfCodecG729MinPTime</code> variable. Default Value: 100	10-100, with increments of 10

2. Restart the Mediatrix 4102 so that the changes may take effect.

DTMF Transport Type

Standards Supported

- ITU-T Recommendation Q.24 : Multifrequency push-button signal reception
- RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

You can define how to transport the DTMFs.

► To set the DTMF transport type:

1. In the `voicelfMIB`, set the DTMF transport type in the `voicelfDtmfTransport` variable (`voicelfDtmfTransportTable` group).

The following choices are available:

Table 117: DTMF Transport Type Parameters

Transport Parameter	Description
<code>inBand</code>	The DTMFs are transmitted like the voice in the RTP stream.
<code>outOfBandUsingRtp</code>	The DTMFs are transmitted as per RFC 2833 (see "DTMF Payload Type" on page 173 for additional information).

DTMF out-of-band

Certain compression codecs such as 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 4102 receives and sends out-of-band DTMFs as per ITU Q.24. DTMFs supported are 0-9, A-D, *, #.

Table 117: DTMF Transport Type Parameters (Continued)

Transport Parameter	Description
outOfBandUsingSignalingProtocol	The DTMFs are transmitted as per the MGCP protocol standard.
signalingProtocolDependent	The signalling protocol has the control to select the DTMF transport mode.

- Restart the Mediatrix 4102 so that the changes may take effect.

DTMF Payload Type

Standards Supported	RFC 1890 – RTP Profile for Audio and Video Conferences with Minimal Control
----------------------------	---

When selecting the *outOfBandUsingRtp* DTMF transport mode (see [“DTMF Transport Type” on page 172](#) for more details), 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.

► To define the DTMF payload type:

- In the *voicelfMIB*, set the DTMF transport type in the *voicelfDtmfTransport* variable (*voicelfDtmfTransportTable* group) to **outOfBandUsingRtp**.
- Set the payload type in the *voicelfDtmfPayloadType* variable.
Available values range from 96 to 127.

DTMF Detection

The default DTMF detection parameters of the Mediatrix 4102 may sometimes not be enough to properly detect the DTMFs. This section describes how to set additional DTMF detection parameters.

DTMF Frequencies

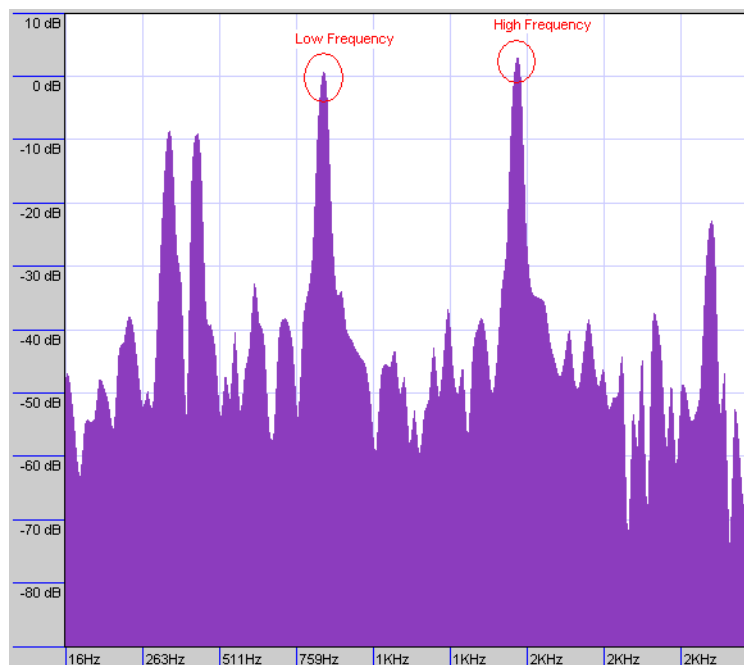
The DTMF keypad is laid out in a 4x4 matrix, with each row representing a low frequency, and each column representing a high frequency. For example, pressing a single key (such as '1') sends a sinusoidal tone of the two frequencies (697 Hz and 1209 Hz). When the unit is configured to send DTMFs out-of-band, its DSP detects these DTMFs, removes them from the RTP stream, and sends them out-of-band.

Table 118: 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 43: DTMF Detection Example

To detect this DTMF, the DSP relies on several parameters. The following table lists the default values that the Mediatrix 4102 uses. You can override any one of these values.

Table 119: DTMF Detection Default Parameters

Parameter	Value
MinPowerThreshold	-30 dBm0
MaxPowerThreshold	1 dBm0
BreakPowerThreshold	32 dBm0
PositiveTwist	6 dBm0
NegativeTwist	9 dBm0
RiseTimeCriteria	confirmSnr

► **To configure the DTMF detection:**

1. In the *voicelfMIB*, set the maximum absolute power threshold (dBm0) for the low and high frequencies in a DTMF in the *voicelfDtmfDetectionUnitMaxPowerThreshold* variable.
The high AND low DTMF frequencies MUST be lower than this threshold otherwise the DTMF is not detected.
Raising this value increases the sensitivity of the DTMF detection. Raising this value too high may also cause false detections of DTMFs.
2. Set the minimum absolute power threshold (dBm0) for the low and high frequencies in a DTMF in the *voicelfDtmfDetectionUnitMinPowerThreshold* variable.
The high AND low DTMF frequencies MUST be higher than this threshold otherwise the DTMF is not detected.
You could, for instance use one of the following settings:
 - -15 dBm0: This configuration detects even more false DTMFs in the voice pattern.
 - -20 dBm0: This configuration detects more DTMFs in the voice pattern.
 - -35 dBm0: his configuration detects less DTMFs in the voice pattern.

- -40 dBm0: This configuration detects even less DTMFs in the voice pattern.

Raising this value reduces the sensitivity to DTMF detection.

3. Set the break absolute power threshold (dBm0) for on-off transition of a DTMF in the *voicelfDtmfDetectionUnitBreakPowerThreshold* variable.
While a DTMF has been positively detected, the DTMF will be considered OFF as soon as the high OR low frequency in the DTMF gets below this threshold.
4. Set the *voicelfDtmfDetectionUnitPositiveTwist* variable.
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.
5. Set the *voicelfDtmfDetectionUnitNegativeTwist* variable.
When the low frequency of a DTMF is more powerful than the high frequency, the difference between the low frequency absolute power and the high 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.
6. Define how the Rise Time criteria should be configured for DTMF detection in the *voicelfDtmfDetectionRiseTimeCriteria* variable.

Table 120: RiseTimeCriteria Parameters

Parameter	Description
checkSr	Enable the Step Rise criteria and disable the Confirm DTMF SNR criteria.
confirmSnr	Enable the Confirm DTMF SNR criteria and disable the Step Rise criteria.

The Step Rise criteria compares the current frame energy to the high frequency power of the previous frame. If the current frame energy is high enough, then it passes the test, further validating the DTMF.

Disabling the Step Rise criteria may result in deteriorated talk-off performance, but increases the detection of malformed DTMF.

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.

Adaptative Jitter Buffer

The jitter buffer allows better protection against packet loss, but increases the voice delay. If the network to which the Mediatrix 4102 is connected suffers from a high level of congestion, the jitter buffer protection level should be higher. If the network to which the Mediatrix 4102 is connected suffers from a low level of congestion, the jitter buffer protection level should be lower.



Note: Do not put 0 as values for the *voicelfTargetJitterBufferLength* and *voicelfMaxJitterBufferLength* variables.

► To set Jitter Buffer variables:

1. In the *voicelfMIB*, locate the *voicelfTable* group.

2. Define the jitter buffer length in the *voicelfTargetJitterBufferLength* variable.
 The adaptive jitter buffer attempts to hold packets to the target holding time. This is the minimum delay the jitter buffer adds to the system. The target jitter buffer length is in ms and must be equal to or smaller than the maximum 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 multiple of 5 ms.
 It is best not to set target jitter values below the default value. Setting a target 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 176](#) for more details.
3. Define the maximum jitter buffer length in the *voicelfMaxJitterBufferLength* variable.
 This is the maximum jitter the adaptive jitter buffer can handle. The jitter buffer length is in ms and must be equal to or greater than the target 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 multiple of 5 ms.
 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
 See [“About Changing Jitter Buffer Values” on page 176](#) for more details.
4. Restart the Mediatrix 4102 so that the changes may take effect.

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 135 ms and the delay measured is 130 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.

Voice Activity Detection

The Voice Activity Detection (VAD) defines how the Mediatrix 4102 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, the VAD may affect packets that are not really silent (for instance, cut sounds that are too low). The VAD can thus slightly affect the voice quality.

G.711 and G.726 VAD

The G.711/G.726 VAD is generic – when enabling VAD, G.711/G.726 sends speech frames only during periods of audio activity. During silence periods, G.711/G.726 does not send speech frames, but it may send Comfort Noise (CN) packets (payload 13) containing information about background noise.



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

► **To enable G.711 and G.726 VAD:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the sensitivity of the VAD algorithm to silence periods in the *voicelfG711VoiceActivityDetectionEnable* variable.

The following settings are available:

Table 121: 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.

The default value is **conservative**.

3. Restart the Mediatix 4102 so that the changes may take effect.

G.729 VAD

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.

► **To enable G.729 VAD:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the *voicelfG729VoiceActivityDetectionEnable* variable.

The following settings are available:

Table 122: G.729 VAD Settings

Setting	Description
disable	G.729 uses annex A only. The Mediatix 4102 does not send G.729 Annex B comfort noise frames.
enable	G.729 annex A is used with annex B. The Mediatix 4102 sends G.729 Annex B comfort noise frames during silence periods.

See [“Enabling Individual Codecs” on page 169](#) for more details.

G.729 Annex B Negotiation

You can indicate whether the G.729 Annex B is negotiated through the Session Description Protocol (SDP) or not.

RFC 3555 (MIME Type Registration of RTP Payload Formats), July 2003 explains how the Annex B can be negotiated by using the SDP.

The Annex B indicates that Annex B, voice activity detection, is used or preferred. Permissible values are 'yes' and 'no' (without the quotes); 'yes' is implied if this parameter is omitted.

```
m=audio 5004 RTP/AVP 0 18 13
a=fmtp:18 annexb=yes
```

► To define the G.729 Annex B negotiation:

1. In the *mgcpnicsExperimentalMIB*, set the *mgcpnicsG729AnnexBNegotiation* variable to the proper value.

The following values are available:

Table 123: G.729 Annex B Negotiation Parameters

Parameter	Description
disable	The G.729 Annex B is NOT negotiated through the SDP. This is the default value. In that case, the G.729 Annex B is based on the MIB variable <i>voicelfG729VoiceActivityDetectionEnable</i>. When this variable is set to enable, the G.729 codec negotiated as payload number 18 (G729) supports the Annex B implicitly. However, when the <i>voicelfG729VoiceActivityDetectionEnable</i> variable is set to disable, the G.729 codec negotiated as payload number 18 (G729) does NOT support the Annex B implicitly.
enable	The G.729 Annex B is negotiated through the SDP. In that case, the G.729 Annex B is advertised in the offer. The value depends on the MIB variable <i>voicelfG729VoiceActivityDetectionEnable</i>. If this variable is set to enable, then the Annex B is set to 'yes'; otherwise, the value 'no' is advertised. The answerer MAY not be able to support the Annex B. In that case, the answer to the Annex B can be set to 'no'. This forces the offerer not to use the Annex B in G.729. However, the opposite is not possible. The answerer can NOT force the offerer to use the Annex B if this one does not bear such capability.

Echo Cancellation

Echo cancellation eliminates the echo effect caused by signal reflections. An echo is a signal that has been reflected or otherwise returned with enough magnitude and delay to be perceived. The echo cancellation is usually an active process in which echo signals are measured and cancelled or eliminated by combining an inverted signal with the echo signal.

Comfort Noise

Standards Supported

- RFC 3389: Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)

Comfort Noise (CN) defines how the Mediatrix 4102 processes silence periods information it receives.



Note: Comfort noise only applies to the G.711 and G.726 codecs. G.729 CNG is not configurable because it is part of the codec.

During silence periods, the Mediatrix 4102 may receive CN packets containing information about background noise. When enabling Comfort Noise Generation (CNG), those packets are used to generate local comfort noise.

► **To enable Comfort Noise:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the type of comfort noise in the *voicelfG711ComfortNoiseGenerationEnable* variable. The following settings are available:

Table 124: Comfort Noise Settings

Setting	Description
disable	CNG disabled.
whiteNoise	CNG enabled – white noise.
customNoise	CNG enabled – custom noise. More elaborated background noise that sounds better than white comfort noise.

3. Restart the Mediatrix 4102 so that the changes may take effect.

User Gain

The user gain allows you to modify the input and output sound level of the Mediatrix 4102.



Caution: Use these settings with great care. Media5 recommends not to modify the user gain variables unless absolutely necessary because default calibrations may not be valid anymore.

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 not be recognized anymore. 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 4102 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, simply put 1 for user gain input).



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

► **To set user gain variables:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the following variables:
 - *voicelfUserInputGainOffset*: User input gain offset in dB (from analog to digital).
 - *voicelfUserOutputGainOffset*: User output gain offset in dB (from digital to analog).

Values range from -30 dB to +20 dB. However, going above +6 dB may introduce clipping/distortion depending on the country selected. Under -24 dB, you will not have much signal either.
3. Restart the Mediatrix 4102 so that the changes may take effect.

This chapter describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 4102.

Introduction

The Mediatrix 4102 handles G3 fax transmissions at speeds up to 14.4 kbps. Automatic fax mode detection is standard on all lines. Real-Time Fax Over UDP with the T.38 protocol stack is also available.

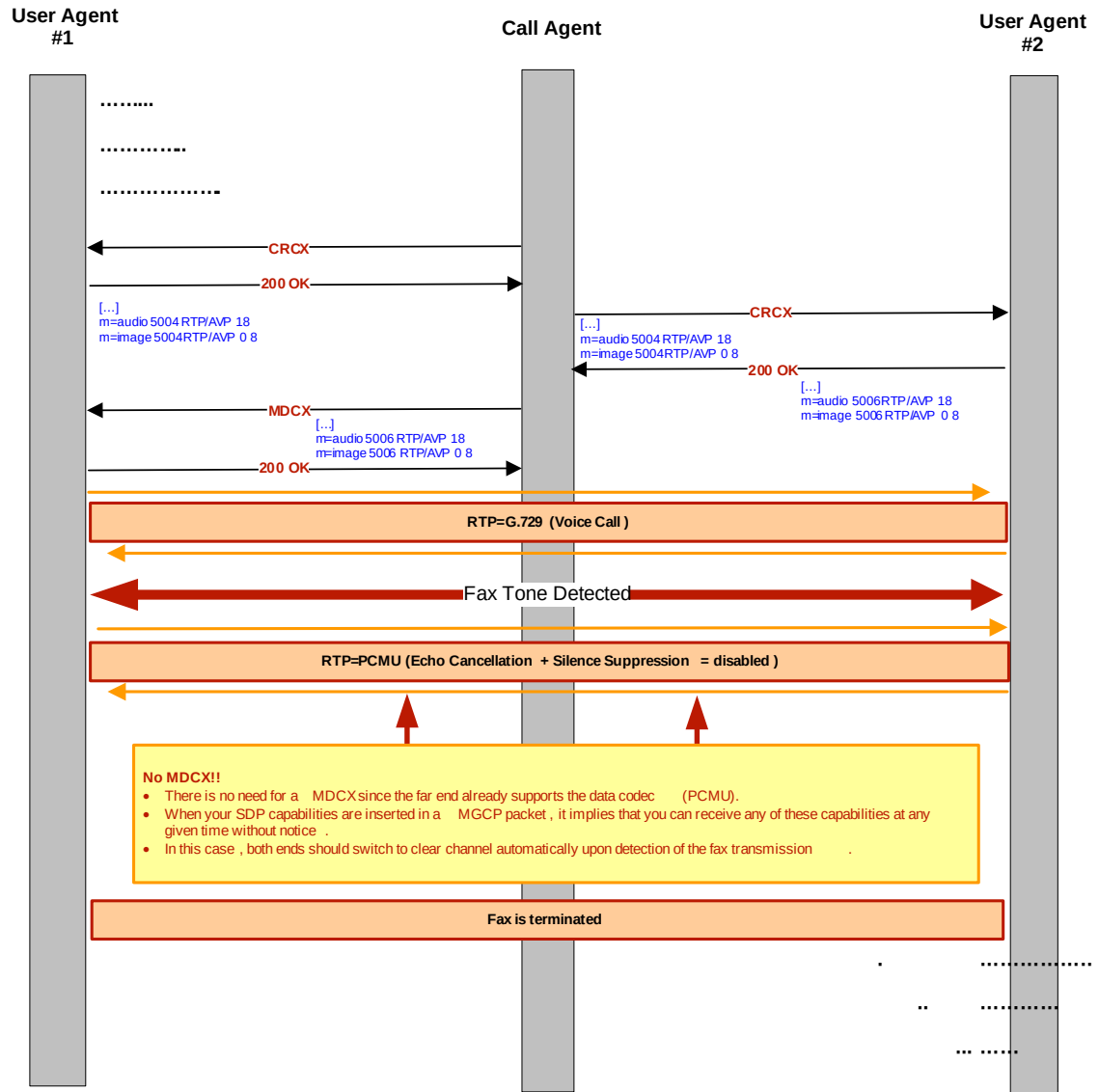
The quality of T.38 fax transmissions depends upon the system configuration, type of call control system used, type of Mediatrix units deployed, as well as the model of fax machines used. Should some of these conditions be unsatisfactory, performance of T.38 fax transmissions may vary and be reduced below expectations.

All lines of the Mediatrix 4102 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** line.

Clear Channel Fax

The Mediatrix 4102 can send faxes in clear channel. The following is a clear channel fax call flow:

Figure 44: Clear Channel Fax Call Flow



► **To set clear channel fax transmission via codec negotiation:**

1. Choose the codec you want to favour during negotiation in the *dataIfCodecMediaTypeImageEnable* variable.

Table 125: Codec Negotiation Parameters

Parameter	Description
disable	The image media type is not present in the SDP.
pcmu	The image media type is present in the SDP for PCMU only.
pcma	The image media type is present in the SDP for PCMA only.

Table 125: Codec Negotiation Parameters (Continued)

Parameter	Description
pcmu-pcma	The image media type is present in the SDP for PCMU and PCMA.
g726	The image media type is present in the SDP for G.726 only.
pcmu-g726	The image media type is present in the SDP for PCMU and G.726.
pcma-g726	The image media type is present in the SDP for PCMA and G.726.
pcmu-pcma-g726	The image media type is present in the SDP for PCMU, PCMA and G.726.

If the selected codec is disabled, it is ignored.

► **To set a preferred clear channel fax transmission codec:**

1. Set the *datafCodecT38Enable* variable to **disable**.
2. Set the clear channel codec to use upon detecting a fax tone in the *datafClearChannelCodecPreferred* variable.

This variable is used to decide which of the following codecs is preferred, even for voice transmissions:

- PCMU
- PCMA
- G.726 at 32 kbs
- G.726 at 40 kbs



Note: In clear channel, G.726 at 16 kbs and 24 kbs are not available for fax transmission.



Note: If you want to set the G.726 codec at 32 kbs or at 40 kbs as the preferred clear channel codec, you must also select the corresponding G.726 codec as the preferred voice codec as described in ["Preferred Codec" on page 169](#). Otherwise, the Mediatrix 4102 will fail to switch to the G.726 codec for clear channel faxes because G.726 is not negotiated.

There is no codec negotiation. The Mediatrix 4102 uses this codec if the remote unit suggests both PCMU and PCMA for its fax. If the preferred codec is PCMU and the remote unit only suggests PCMA, the call uses PCMA.

This variable increases the relative priority of the selected codec vs other data-capable codecs. However, the priority of the preferred clear channel codec remains lower than the *voicelfCodecPreferred* variable (see ["Preferred Codec" on page 169](#)).

Moreover, when no data-capable codec is part of the list of negotiated codecs, this variable indicates which codec to use when fax or modem tones are detected. However, if the negotiated voice codec is data-capable, the voice codec will be used for data instead of the preferred data codec.

Media5 suggests to use *pcma* if you are located in Europe and *pcmu* anywhere else. However, you should check first which codec is supported in your telephone network.

T.38 Fax

Standards Supported

- Recommendation ITU T.38 version 0

T.38 fax relay is a real-time fax transmission; that is, two fax machines communicating with each other as if there were a direct phone line between the two. T.38 is called a fax relay, which means that instead of sending inband fax signals, which implies a loss of signal quality, it sends those fax signals out-of-band in a T.38 payload, so that the remote end can reproduce the signal locally.

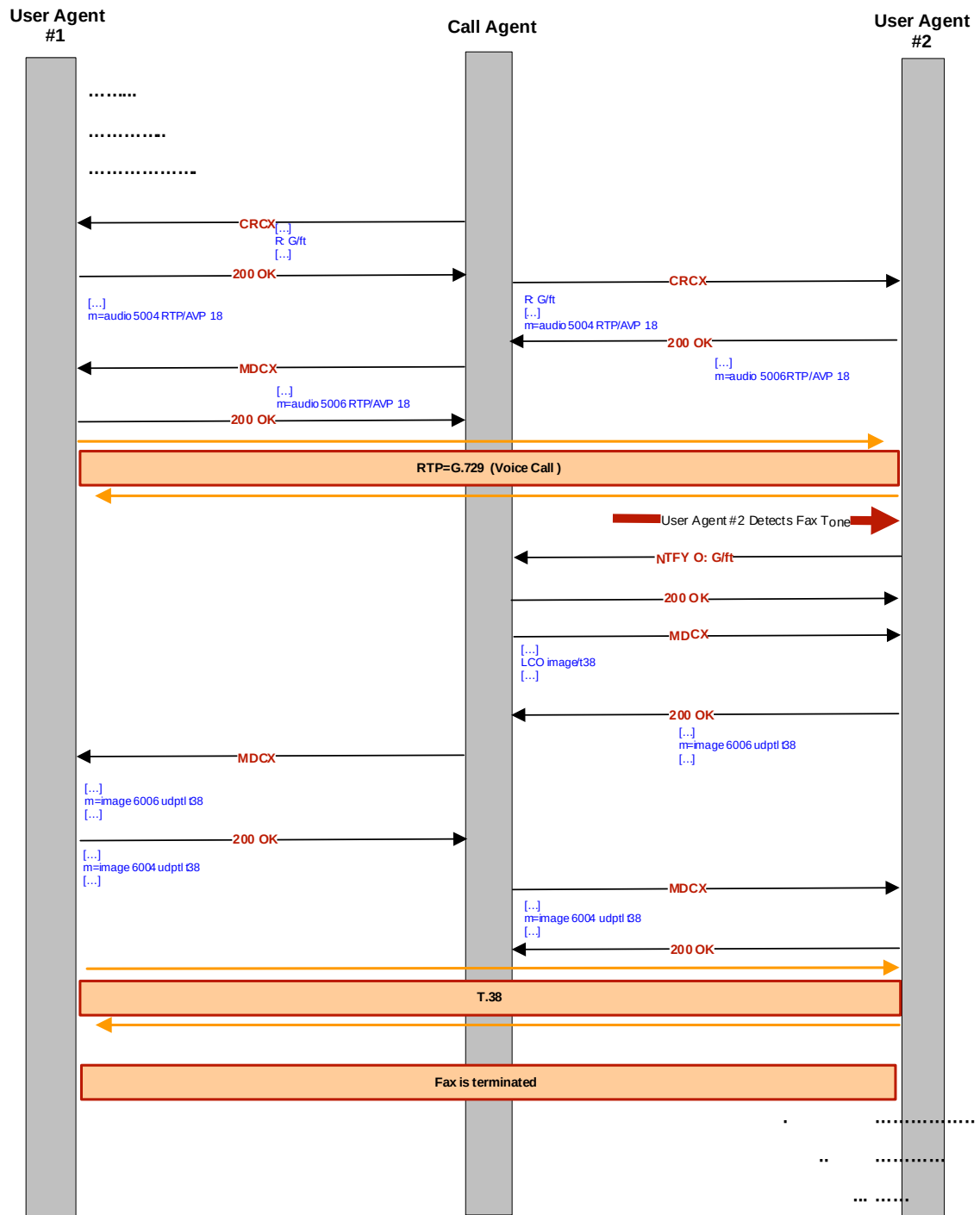
The Mediatrix 4102 can send faxes in T.38 mode over UDP. T.38 is used for fax if both units are T.38 capable; otherwise, transmission in clear channel over G.711 as defined is used (if G.711 μ -law and/or G.711 A-law are enabled). If no clear channel codecs are enabled and the other endpoint is not T.38 capable, the fax transmission fails.



In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.

The following is a T.38 fax call flow:

Figure 45: T.38 Fax Call Flow



► To set T.38 fax transmission:

1. Enable T.38 by setting the *dataIcfCodecT38Enable* variable to **enable**.
If you select the *signalingProtocolDependent* option of the *voicelfDtmfTransport* variable (["DTMF Transport Type" on page 172](#)), the signaling protocol has the control to enable or disable T.38.
2. Set the number of redundancy packets sent with the current packet in the *dataIcfCodecT38ProtectionLevel* variable.
This is the standard redundancy offered by T.38.
Available values range from 1 to 5, 3 being the default value.
3. Restart the Mediatrix 4102 so that the changes may take effect.

T.38 No-Signal

You can set the Mediatrix 4102 to send no-signal packets during a T.38 fax transmission. The Mediatrix 4102 sends no-signal packets if no meaningful data have been sent for a user-specified period of time.

► To send T.38 no-signal:

1. Set the period, in seconds, at which no-signal packets are sent during a T.38 transmission in the *dataIcfT38NoSignalTimeout* variable.
No-signal packets are sent out if there are no valid data to send.
2. Enable the sending of T.38 no-signal packets by setting the *dataIcfT38NoSignalEnable* variable to **enable**.

This chapter describes how to configure the STUN client of the Mediatrix 4102.

What is STUN?

Standards Supported	RFC 3489 – STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
STUN (Simple Traversal of UDP through NATs) is a simple client / server protocol that uses UDP packets to discover the configuration information of NATs and firewalls between a device and the public Internet: ▶ NAT type ▶ NAT binding public address ▶ NAT binding time to live NAT (Network Address Translator) is a device that translates the IP address used within a “private” network to a different IP address known in another “public” network. See “NAT Traversal” on page 267 for more details. STUN supports a variety of existing NAT devices and does not require any additional hardware or software upgrades on the NAT device. The Mediatrix 4102 uses the STUN protocol to discover its NAT binding for the following two IP addresses/ ports (sockets): ▶ RTP IP address/port ▶ T.38 IP address/port	

Restrictions on the Media5 STUN Implementation

- ▶ The Mediatrix 4102 does not currently support NAT type discovery.
- ▶ The Mediatrix 4102 does not currently support STUN NAT binding time to live discovery.
- ▶ The Mediatrix 4102 does not currently support the TLS security mechanism.
- ▶ Due to a limitation of most routers, an RTP portal might be required in order for two units behind the same NAT/firewall to be able to communicate with each other.

STUN Client Configuration

The following describes how to configure the Mediatix 4102 STUN client via SNMP. You can also use the web interface to configure the STUN parameters. See ["STUN Page" on page 32](#) for more details.

► **To configure the STUN client:**

1. In the *ipAddressConfig* folder, locate the *ipAddressConfigStunStatic* group.
No DHCP value is available, you can only define STUN server information with static values.
2. Set the static STUN server IP address or Fully Qualified Domain Name (FQDN) in the *stunStaticHost* variable.
The default value is **192.168.0.10**.
3. Set the static STUN server IP port number in the *stunStaticPort* variable.
The default value is **3478**.
4. In the *stunMIB*, set the amount of time, in seconds, the Mediatix 4102 should keep a STUN query result in its internal cache in the *stunQueryCacheDuration* variable.
Keeping a query in a cache helps to reduce the amount of unnecessary STUN queries when an RTP or T.38 socket is re-used within a short period of time. Available values range from 0 s to 3600 s.
When set to **0**, the cache is disabled and the unit performs a STUN query each time a socket needs to be used.
5. Set the maximum amount of time, in milliseconds, the Mediatix 4102 should wait for an answer to a STUN query sent to a STUN server in the *stunQueryTimeout* variable.
Available values range from 500 ms to 10000 ms. The default value is 1000 ms.
Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure.
6. Define the interval, in seconds, at which the Mediatix 4102 sends blank keepalive messages to keep a firewall hole opened in the *stunKeepAliveInterval* variable.
Keepalive messages are used by the RTP socket to keep the connection opened through a firewall. Available values range from 0 s to 120 s. The default value is 30 s.
When set to **0**, no keepalive packet is sent.



Note: Keepalive messages are not supported on the T.38 socket.

See ["Firewall Traversal" on page 92](#) for information on the keepalive parameter for the signalling MGCP.

7. Enable the STUN client by setting the *stunEnable* variable to **enable**.
This enables the STUN client for all sockets (RTP and T.38) altogether.
8. Restart the Mediatix 4102 so that the changes may take effect.

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix 4102. It updates the internal clock of the unit, which is the client of a SNTP server. It is required when dealing with features such as the caller ID.

SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport.

Enabling the SNTP Client

Standards Supported

RFC 1769 – Simple Network Time Protocol (SNTP)

You must enable the SNTP client of the Mediatrix 4102 to properly connect to a a SNTP or NTP server.

► To enable the SNTP feature:

1. In the *sntpMIB*, set the *sntpEnable* variable to **enable**.
2. Set the following synchronization information:

Table 126: SNTP Synchronization Information

Variable	Description
sntpSynchronizationPeriod	Time interval (in minutes) between requests made to the SNTP server. The result is used to synchronize the unit with the time server. The maximum value is set to 1440 minutes (24 hours). Default Value: 1440
sntpSynchronizationPeriodOnError	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1440 (24 hours). Default Value: 60

Configuration Source

The Mediatrix 4102 must know the IP address and port number of the SNTP server. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself with the static variables.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *SNTP*.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► **To use DHCP-assigned information:**

1. In the *ipAddressConfig* folder, locate the *sntpSelectConfig Source* variable (under the *ipAddressConfigSntp* group).
This variable defines whether the Mediatrix 4102 must ask for its SNTP server settings through a DHCP server or not.
2. Set the *sntpSelectConfigSource* variable to **dhcp**.
You can query the SNTP server's IP address and port number assigned by the DHCP server in the *sntpHost* and *sntpPort* read-only variables (under the *ipAddressStatusSntp* group).
3. Set the DHCP Vendor Specific code of the SNTP feature in your DHCP server.
See [“SNTP” on page 65](#) for more details.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *sntpSelectConfig Source* variable (under the *ipAddressConfigSntp* group).
This variable defines whether the Mediatrix 4102 must ask for its SNTP server settings through a DHCP server or not.
2. Set the *sntpSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 127: SNTP Static Address

Variable	Description
sntpStaticHost	Static SNTP server IP address or domain name. Default Value: 192.168.0.10
sntpStaticPort	Static SNTP server IP port number. Default Value: 123

Defining a Custom Time Zone

Standards Supported

bootp-dhcp-option-88.txt Internet draft

When starting, the Mediatrix 4102 queries a NTP or SNTP server to receive time information. It receives the information in Greenwich Mean Time (GMT) format (also known as Universal Time Coordinated - UTC), so it needs to convert this GMT time into the proper time zone. To do this, the Mediatrix 4102 offers time zone configuration with daylight saving settings.

► To define a custom time zone:

1. In the *sntpMIB*, enter a valid POSIX (Portable Operating System Interface) string in the *sntpTimeZoneString* variable as defined in the <bootp-dhcp-option-88.txt> Internet draft.
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.txt> Internet draft as:
STD0FFSET[DST[OFFSET],[START[/TIME],END[/TIME]]]
Refer to the following sub-sections for explanations on each part of the string.

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). As an example:
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.

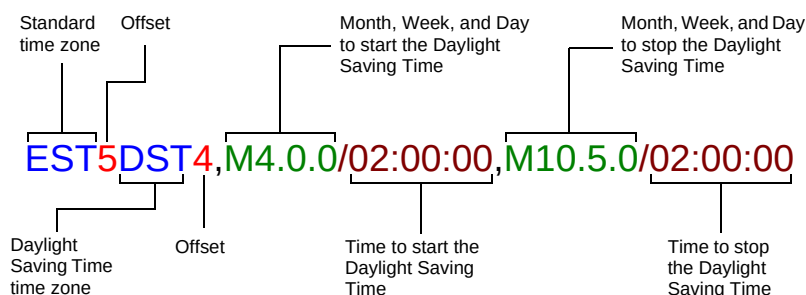
M10.1.6

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 128: 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

Management Server Configuration

The Management Server is a generic name for a module or software that is used to remotely set up Mediatrix 4102 units. For instance, the Management Server could be the Media5's Unit Manager Network product. See ["Unit Manager Network – Element Management System" on page xvii](#) for more details.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Unit Manager Server*.

Using the Management Server

You have the choice of setting up Mediatrix 4102 units directly with a SNMP browser or with the Management Server. If you want to use the Management Server to setup the units, you shall tell these units how to reach the Management Server.

► To use the Management Server:

1. In the *msMIB*, locate the *msEnable* variable.
This variable enables the Management Server to remotely manage the Mediatrix 4102.
2. Set the *msEnable* variable to **enable**.
3. Set the Trap retransmission period (*msTrapRetransmissionPeriod* variable) to the desired value.
The available values range from 10 ms to 604 800 000 ms (1 week). The default value is 60 000 ms.
4. Set the Trap retransmission retry count (*msTrapRetransmissionRetryCount* variable) to the desired value.
When the retry count is elapsed, the Mediatrix 4102 stops the provisioning sequence. The default value is 10. If this variable is set to -1, then the provisioning sequence never stops. The trap is sent until the Management Server replies.

Configuration Source

The Mediatrix 4102 must know the IP address and port number of the Management Server. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See ["Chapter 5 - IP Address and Network Configuration" on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *msSelectConfig Source* variable.
This variable defines whether the Mediatrix 4102 shall get its Management Server configuration through a DHCP server or not.
2. Set the *msSelectConfigSource* variable to **dhcp**.
You can query the Management Server's IP address and port number assigned by the DHCP server in the *msHost* and *msTrapPort* read-only variables (in the *ipAddressStatus* folder).

3. Set how you want to define the Management Server information in the DHCP server:

Table 129: Management Server DHCP Information

To use a...	Set...
vendor specific code	The <i>msDhcpSiteSpecificCode</i> variable to 0 . Set the management server IP address in the DHCP server inside the vendor specific sub-option 200 (hexadecimal 0xC8).
site specific code	The <i>msDhcpSiteSpecificCode</i> variable to any value between 128 and 254. Set the management server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>msDhcpSiteSpecificCode</i> variable in the unit's configuration).

See ["Vendor and Site Specific DHCP Options" on page 67](#) for more details.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► To use static information:

1. In the *ipAddressConfig* folder, locate the *msSelectConfig Source* variable.
This variable defines whether the Mediatrix 4102 shall get its Management Server configuration through a DHCP server or not.
2. Set the *msSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 130: Management Server Static Address

Variable	Description
msStaticHost	Static management server IP address or domain name. Default Value: 192.168.0.10
msStaticTrapPort	Static management server IP port number. Restart the unit to update this parameter. Default Value: 162 Note: Change the port used in the management server. Not doing so will prevent you from viewing the received traps from the unit. The management server could be a product such as the Unit Manager Network.

MGCP/NCSQoS (Quality of Service) features enable network managers to decide on packet priority queuing. The Mediatrix 4102 supports the Differentiated Services (DS) field and 802.1q taggings. There are three variables – one variable for signalling (MGCP/NCS) and one variable for each of voice and T.38 media.

The Mediatrix 4102 supports the Real Time Control Protocol (RTCP), which is used to send packets to convey feedback on quality of data delivery.

The Mediatrix 4102 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.

It is the network administrator's responsibility to provision the Mediatrix 4102 with standard and correct values.



Note: If you are using the Mediatrix 4102 in router mode, you may want to differentiate the packets sent by the PC from the packets sent by the Mediatrix 4102. In this case, you must use a substitution value, as described in ["Configuring TAS" on page 119](#).

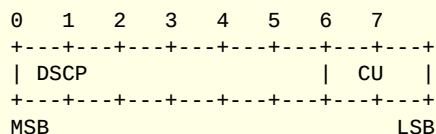
► To enable the DS field configuration:

1. In the *qosDiffServ* group of the *qosMIB*, locate the following variables:
 - *qosSignalingDiffServ*

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.

- qosVoiceDiffServ
- qosT38FaxDiffServ

These variables are 1 octet scalar ranging from 0 to 255. The DSCP default value should be 101110. This results in the DS field value of 10111000 (184).

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 Mediatix 4102. 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.

2. Set the value you want to use.

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. Restart the Mediatix 4102 so that the changes may take effect.

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 Mediatix 4102 with standard and correct values.

► To enable the IEEE 802.1q user priority configuration:

1. In the *qos/ieee8021q* group of the *qosMIB*, locate the following variables:
 - qosSignalingieee8021qEnable
 - qosVoiceieee8021qEnable
 - qosT38Faxieee8021qEnable

2. Set the value of these variables to **enable**.
The corresponding user priority configuration is enabled.

3. In the *qos/ieee8021q* group of the *qosMIB*, locate the following variables:
 - qosSignalingieee8021qUserPriority
 - qosVoiceieee8021qUserPriority
 - qosT38Faxieee8021qUserPriority

These variables are 1 octet scalar ranging from 0 to 7. The 802.1q default priority value should be 6 for both signalling and media packets.

4. Set the value you want to use.

- Restart the Mediatrix 4102 so that the changes may take effect.

For more information, please refer to the *MIB Reference* manual.

VLAN

You can set various VLAN parameters to control user priority.

► To enable the VLAN configuration:

- In the *qosVlanleeee8021q* group of the *qosMIB*, locate the *qosVlanleeee8021qTaggingEnable* variable.
- Set the value of this parameter to **enable**.
The VLAN configuration is enabled.
- Locate the following variables:
 - qosVlanleeee8021qVirtualLanID*
 - qosVlanleeee8021qDefaultUserPriority*

When both VLAN tagging and VLAN Substitution are enabled and their VLAN ID is the same, VLAN Tagging has precedence over VLAN Substitution. If VLAN Substitution has the same ID as VLAN Tagging, VLAN Substitution is not enabled and the Mediatrix 4102 behaves as such. You should change the ID of one of the features to enable VLAN Substitution. See [“VLAN Substitution” on page 198](#) for more details.

You can also use the priorities set in [“IEEE 802.1q” on page 196](#) Step 3 without putting the Mediatrix 4102 in a VLAN. To do so, you must set the *qosVlanleeee8021qTaggingEnable* variable to **enable** and the *qosVlanleeee8021qVirtualLanID* variable to **0**. This is a null VLAN ID, which indicates that the tag header contains only priority information; no VLAN identifier is present in the frame.

- Set the value of these variables.
- Restart the Mediatrix 4102 so that the changes may take effect.

VLANs

VLANs are created with standard Layer 2 Ethernet. A VLAN Identifier (VID) is associated with each VLAN. VLANs offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.

The VLAN field in the Ethernet file is located after both destination and source addresses:

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7   (byte)
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Dest Addr | Src Addr | VLAN | Type/Length | ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The VLAN field is separated as follows:

```

0 (bit)           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               0x8100                               | Pri | T | VID |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

For both signalling and media packets, the VLAN priority section is configurable independently.

For more information, please refer to the *MIB Reference* manual.

VLAN Substitution

The Mediatrix 4102 can tag the packets relayed from the LAN port to the WAN port with a VLAN ID different from the standard value defined in ["VLAN" on page 197](#).



Note: This feature only works when TAS is disabled. See ["Chapter 9 - Transparent Address Sharing" on page 113](#) for more details.

In this case, the packets coming from the LAN (usually a router or a PC) are tagged with a substitution VLAN ID before sending the packets to the WAN. In the opposite direction, the Mediatrix 4102 removes the VLAN tags and then send the packets to the LAN. The packets generated by the Mediatrix 4102 for VoIP/Signaling/Management can also be tagged with a different VLAN ID.

This can be used to prioritize VoIP in a network.

► To configure the VLAN substitution:

1. In the *qosleee8021qSubstitution* group of the *qosMIB*, define the substitution IEEE 802.1Q Virtual LAN ID in the *qosVlanleee8021qSubstitutionVlanID* variable.
The value 1 is the default Port VID (PVID) for bridge port. The 4095 VID (0xFFFF) is reserved for implementation use and it must not be used in the tag header.
You can use a VID of 0.
As per the standard, some bridges may not support the full range of VID.
When both VLAN tagging and VLAN Substitution are enabled and their VLAN ID is the same, VLAN Tagging has precedence over VLAN Substitution. If VLAN Substitution has the same ID as VLAN Tagging, VLAN Substitution is not enabled and the Mediatrix 4102 behaves as such. You should change the ID of one of the features to enable VLAN Substitution. See ["VLAN" on page 197](#) for more details.
2. Set the substitution IEEE 802.1Q Virtual LAN default user priority in the *qosVlanleee8021qSubstitutionUserPriority* variable.
This value applies to all protocols for which no priority filtering is enabled (e.g. ARP, ICMP).
 - 7 = High priority
 - 0 = Low priority
3. Enable the VLAN substitution by setting the *qosVlanleee8021qSubstitutionEnable* variable to **enable**.
The QoS 802.1q fields of the packets sent from the PC to the WAN are assigned the value defined in the *qosVlanleee8021qSubstitutionVlanID* variable.
4. Restart the Mediatrix 4102 so that the changes may take effect.

Ethernet Frames Issue

There is currently an issue with the CPU of the Mediatrix 4102. This issue prevents Ethernet frames, which have a 802.1q tag, to be correctly forwarded through the LAN port of the Mediatrix 4102, if these frames have less than 68 bytes (including FCS).

For example, it is valid to have an Ethernet frame of 64 bytes, even if it includes a 802.1q tag. However, when the CPU switch forwards this packet through the LAN port, it removes the 802.1q tag, but does not add any padding byte. The Ethernet frame is output with only 60 bytes, which is invalid and dropped by most equipment.

A workaround would be to modify the behaviour of your router to generate 802.1q frames with at least 68 bytes.

VLAN ID Filtering

VLAN ID filtering may be applied when VLAN substitution is enabled. This feature filters the packets and prevents the *Computer* connector from receiving untagged packets or packets with an invalid tag. It is especially useful to restrain the broadcast domain between each connector's subnet. The following table describes the VLAN ID filtering behaviour:

Table 131: VLAN ID Filtering

Status	Description
Enabled	Packets sent to the <i>Computer</i> connector must have the proper VLAN ID. Packets with a different VLAN ID, or untagged packets, are dropped.
Disabled	Packets sent to the <i>Computer</i> connector (tagged with any tag or untagged) are forwarded from the <i>Network</i> connector to the <i>Computer</i> connector. This effectively extends the broadcast domain and allows nodes behind the <i>Computer</i> connector to share the same IP subnet as the unit itself.

► **To enable VLAN ID Filtering:**

1. In the *qosleee8021qSubstitution* group of the *qosMIB*, set the *qosVlanleee8021qSubstitutionEnable* variable to **enable**.
See ["VLAN Substitution" on page 198](#) for more details.
2. Enable VLAN ID filtering by setting the *qosVlanleee8021qSubstitutionFiltering* variable to **enable**.
3. Restart the Mediatrix 4102 so that the changes may take effect.

LAN and WAN with VLAN substitution

LAN and WAN interfaces with VLAN substitution is used to forward network traffic between the WAN and the LAN interfaces of the Mediatrix 4102. It allows devices on the LAN side to communicate with the WAN side.

The *LAN* connector of the Mediatrix 4102 has an IP address and *WAN* connector could also have one. You can configure the IP address of the *LAN* connector statically. The PC connected to the Mediatrix 4102 could then use this address to contact the Mediatrix 4102.

For more information on how to set the *LAN* connector IP address of the Mediatrix 4102, refer to ["LAN Connector Static IP Address" on page 65](#).

Switch Mechanism with LAN and WAN with VLAN Substitution

The following table describes the various behaviours of the switch mechanism.

Table 132: Switch Mechanism Description

Behaviour	Description
Switch of outbound packets	The Mediatrix 4102 directly sends outbound packets either to the WAN or to the PC, depending on the destination MAC address.
Switch of inbound packets from the LAN	If the destination MAC address is the Mediatrix 4102's WAN MAC address, the packet is processed locally; otherwise, it is encapsulated into a VLAN 802.1q packet and sent to the WAN interface.
Switch of inbound packets from the WAN	If the destination MAC address is the Mediatrix 4102's WAN MAC address, the packet is processed locally; otherwise, if it is a VLAN encapsulated packet, the Mediatrix 4102 removes the encapsulation and sends it to the LAN interface.

This chapter describes how to configure and use the Syslog daemon.

Syslog Daemon Configuration

Standards Supported

RFC 3164 – The BSD Syslog Protocol

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from the Mediatrix 4102 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 software into the Mediatrix 4102, you can monitor each step of the software download phase. Furthermore, if the unit encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.



In the *Unit Manager Network Administration Manual*, refer to chapter *Administration Parameters*, section *Syslog Daemon*.

► To enable the Syslog daemon:

1. In the *syslogMIB*, locate the *syslogMsgMaxSeverity* variable.

This variable indicates which syslog message is processed. Any syslog message with a severity value greater than the selected value is ignored by the agent.

- disabled
- critical
- error
- warning
- informational
- debug

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

The following are some of the messages the unit sends:

Table 133: Syslog Messages Examples

Event	Level	Message
The configuration update with the specific configuration file has been successful (configuration file fetching)	Informational	The specific configuration update succeeded.
The configuration update with the specific configuration file experienced an error and has not been completed (configuration file fetching)	Error	The specific configuration update failed.
The software update has been successful	Informational	The software update succeeded.
The software update experienced an error and has not been completed	Error	The software update failed.

Configuration Source

The Mediatrix 4102 must know the IP address and port number of the Syslog server. You can assign these information to the Mediatrix 4102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See [“Chapter 5 - IP Address and Network Configuration” on page 55](#) for more details.

► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *syslogSelectConfig Source* variable.
This variable defines whether the Mediatrix 4102 shall ask for its Syslog daemon settings through a DHCP server or not.
2. Set the *syslogSelectConfigSource* variable to **dhcp**.
You can query the Syslog daemon's IP address and port number assigned by the DHCP server in the *syslogHost* and *syslogPort* read-only variables (under the *ipAddressStatus Syslog* group of the *ipAddressStatus* folder).
3. Set how you want to define the Syslog information in the DHCP server:

Table 134: Syslog DHCP Information

To use a...	Set...
vendor specific code	The <i>syslogDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSyslogDhcp</i> group) to 0 . Set the Syslog server IP address in the DHCP server inside the vendor specific sub-option 110 (hexadecimal 0x6E).
site specific code	The <i>syslogDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSyslogDhcp</i> group) to any value between 128 and 254. Set the Syslog server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the <i>syslogDhcpSiteSpecific Code</i> variable in the unit's configuration).

See [“Vendor and Site Specific DHCP Options” on page 67](#) for more details.

Static Configuration

Use the static configuration if you are not using a DHCP server or if you want to bypass it.

► To use static information:

1. In the *ipAddressConfig* folder, locate the *syslogSelectConfig Source* variable.
This variable defines whether the Mediatrix 4102 shall ask for its Syslog daemon settings through a DHCP server or not.
2. Set the *syslogSelectConfigSource* variable to **static**.
3. Set the following variables:

Table 135: Syslog Daemon Static Address

Variable	Description
<i>syslogStaticHost</i>	Syslog server static IP address or domain name. Default Value: 192.168.0.10
<i>syslogStaticPort</i>	Syslog server static IP port number. Default Value: 514

Customizing Syslog Messages

You can display additional information in the prefix of syslog messages the Mediatrix 4102 sends. This allows you to later filter the messages. The following is the additional information you can enable:

- ▶ MAC address
- ▶ local time
- ▶ local host



Note: This applies only to syslog messages sent on the network and not the local syslog messages.

▶ **To add the MAC address of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayMacAddress* variable to **enable**.
The MAC address of the Mediatrix 4102 is part of the prefix for all syslog messages.
If you set the variable to **disable**, the MAC address is not displayed in the prefix of the syslog messages.

▶ **To add the local time of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayTime* variable to **enable**.
The current local time of the Mediatrix 4102 is part of the prefix for all syslog messages.
If you set the variable to **disable**, the time is not displayed in the prefix of the syslog messages.
2. Select the timestamp format of the syslog messages in the *syslogMsgDisplayTimeFormat* variable.
The following values are available:

Table 136: Timestamp Format Parameters

Parameter	Description
trueRfcFormat	The timestamp complies with the RFC 3164 format. The timestamp in true RFC 3164 format is <i>Jan 1 09:05:06</i> .
pseudoRfcFormat	The timestamp uses a pseudo-RFC 3164 format. The timestamp in pseudo-RFC 3164 format is <i>Jan 1 9:5:6</i> .

The default value is **pseudoRfcFormat**.

▶ **To add the local host of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayLocalHost* variable to **enable**.
The current local host of the Mediatrix 4102 is part of the prefix for all syslog messages.
If you set the variable to **disable**, the local host is not displayed in the prefix of the syslog messages.

Configuring the Syslog Daemon Application

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

Local Syslog

The local syslog is an internal syslog server to the Mediatrix 4102. It keeps the last *n* syslog messages. These syslog messages are displayed in the *System log* page of the web interface (see [“Chapter 2 - Web Interface – Introduction” on page 25](#) for more details).

► **To set the local syslog:**

1. In the *syslogMIB*, locate the *syslogMsgLocalMaxSeverity* variable.

This variable indicates which syslog message is processed by the Mediatrix 4102. Any syslog message with a severity value greater than the selected value is ignored.

- disabled
- critical
- error
- warning
- informational
- debug

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

The following are some of the messages the unit sends:

Table 137: Syslog Messages Examples

Event	Level	Message
The configuration update has been successful (configuration file fetching)	Informational	The specific configuration update succeeded.
The configuration update experienced an error and has not been completed (configuration file fetching)	Error	The specific configuration update failed.
The software update has been successful	Informational	The software update succeeded.
The software update experienced an error and has not been completed	Error	The software update failed.

2. Set the maximal number of syslog messages the Mediatrix 4102 handles in the *syslogMsgLocalMaxNbr* variable.

Modifying this value resets the messages.

If the Mediatrix 4102 sends a new syslog message and the maximum number of messages is reached, the oldest one is removed.

You can view the syslog messages in the following locations:

- In the *syslogLocalMsgTable* of the *syslogMIB*.
- In the *System log* page of the web interface.

The Mediatrix 4102 collects meaningful statistics that can be read via the RTP, MGCP, and NCS MIBs.

MGCP / NCS Statistics

MGCP / NCS statistics are related to the lines of the Mediatrix 4102:

- ▶ Number of active connections
- ▶ Number of total connections
- ▶ Average connection time

These statistics are located under the *mgcpStats* group of the *mgcpMIB* and the *ncsStats* group of the *ncsMIB*. See the *MIB Reference* manual for more details.

RTP Statistics

RTP statistics are related to the transmission of information and include, but are not limited to:

- ▶ Number of octets transmitted/received
- ▶ Number of packets transmitted/received
- ▶ Number of lost packets
- ▶ Percentage of lost packets
- ▶ Minimum, maximum and average Jitter interarrival time (time, in milliseconds, between the arrival of packets)
- ▶ Minimum, maximum and average latency time

These statistics are located under the *rtpStats* group of the *rtpMIB*. See the *MIB Reference* manual for more details.

Statistics Buffers

Each statistics has three different buffers in which they are collected:

Table 138: Statistics Buffers

Statistic	Description
Last connection	These are the statistics of the last completed connection.
Current	These are the statistics of the current connection. If using the Cumulated buffer, they are added to the cumulated statistics buffer and then reset.
Cumulated	These are the cumulated statistics of all the connections. Define a period of time and maximum number of periods you want to keep. For instance, you could define to keep the statistics for the last 24 periods of 1 hour.

How are Statistics Collected?

When collecting statistics, you can do so in two ways:

- ▶ Continuous collection of statistics.
In this case, the cumulated statistics are not used (disabled) and the current statistics are constantly updated.
- ▶ Collection of statistics for a defined period of time with a user-defined accuracy.
For instance, you could define to keep the statistics for the last 24 periods of 1 hour.

▶ To set statistics collection:

1. In the *sysConfigMIB*, locate the *sysConfigStats* group.
2. Set the period length you want to keep in the *sysConfigStatsPeriodLength* variable.
The length of a period may vary from 5 minutes to 24 hours, by 5-minutes sections. At expiration, the current statistics are added to the cumulated statistics buffer and then reset. Note that modifying the value of this variable resets statistics to 0.
3. Set the maximum number of periods to cumulate in the *sysConfigStatsNumberPeriods* variable.
The maximum number of periods cumulated is 24. If this variable is set to 0, statistics are collected indefinitely in the current variables. Note that modifying the value of this variable resets statistics to 0.

▶ To reset statistics:

1. In the *sysAdminMIB*, set the *sysAdminCommand* variable to **resetStats**.
This resets all cumulated call statistics.

Example

The following is an example with *sysConfigStatsNumberPeriods* = 3 and *sysConfigStatsPeriodLength* = 1 (5 minutes).

Table 139: Statistics Setting Example

Statistics	5-minutes sections					
	1	2	3	4	5	6
<i>rtpStatsCurrentTotalOctetsTransmitted</i>	50	30	60	40	100	50
<i>rtpStatsCumulatedTotalOctetsTransmitted</i>	0	50	80	140	130	200

1. 50 total octets transmitted in the first 5-minutes period.
2. 30 total octets transmitted in the second 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 50.
3. 60 total octets transmitted in the third 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 80.
4. 40 total octets transmitted in the fourth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 140.
5. 100 total octets transmitted in the fifth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable.

In the above example, the *rtpStatsCumulatedxx* variables always contain the statistics for the last 15 minutes (*sysConfigStatsNumberPeriods* X *sysConfigStatsPeriodLength*) accurate to 5 minutes (*sysConfigStatsPeriodLength*). This means that the statistics for the first 5-minutes period are dropped, for a cumulated total octets transmitted of 130.

6. 50 total octets transmitted in the sixth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable.
The statistics for the second 5-minutes period are dropped, for a cumulated total octets transmitted of 200.

Maximum Transmission Unit (MTU)

This chapter describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 4102.

What is MTU?

The *Maximum Transmission Unit* (MTU) is a parameter that determines the largest packet than can be transmitted by an IP interface (without it needing to be broken down into smaller units). Each interface used by TCP/IP may have a different MTU value specified.

The MTU should be larger than or equal to the largest packet you wish to transmit unfragmented. Note that this only prevents fragmentation locally. Some other link in the path may have a smaller MTU: the packet will be fragmented at that point, although some routers may refuse packets larger than their MTU.

Mediatrix 4102 MTU

The Mediatrix 4102 MTU is 1500 bytes, which is the Ethernet typical value.

Possible Hardware Problem

The implementation of the IEEE Standard 802.1q in the Mediatrix 4102 may have a minor problem because of hardware limitations.

802.1q increases the Ethernet frame header by 4 bytes, adding a Virtual LAN ID and a user_priority. This is useful to limit broadcasts that cross bridges, and it may also prioritize frames in the queuing algorithm of switches. However, it also increases the maximum possible size of Ethernet frames from 1518 to 1522 bytes, and this might not be handled adequately by every hardware.

A workaround is available for PCs running Windows to avoid sending 1522 bytes packets (note that this happens only in special and rare cases). The workaround is to reduce the MTU of the interface (the one that sends packets with 802.1q framing) by 4 bytes.

1. Use the registry editor (regedt32) and go to the key:
 Windows 2000 and later:
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
 \<ethernet adapter>
 Windows NT4 and 98:
 \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<ethernet
 adapter>\Parameters\Tcpip
 where <Ethernet adapter> can be found by using the command "ipconfig /all".
2. Add (or modify) a value named MTU of type REG_DWORD. Set it to 1496 (instead of 1500), in decimal. Restart the computer to have those changes in effect.
 In Windows 2000 and later this value is under the following key:
 - Key: *Tcpip\Parameters\Interfaces\ID* for Adapter2

- Value Type: REG_DWORD Number
 - Valid Range: 68 - the MTU of the underlying network
 - Default: 0xFFFFFFFF
 - Description: This parameter overrides the default MTU for a network interface. The MTU is the maximum packet size in bytes that the transport will transmit over the underlying network. The size includes the transport header. Note that an IP datagram may span multiple packets. Values larger than the default for the underlying network will result in the transport using the network default MTU. Values smaller than 68 will result in the transport using an MTU of 68.
3. To validate that the changes are correct, try to ping the Mediatrix 4102 with large packets once restarted:
`ping -l 2000`
- This will cause IP fragmentation, the first fragment being as large as the interface allows it. With the MTU reduced, you should now receive an answer. For more informations, see:
<http://support.microsoft.com/default.aspx?scid=kb;en-us;120642>.

You can experience some problems when connecting the Mediatrix 4102 to the network. The following section examines some of these problems and possible solutions.

A Syslog message lists the problems the Mediatrix 4102 encounters. You can see this message with the Syslog daemon.

This chapter covers the following types of issues:

- ▶ General Operation Issues
- ▶ Calling Issues
- ▶ Fax Issues
- ▶ Software Upgrade Issues
- ▶ SNMP Management Software Issues

General Operation Issues

The following are general operation issues you may encounter.

DESCRIPTION: Unit does not operate – All LEDs are OFF.



POSSIBLE CAUSE: Power is not fed to the unit.

SOLUTION: Check that:

- The power cord is connected to the electrical outlet.
- The power cord is fully inserted into the Mediatrix 4102 power socket.

DESCRIPTION: There is a long delay when starting the Mediatrix 4102.



POSSIBLE CAUSE: If any information is set to come from the DHCP server (for example, SNTP address), the restarting unit waits for a maximum period of two minutes if the DHCP server cannot be reached, even if most other settings are set to “static”.

This delay is caused by the Mediatrix 4102 that cannot function as configured if part of its configuration (the DHCP information) is unavailable.

The two minutes waiting period is an issue with switches that use the Spanning Tree Protocol. When this protocol is enabled, the restarting Mediatrix 4102 may be denied from the network for a certain time (about two minutes). The unit must not ignore transmission errors (i.e., timeouts) because these errors might be caused by the Spanning Tree Protocol.

SOLUTION: Media5 recommends to set up all information to use a static value, or have a DHCP server answer the requests. See [“Static Configuration” on page 57](#) for more details.

DESCRIPTION: I changed the IP address of my unit, but I can't reach the DHCP server anymore.

- **POSSIBLE CAUSE:** A subnet mask is used to determine to which subnet an IP address belongs. An IP address has two components, the network address and the host address. For example, let's consider the IP address 192.168.0.1. Assuming this is part of a Class B network, the first two numbers (192.168) represent the Class B network address, and the second two numbers (0.1) identify a particular host on this network.

Let's say you have the following information:

- Mediatix 4102 IP address: 192.168.0.1
- Subnet Mask: 255.255.0.0 (Class B)
- DHCP Server IP address: 192.168.0.20

If you happen to change the Mediatix 4102 IP address to 192.169.0.1, for instance, the subnet mask is still valid, but cannot reach your DHCP server anymore. Refer to subnet mask documentation for more details.

DESCRIPTION: Unable to reach the Mediatix 4102 after changing the Ethernet speed at run-time.

- **POSSIBLE CAUSE:** Some hubs cannot adapt completely their port speed at run-time.

SOLUTION: Always restart the Mediatix 4102 for the new setting to take effect. See ["Ethernet Connection Speed" on page 73](#) for more details.

DESCRIPTION: In the case where my NAT/Firewall device is connected to the *ComputerLAN* port of the Mediatix 4102 and I have a PC connected to the NAT/Firewall, the PC has limited web access in time.

- **POSSIBLE CAUSE:** The NAT/Firewall device does not support well the small DHCP lease time of the Mediatix 4102 (30 seconds).

SOLUTION: Modify the *ipRoutingDhcpServerLeaseTime* variable with a value greater than 30 seconds, for instance 3600 seconds (1 hour). See ["Enabling TAS" on page 122](#) for more details.

However, note that the downtime will be greater when the ISP gives another IP address. Try several values and find out what is the smallest setting for your NAT/firewall device.

DESCRIPTION: The PC connected to the *LAN* connector of the Mediatix 4102 cannot register to IGMP services.

- **POSSIBLE CAUSE:** The Mediatix 4102 does not support the IGMP (Internet Group Management Protocol) protocol.

SOLUTION: There are no solutions.

DESCRIPTION: When I install a Mediatix 4102 in an enterprise network and there is a PC connected to the *LAN* port, the PC will not receive the WINS Server.

- **POSSIBLE CAUSE:** The embedded DHCP server of the Mediatix 4102 does not support the WINS Server. See ["DHCP Server" on page 125](#) for more details.

SOLUTION: Disable the TAS feature as described in ["Enabling TAS" on page 122](#) because the IP address is not an issue in private networks.

DESCRIPTION: Setting the MIB variable *voicelfAdaptativeJitterBufferEnable* to **disable** has no effect.

■ **POSSIBLE CAUSE:** You cannot disable the adaptative jitter buffer on the Mediatrix 4102.

SOLUTION: If you set the *voicelfTargetJitterBufferLength* and *voicelfMaxJitterBufferLength* variables to the same value, you will have a non-adaptative jitter buffer. See [“Adaptative Jitter Buffer” on page 175](#) for more details.

DESCRIPTION: When I set values such as the User Name and Display Name, the value is not accepted and is reset to its default value once the Mediatrix 4102 restarts.

■ **POSSIBLE CAUSE:** When you enter values that contain non-standard English characters in entries that accept strings of characters, this invalidates the value and resets it to its default value. However, this may be visible only once the Mediatrix 4102 restarts.

SOLUTION: Make sure that your string of characters contain only characters that are part of the following ASCII characters list:

10 LF, line feed	62 >, greater than	94 ^, caret
13 CR, carriage return	63 ?, question mark	95 _, underscore
32 space	64 @, commercial at	96 `, back quote
33 !, exclamation mark	65 A	97 a
34 ", double quote	66 B	98 b
35 #, hash	67 C	99 c
36 \$, dollar	68 D	100 d
37 %, percent	69 E	101 e
38 &, ampersand	70 F	102 f
39 ', quote	71 G	103 g
40 (, open parenthesis	72 H	104 h
41), close parenthesis	73 I	105 i
42 *, asterisk	74 J	106 j
43 +, plus	75 K	107 k
44 ,, comma	76 L	108 l
45 -, minus	77 M	109 m
46 ., full stop	78 N	110 n
47 /, oblique stroke	79 O	111 o
48 0, zero	80 P	112 p
49 1	81 Q	113 q
50 2	82 R	114 r
51 3	83 S	115 s
52 4	84 T	116 t
53 5	85 U	117 u
54 6	86 V	118 v
55 7	87 W	119 w
56 8	88 X	120 x
57 9	89 Y	121 y
58 :, colon	90 Z	122 z
59 ;, semicolon	91 [, open square bracket	123 {, open curly bracket
60 <, less than	92 \, backslash	124 , vertical bar
61 =, equals	93], close square bracket	125 }, close curly bracket
		126 ~, tilde

DESCRIPTION: I am unable to access the LAN web page.

■ **POSSIBLE CAUSE:** With a PC connected to the Mediatrix 4102 and IP routing disabled on the unit, you enabled IP routing (see [“Enabling TAS” on page 122](#) for details). As a result, the ARP table of the PC's network interface is no longer valid. The ARP table on the PC kept the MAC address of the default gateway whereas it must be set to the Mediatrix 4102 MAC address when IP routing is enabled.

SOLUTION: Restart the PC.

DESCRIPTION: Media5 Technical Support personnel asked me to enable the PCM traces. How do I do it?

■ **POSSIBLE CAUSE:** PCM traces are an efficient tool to identify problems with:

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

SOLUTION: Do the following:

- a. Enable the PCM traces by setting the *mxDebugPcmCaptureEnable* MIB variable to **enable**.
- b. Set the destination IP address for the PCM traces in the *mxDebugPcmCaptureIpAddress* MIB variable.
 - This IP address does not have to be listening on ports 5001/2 - 6001/2, as it is easy to filter out ICMP "port unreachable" messages afterwards.
 - The PCM traces destination must be set so it can be recorded in a Wireshark capture on your network, normally sent to the PC doing the capture.
- c. Set the endpoint number on which to perform the PCM capture in the *mxDebugPcmCaptureEndpointNumber* variable.

For more details on the PCM traces, refer to *Technical Bulletin 0648 - PCM Traces*.

Calling Issues

The following are general calling issues you may encounter.

DESCRIPTION: Impossible to make a call.

If the following happens:

- ▶ Dial tone present.
- ▶ *Power* LED lit.
- ▶ LED lit.

■ **POSSIBLE CAUSE:** Network communication is not working.

SOLUTION: Check that:

- The LAN cable is securely connected to the Mediatrix 4102 and to the network connector.
- You did not connect a crossover network cable.

■ **POSSIBLE CAUSE:** Configurable parameters of the Mediatrix 4102 are not set properly.

SOLUTION: Refer to this manual for a complete description of the configurable Mediatrix 4102 parameters.

DESCRIPTION: Unable to establish a call from the Mediatrix 4102 to an endpoint such as an IP phone, a gateway or another access device.

- **POSSIBLE CAUSE:** When the Mediatrix 4102 – with its T.38 capability enabled – tries to establish a call with an endpoint that does not support T.38, this an endpoint rejects the call instead of ignoring the capability it does not support, i.e., T.38.

SOLUTION: Disable the T.38 capability in the Mediatrix 4102. See ["T.38 Fax" on page 183](#) for more details.

- **POSSIBLE CAUSE:** If the unit is running either in MGCP or NCS mode, the silence suppression settings may not be the same in the MIB and the Call Agent. These settings shall be identical.

SOLUTION:

- a. Modify the configuration of the *voicelfG711VoiceActivity DetectionEnable* MIB variable to have the same setting as the Call Agent.
- b. Restart the unit.

See ["Voice Activity Detection" on page 176](#) for more details.

Fax Issues

The following gives information pertaining to faxes.

DESCRIPTION: "Poor line condition" error during a fax transmission.

- **POSSIBLE CAUSE:** The analog transmission between the fax machine and the Mediatrix 4102 is flaky, preventing the fax transmission to terminate properly. This problem is known to occur with some fax machines and it can also occur with a few fax modems.

SOLUTION: Set the *Input sound level* to **-6 dB**. If this still does not solve the problem, try the **+6 dB** value. See ["User Gain" on page 179](#) for more details.

DESCRIPTION: Unable to send a fax in T.38 and Clear Channel.

- **POSSIBLE CAUSE:** To properly send faxes, both units must be configured with the same settings. If you are attempting to send a fax and the transmission fails, there could be many reasons for this, but most likely the fax codec settings are at fault. The following explains the logic behind fax transmissions.

When transmitting a fax, Unit A first verifies if Unit B supports the codec you have set in Unit A. If the codec is supported, the fax should be transmitted properly.

If the fax codec is not supported by Unit B, Unit A tries to find a common preferred G.711 clear channel codec between the two units. If Unit A finds one, it uses this common clear channel codec and the fax should be transmitted properly. If there are no common clear channel codecs between the units, the fax transmission fails.

SOLUTION: To avoid fax transmission problems, configure both units with the same T.38 and clear channel settings and the fax should be sent properly.

DESCRIPTION: Voice does not switch back to the original negotiated codec after a clear channel fax is performed.

- **POSSIBLE CAUSE:** The Mediatrix 4102 suffers from a limitation of its DSP. The Mediatrix 4102 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 4102 is not notified by the DSP. The unit thus stays in the clear channel codec and does not switch back to G.729.

SOLUTION: There is no solution.

DESCRIPTION: When using the Mediatrix 4102 with the Cyberguard SG530 broadband router, the router blocks fax transmissions.

- **POSSIBLE CAUSE:** Cyberguard Version 2.0.2 seems to be the problem.
- SOLUTION:** Upgrade the Cyberguard to version 2.1.3.
-

Software Upgrade Issues

The following are issues you may encounter when performing a software upgrade operation.

DESCRIPTION: An error occurs when the Mediatrix 4102 attempts to communicate with the image server.

- **POSSIBLE CAUSE:** The directory specified in the upgrade command does not exist or does not contain the files required for the software download process.

SOLUTION:

- Check the directory name.
- Be sure that the directory contains files. If not, extract them from the zip file again. See ["Download Procedure" on page 152](#) for more details.
- Be sure that the software server is running and properly configured.

- **POSSIBLE CAUSE:** The IP address of the software server is not the correct one.

SOLUTION:

- Check the given IP address.
 - Check the IP port.
-

DESCRIPTION: An error occurs when the Mediatrix 4102 attempts to transfer the software upgrade.

- **POSSIBLE CAUSE:** The Ethernet cable has become disconnected from the Mediatrix 4102 or the PC running the file transfer.

SOLUTION: Reconnect the cable and start again.

- **POSSIBLE CAUSE:** Power to the Mediatrix 4102 has been disrupted during the file transfer.

SOLUTION: Check the power connection to the Mediatrix 4102 and start again.

DESCRIPTION: The TFTP server does not recognize the download path and produces an error.

- **POSSIBLE CAUSE:** You should use the "/" character when defining the path to indicate sub-directories, i.e., *c:/temp/download*. However, some TFTP servers on the Windows operating system do not recognize the "/" character and produce an error.

SOLUTION: Use the "\" character in the path definition.

DESCRIPTION: Performing a software download takes an unusually long time.

- **POSSIBLE CAUSE:** If the following happens:
- Any information is set to come from the DHCP server (for example, the SNTP server address) and the DHCP server cannot be reached.
 - The primary software server address is invalid (either set by DHCP or static).

The unit tries to reach the primary software server without realizing that the address is invalid. It keeps trying for a few minutes, even if the download procedure fails.

This delay is caused by the Mediatrix 4102 that cannot function as configured if part of its configuration (the DHCP information) is unavailable. Furthermore, there is an issue with switches that use the Spanning Tree Protocol. When this protocol is enabled, the Mediatrix 4102 may be denied from the network for a certain time, which causes the long delay.

SOLUTION: Media5 recommends to set up all information to use a valid static value, or have a DHCP server answer the requests. See ["Static Configuration" on page 57](#) for more details.

SNMP Management Software Issues

The following are issues you may encounter when trying to contact the Mediatrix 4102 with a SNMP management software.

DESCRIPTION: The SNMP network management software cannot access the Mediatrix 4102.

- **POSSIBLE CAUSE:** The SNMP network management software does not have the proper Mediatrix 4102 information.

SOLUTION: Check that:

- The IP information for the Mediatrix 4102 is correctly configured.
- The Mediatrix 4102 was restarted after defining the IP information.
- The line through which you are trying to access the Mediatrix 4102 has been unlocked or is not the correct line. If it is locked, check the connections and network cabling for the connector.

Try to locate the Mediatrix 4102 IP address. If impossible, perform a recovery reset as indicated in section ["Reset / Default Switch" on page 20](#).

DESCRIPTION: There is no response when trying to access the Mediatrix 4102.

- **POSSIBLE CAUSE:** The Mediatrix 4102 speaks the three most common SNMP protocols: SNMPv1, SNMPv2c, and SNMPv3. If you try to access it by using any other protocol, it stays silent.

DESCRIPTION: The SNMP network manager does not receive Traps.

■ **POSSIBLE CAUSE:** The IP information is not correct.

SOLUTION: Check that the IP information (IP address + IP port) of the SNMP network manager software is correctly recorded by the Mediatrix 4102.

DESCRIPTION: When trying to set a variable, the Mediatrix 4102 does not respond, nor sends an error message.

■ **POSSIBLE CAUSE:** In secure management mode, the Mediatrix 4102 does not accept SNMPv1 and SNMPv2c SET requests. However, the MIB variables are viewable in any management mode (secure and not secure).

DESCRIPTION: When entering a value such as “.23” in a MIB variable, the Mediatrix 4102 returns a “Wrong value” error message.

■ **POSSIBLE CAUSE:** The Mediatrix 4102 does not support a value such as “.23”.

SOLUTION: Enter a value such as “0.23” instead.

DESCRIPTION: When I try to set a variable with a MIB configuration tool such as Media5 Unit Manager Network, nothing happens.

■ **POSSIBLE CAUSE:** The variable may be in a MIB that is located under the *mediatrixExperimental* branch of the MIB structure.

Media5 configuration tool – the Unit Manager Network – does not support MIBs that are located under the *mediatrixExperimental* branch of the MIB structure. The Unit Manager Network does not have specific tasks to manage variables in experimental MIBs.

The *mediatrixExperimental* branch is the area where objects and events in MIBs under development can be placed without fear of conflicting with other MIBs. When the items rooted under an experimental sub-tree are ready for release, they will be under a permanent branch.

Even though the Unit Manager Network can view experimental MIBs, SNMP operations may not work properly on them.

DESCRIPTION: After downgrading the software version, one or more MIB variables are “empty” (the Unit Manager Network shows an “unknown enumeration value”) and the Mediatrix 4102 uses the default value instead of the value I had set.

■ **POSSIBLE CAUSE:** The more recent version of the software has MIB variables that contain settings not available in the previous version. The Mediatrix 4102 cannot recognize the values and automatically uses the default value.

SOLUTION: Manually set the MIB variable to the value you want and restart the Mediatrix 4102.

DESCRIPTION: When viewing a table, the unit does not respond.

■ **POSSIBLE CAUSE:** It may take time to fill completely a table: from 1 to 5 seconds. This is normal, because the unit is an embedded device with limited processing power.

DESCRIPTION: Is it possible for a hacker to change the content of SNMPv3 variables once the Mediatrix 4102 is in secure mode management?

- **POSSIBLE CAUSE:** In secure management mode, the Mediatrix 4102 works in SNMPv1 read-only, SNMPv2c read-only, and SNMPv3 read/write. SNMP requests using the first two protocols are read-only, and tables used for setting up SNMPv3 users hide the passwords they carry. Because hackers do not know what password to use in SNMPv3 requests, they cannot access the Mediatrix 4102 with read-write permission.

Appendices

Page Left Intentionally Blank

Standards Compliance and Safety Information

This Appendix lists the various standards compliance of the Mediatrix 4102.

Standards Supported

The Mediatrix 4102 complies to the following standards:

Table 140: Standards Compliance

Category	Specification
Agency approvals	- European Union, CE mark (Declaration of Conformity) - FCC
Safety standards	- UL60950 - IEC 60950 (1st Edition 2001 With all national deviations)
Emissions	- FCC Part 15:1998 Class B - EN55022 (2006) Class B (With amendments A1 and A2) - EN61000-3-2 (2000) Harmonic current emissions - EN61000-3-3 (1995) Voltage fluctuations and flicker
Immunity	EN55024:1998 including the following: - EN61000-4-2 (1995), ESD - EN61000-4-3 (1996), Radiated RF - EN61000-4-4 (1995), Burst Transients - EN61000-4-5 (1995), Surge - EN61000-4-6 (1996), Conducted RF - EN61000-4-11 (1995), Voltage Dips and Interruptions



Note: The standards compliance of the Mediatrix 4102 are printed on a sticker located on the bottom of the unit.

Disclaimers

The following are the disclaimers related to the Mediatrix 4102.

Federal Communications Commission (FCC) Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ▶ Reorient or relocate the receiving antenna.
- ▶ Increase the separation between the equipment and receiver.
- ▶ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ▶ Consult the dealer or an experienced radio/TV technician for help



Note: Any changes or modifications not expressly approved by Media5 could void the user's authority to operate the equipment.

CE Marking



DECLARATION OF CONFORMITY

We Media5 Corporation located at 4229 Garlock st. Sherbrooke, Québec, Canada J1L 2C8 declare that for the hereinafter mentioned product the presumption of conformity with the applicable essential requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN

PARLIAMENT (RTTE DIRECTIVE) is given.

Any unauthorized modification of the product voids this declaration.

For a copy of the original signed Declaration Of Conformity please contact Media5 at the above address.

RoHS China

这个文件涉及的是在中华人民共和国境内进口或销售的电子信息产品
Include this document with all Electronic Information Products
imported or sold in the People’s Republic of China

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr ⁶⁺)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	×	×
集成电路 (Integrated Circuit)	×	○	×	○	×	×
○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T-11363 - 2006规定的限量要求以下。 Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T-11363 - 2006 standard. ×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量可能超出SJ/T-11363 - 2006规定的限量要求。 Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts might exceed the relevant threshold of the SJ/T-11363 - 2006 standard.						

除非另外特别的标注,此标志为针对所涉及产品的环保使用期限标志. 某些可更换的零部件会有一个不同的环保使用期限(例如,电池单元模块)贴在其产品上.

此环保使用期限只适用于产品是在产品手册中所规定的条件下工作.

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain field-replaceable parts have a different EFUP (for example, battery modules) and so are marked to reflect such.

The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

Translated Warning Definition

The following information provides an explanation of the symbols which appear on the Mediatrix 4102 and in the documentation for the product.



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 familiar with standard practices for preventing accidents.

Waarschuwing: Dit waarschuwingssymbool betekent gevaar. U overtreedt in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus: Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention: Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung: Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza: Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel: Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso: Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Advertencia!: Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning!: Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Safety Warnings

This section lists the following safety warnings:

- ▶ Circuit Breaker (20A) Warning
- ▶ TN Power Warning
- ▶ Product Disposal Warning
- ▶ No. 26 AWG Warning
- ▶ WAN, LAN, Phone-Fax 1 and Phone-Fax 2 Connectors Warning
- ▶ LAN and FXS Ports Connectors Warning
- ▶ Socket Outlet Warning

Circuit Breaker (20A) Warning



Warning: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 20A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

TN Power Warning



Warning: The device is designed to work with TN power systems.

Product Disposal Warning



Warning: Ultimate disposal of this product should be handled according to all national laws and regulations.

No. 26 AWG Warning



Warning: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

WAN, LAN, Phone-Fax 1 and Phone-Fax 2 Connectors Warning



Warning: Do not connect the *WAN*, *LAN*, *Phone-Fax 1* and *Phone-Fax 2* connectors directly to the Public Switched Telephone Network (PSTN), to an off premise application, an out of plant application, any exposed plant application, or to any equipment other than the intended application, connection may result in a safety hazard, and/or defective operation and/or equipment damage.

Exposed plant means where any portion of the circuit is subject to accidental contact with electric lighting or power conductors operating at a voltage exceeding 300V between conductors or is subject to lightning strikes.

LAN and FXS Ports Connectors Warning



Warning: Do not connect the LAN and the FXS ports connectors directly to the Public Switched Telephone Network (PSTN), to an off premise application, an out of plant application, any exposed plant application, or to any equipment other than the intended application, connection may result in a safety hazard, and/or defective operation and/or equipment damage.

Exposed plant means where any portion of the circuit is subject to accidental contact with electric lighting or power conductors operating at a voltage exceeding 300V between conductors or is subject to lightning strikes.

Socket Outlet Warning



Warning: The socket outlet, if used, shall be located near the equipment and shall be easily accessible by the user.

Safety Recommendations

To insure general safety follow these guidelines:

- ▶ Do not open or disassemble this product.
- ▶ Do not get this product wet or pour liquids into it.
- ▶ Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.



Caution: When using this equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

Standard Hardware Information

The specifications and information regarding this product are subject to change without notice. Every effort is made to ensure the accuracy of this document. Because of ongoing product improvements and revisions, Media5 cannot guarantee its accuracy, nor can be responsible for errors or omissions. Please contact your Media5 sales representative to obtain the latest version of the technical specifications.

Industry Standard Protocols

The Mediatrix 4102 has been designed to support all major industry standards used today, as well as those that will eventually be implemented at a later date. Because of this specific design characteristic, the Mediatrix 4102 can be integrated with existing telephone, fax and data equipment such as PCs and routers.

Table 141: Industry Standard Protocols

Parameter	Description
Vocoders	- G.711 (a-law, u-law) - G.726 (40, 32, 24, 16 kbit/s) - G.729a - G.729ab
IP Telephony Protocols	- MGCP - RFC 3435 - PacketCable™ network-based call signaling (NCS) protocol, PKT-SP-EC-MGCP-I01-990312
Real-Time Transport Protocols	RTP/RTCP - RFC 1889, RFC 1890, RFC 2833, RFC 3389
Network Management Protocols	- SNMPv3 - DHCP - RFC 2131, RFC 2132 - TFTP - RFC 1350, RFC 2347, RFC 2348, RFC 2349 - Syslog - RFC 3164HTTP 1.0 - RFC 1945 - HTTP 1.1 - RFC 2616 - Basic and digest HTTP authentication - RFC 2617
Data Features	- PPPoE client - RFC 1332, RFC 1661, RFC 1334, RFC 1994, RFC 2516, RFC 1471, RFC 1472, RFC 1473, RFC 1877. Note: some PPPoE RFCs are implemented partially. - TFTP or HTTP auto-provisioning - Transparent IP address sharing (Media5 patent pending technology allowing the same IP address to be shared between both Ethernet ports and distinguishing voice traffic from data traffic) - DHCP server - STUN client

Table 141: Industry Standard Protocols (Continued)

Parameter	Description
QoS	• ToS • DiffServ • 802.1p • 802.1Q • STUN - RFC 3489

Hardware Features

Display

- ▶ Power LED
- ▶ LANactivity LED
- ▶ Activity/In-Use LED indication on FXS ports
- ▶ Ready LED

Interfaces

- ▶ 2 x RJ-11 connectors, analog phone/fax (FXS) interface.
- ▶ 2 x RJ-45 connectors, 10/100 BaseT Ethernet access (autosense: up to 100 Mbits).

Power

- ▶ External 12 Vdc power supply (wall plug or desktop, based on country/area model).
- ▶ Seamless switch over period if the client UPS detects a power loss and activates within ms.

Casing / Installation

- ▶ Casing: Desktop (Plastic ABS UL94).
- ▶ Installation: The Mediatrix 4102 is designed for the desktop or can be wall-mountable.

Product Architecture Details

- ▶ Supports two concurrent communications using any vocoders.
- ▶ DSP-based DTMF detection generation.
- ▶ DSP-based fax/data relay.
- ▶ Embedded operating system with 32-bit real-time multitasking Kernel.
- ▶ Embedded IPv4 TCP/IP stack with configurable QoS implemented by:
 - ToS byte at Network layer 3
 - 802.1p at Data Link layer 2
- ▶ Network parameters assigned via DHCP

Real Time Fax Router Technical Specifications

Automatic selection between voice and fax.

Table 142: Fax Technical Specifications

Parameter	Description
Ethernet	10/100 BaseT Ethernet
Data Link	Ethernet II
Network	IP (Internet Protocol)
Transport	TCP / UDP
Protocols	Group 3 Fax Clear channel (G.711), G.726, or T.38 Real Time Fax Over IP protocol Stack
Fax Data Compression	MH
Fax Transmission	Up to 14.4 kbps

Analog Line Interface (FXS)

- ▶ RJ-11 connectors
- ▶ Direct connection to a fax machine or telephone (Internal installation and internal cabling)
- ▶ DC feeding of the access line protected for over voltage
- ▶ Loop current detection and hook flash detection capable
- ▶ Generation of Selective Ring

Table 143: Analog Line Interface

Parameter	Description
Trunk Type	Loop Start: capable of Wink and Immediate signalization
Ring Source	50 VRMS max @ 20 up to 50 Hz (selectable) sine signal
Nominal Impedance	BellCore compliant 600/900 ohms default setting. Impedance Software Configurable.
Ring Drive Capacity	Up to 4 ringer equivalents (4 RENs) per port.
Loop Current Range	15 to 32 mA factory set. Default 20 mA regulated.
Ring Trip Detection Time	2 ring cycles max
On Hook Voltage	-48 VDC
Frequency Response	200 Hz to 3400 Hz ± 3 dB (Tx/Rx)
Return Loss	500-3200 Hz: 30 dB

Audio Specifications

- ▶ Software input and output level adjustable within the range of -30 dB to +20 dB.
- ▶ Software-adjustable dynamic and static jitter buffer protection.
- ▶ Programmable by country: Call progress tone generation including dial tone, busy tone, ringback and error tones.
- ▶ DSP-based echo control device.
- ▶ Silence detection/suppression level software adjustable.

DTMF Tone Detection

Table 144: DTMF Tone Detection

Parameter	Description
16-Digit DTMF Decoding	0 to 9, *, #, A, B, C, D
Permitted Amplitude Tilt	High frequency can be +2 dB to -8 dB relative to low frequency
Dynamic Range	-35 dBm to +3 dBm per tone
Frequency Accept	± 1.5% of nominal frequencies
Minimum Tone Duration	40 ms, can be increased with software configuration
Interdigit Timing	Detects like digits with a 40 ms interdigit delay

DTMF Tone Generation

Table 145: DTMF Tone Generation

Parameter	Description
Per Frequency Nominal	-6 dBm to -4 dBm
Frequency Deviation	Within 1.5% of nominal values

MTBF Value

The estimated Mean Time Before Failure (MTBF) value of the Mediatix 4102 is 750,000 hours at 25 degrees Celsius ambient temperature (excluding the power adaptor). It has been defined using RelCalc v5.0, Bellcore method (LimitedStress - Method I, Case 3).

Power Consumption

Measurements at the DC input

Table 146: Power Consumption at the DC Input

Parameter	Description
Idle Mode, 12Vdc	240 mA
2 Extensions Off-Hook: 12Vdc	450 mA
2 Extensions ringing: 12Vdc	475 mA

Operating Environment

Table 147: Operating Environment

Parameter	Description
Operating Temperature	-40°C to 85°C
Humidity	Up to 85 %, non-condensing
Storage	-40°C to +85°C

Dimensions and Weight

Table 148: Dimensions and Weight

Parameter	Description
Dimensions	3.1 cm x 12.7 cm x 9.9 cm - 1.2 in. x 5 in. x 3.9 in. (approx.)
Weight	170 g (0.37 lb)

Warranty

All Media5 products carry Media5's standard three-year hardware and software warranty. An extended warranty is available.



Cabling Considerations

This Appendix describes the pin-to-pin connections for cables used with the Mediatix 4102.



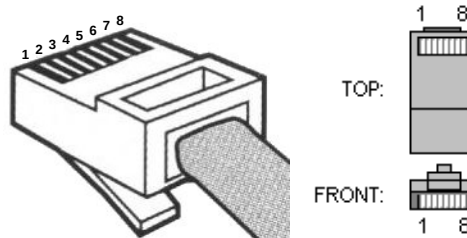
Warning: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

RJ-45 Cable

The RJ-45 connector is commonly used for network cabling and for telephony applications. It is used to wire both ends identically so the signals pass straight through.

RJ-45 cabling is also known as Twisted-pair Ethernet (TPE), Unshielded twisted pair (UTP) and 10/100 Base-T.

Figure 46: RJ-45 Cable



Straight Through Cable

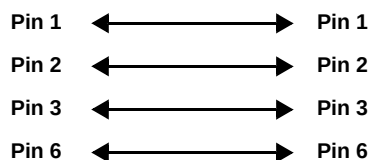
A RJ-45 straight through cable is used to connect a computer to a network device. For example straight through cables are the type of cables that connect a computer to a network hub, network switch, and network routers.

Table 149: RJ-45 Pinout Information

Pin #	Function	Colour Coding	
		EIA/TIA 568A	EIA/TIA 568B AT&T 258A
1	Transmit +	White with green stripe	White with orange stripe
2	Transmit -	Green with white stripe or solid green	Orange with white stripe or solid orange
3	Receive +	White with orange stripe	White with green stripe
4	N/A	Blue with white stripe or solid blue	Blue with white stripe or solid blue
5	N/A	White with blue stripe	White with blue stripe
6	Receive -	Orange with white stripe or solid orange	Green with white stripe or solid green
7	N/A	White with brown stripe or solid brown	White with brown stripe or solid brown
8	N/A	Brown with white stripe or solid brown	Brown with white stripe or solid brown

The RJ-45 cable uses two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 1 & 2 are on one twisted pair and pins 3 & 6 are on a second pair according to common wiring standards which meet the EIA/TIA T568A and T568B requirements.

Figure 47: Straight Through Connectivity



Pin Name And Function

The following is the meaning of each pin in a RJ-45 cable.

Table 150: Pin Name and Function

Pin #	Name	Function
1	Transmit Data Plus	The positive signal for the TD differential pair. This signal contains the serial output data stream transmitted onto the network.
2	Transmit Data Minus	The negative signal for the TD differential pair. This contains the same output as pin 1.
3	Receive Data Plus	The positive signal for the RD differential pair. This signal contains the serial input data stream received from the network.
4	not connected	
5	not connected	
6	Receive data minus	The negative signal for the RD differential pair. This signal contains the same input as pin 3.
7	not connected	
8	not connected	

Crossover Cable

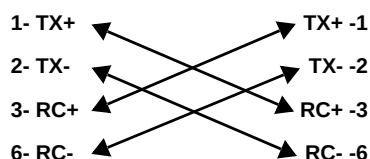
A RJ-45 crossover cable is used when only two systems are to be connected to each other, peer to peer, at the Ethernet Cards by “crossing over” (reversing) their respective pin contacts. An example would be connecting two computers together to create a network. The crossover eliminates the need for a hub when connecting two computers. A crossover cable may also be required when connecting a hub to a hub, or a transceiver to transceiver or repeater to repeater. When connecting a hub to a transceiver, a straight through cable is always used.



Note: This is not an IEEE supported configuration and should be used for test purposes only.

A crossover cable is sometimes called a null modem. The coloured wires at either end are put into different pin numbers, or crossed over.

Figure 48: Crossover Connectivity



RJ-11 (Telephone) Cable

The RJ-11 cable is commonly used for telephone connection.



Caution: Do not plug a phone jack connector into an RJ-45 port.

Wiring Conventions

For telephone connections, a cable requires one pair of wires. Each wire is identified by different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-11 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-11 connectors in a specific orientation. The following figure illustrates how the pins on the RJ-11 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

Figure 49: RJ-11 Connector Pin Numbers

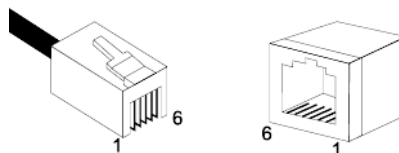


Table 151: RJ-11 Pinout Information

Pin #	Function
1	Not used
2	Not used
3	Ring
4	Tip
5	Not used
6	Not used

The RJ-11 pair of wires is wired so that pins 3 and 4 are connected to the Ring and Tip, which meets the following requirements:

- ▶ EIA/TIA-IS 968
- ▶ CS-03 Issue 8, Part III requirements.



Warning: The RJ-11 cable should comply with UL 1863 and CSA C22.2 No 233 standards.



Country-Specific Parameters

The following parameters differ depending on the country in which you are.

Definitions

The following are some useful definitions.

Table 152: Definitions

Term	Description
Dial Tone	Indicates the line is ready to receive dialing.
Busy Tone	Indicates the line or equipment is in use, engaged or occupied.
Ringback Tone	Indicates the called line is ringing out.
Special Information Tone	Identifies network-provided announcements.
Stutter Dial Tone	Notifies the user that they have a voice mail message when the phone does not or cannot have a message-waiting light.
Confirmation Tone	Confirms a command performed by the user (such as activate a service).
Receiver Off Hook (ROH) Tone	Indicates that the telephone is not hung up correctly.
Message Waiting Indicator Tone	Indicates there is a message waiting somewhere for the owner of the phone.
Reorder Tone	Indicates that all switching paths are busy, all toll trunks are busy, there are equipment blockages, the caller dialed an unassigned code, or the digits dialed got messed up along the way.
Call Waiting Tone	Indicates someone is trying to call.
Alternative Call Waiting Tone	Indicates someone is trying to call.
Network Congestion Tone	Indicates that all switching paths are busy, all toll trunks are busy, or there are equipment blockages.
Intercept Tone	Indicates that you have dialed incorrectly or that the feature you've requested is not available on your terminal.
Preemption Tone	In military telephone systems, a distinctive tone that is used to indicate to connected users, i.e., subscribers, that their call has been preempted by a call of higher precedence.

Supported MGCP/NCS Signals

The following are the different MGCP and NCS signals supported by the Mediatrix 4102.

Table 153: Supported MGCP/NCS Signals

Tone	MGCP Signal	NCS Signal
Dial Tone	L/dl	dl
Busy Tone	L/bz	bz
Ringback Tone	G/rt, G/rbk	rt, rbk
Special Information Tone	L/sit	sit
Stutter Dial Tone	L/sl, L/sdl	sl, sdl
Confirmation Tone	G/cf	cf
Receiver Off Hook (ROH) Tone	L/ot	ot
Message Waiting Indicator Tone	L/mwi	mwi
Reorder Tone	L/ro	ro
Call Waiting Tone	L/wt	wt
Alternative Call Waiting Tone	L/wt1, L/wt2, L/wt3, L/wt4	wt1, wt2, wt3, wt4
Network Congestion Tone	G/cg	cg
Intercept Tone	G/it	it
Preemption Tone	G/pt	pt
Ring	L/rg	rg

Conventions

The following conventions apply to this Appendix.

Frequencies

- ▶ Symbol "*" means modulated. For instance: 425 Hz * 25 means 425 Hz modulated at 25 Hz.
- ▶ Symbol "+" means added. For instance: 425 Hz + 330 Hz means that both 425 Hz and 330 Hz sines are played at the same time.
- ▶ When a tone is composed of more than one frequency, if not otherwise specified, the given electrical level applies to each frequency taken separately.

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

When representing an impedance, the following applies:

- ▶ Symbol "/" means parallel.
- ▶ Symbol "+" means serial.

Furthermore, there are two types of impedances:

- ▶ Input Impedance
- ▶ Terminal Balance Return Loss (TBRL) Impedance

Input Impedance

Impedance of the Mediatrix 4102 at the Tip and Ring wires.

Terminal Balance Return Loss (TBRL) Impedance

Balance return loss attributable to transmission loss between two points. It is used to characterize an impedance balancing property of the 2-wire analog equipment port.

Each country has its own definition of the TBRL value. For instance, in North America, TIA/EIA 464 (and TIA/EIA 912) define two TBRL values:

- ▶ 600 Ω for “on-premise” or short loop ports.
- ▶ 350 Ω + (1000 Ω || 21 nF) for “off-premise” or long loop ports.

A wire length above 2.5 km is considered long loop according to TIA/EIA 912 section 6.4 (7)(b)).

In Europe, ETSI 300 439 also mentions a TBRL value. However, most European countries have different requirements regarding the TBRL Impedance. This is also true for other countries around the world. Each one of them has different requirements.

Line Attenuation

Values are given in dBr (decibel relative):

- ▶ A “+” for input means that the digital side is attenuated by x decibels relative to the analog side.
- ▶ A “+” for output means that the analog side is amplified by x decibels relative to the digital side.
- ▶ A “-” for input means that the digital side is amplified by x decibels relative to the analog side.
- ▶ A “-” for output means that the analog side is attenuated by x decibels relative to the digital side.

On-Off Sequences

Values in bold are “on” cycles, where tones are audible. Values in normal style are “off” cycles, where tones are not audible. When not otherwise specified, sequences repeat forever. A “x” symbol means that the sequences between parenthesis is repeated x times. The next cycle(s) repeat forever, unless otherwise specified. Values are in seconds.

For instance:

3*(**0.1** - 0.1) then **0.6** - 1.0 - **0.2** - 0.2

means that the 0.1s on and 0.1s off sequence is repeated 3 times, afterwards the 0.6s on, 1.0s off, 0.2s on and 0.2s off sequence repeats forever.

Australia

The following parameters apply if you have selected Australia as location.

Australia 1

The following parameters apply if you have selected Australia1 as location.

Table 154: Australia 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	CONTINUOUS	-18 dBm
Busy Tone	400 Hz	0.375 – 0.375	-18 dBm
Ringback Tone	425 Hz * 17	0.4 – 0.2, 0.4 – 2.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	CONTINUOUS	-18 dBm
Confirmation Tone	450 Hz	(0.15 – 0.15 – 0.15) x 2 End	-18 dBm
Receiver Off Hook (ROH) Tone	1400+2067+2467+2600 Hz	0.1 – 0.1	-21 dBm
Message Waiting Indicator Tone	425 Hz * 25	0.1 – 0.04, repeated during 10 seconds	-18 dBm
Reorder Tone	425 Hz	2.5 – 0.5	-18 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Intercept Tone	425 Hz	CONTINUOUS	-18 dBm
Preemption Tone	425 Hz	0.8	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 2.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6 dBr

Australia 2

The following parameters apply if you have selected Australia2 as location.

Table 155: Australia 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	CONTINUOUS	-18 dBm
Busy Tone	400 Hz	0.375 – 0.375	-18 dBm
Ringback Tone	425 Hz * 17	0.4 – 0.2, 0.4 – 2.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	CONTINUOUS	-18 dBm
Confirmation Tone	450 Hz	(0.15 – 0.15 – 0.15) x 2 End	-18 dBm
Receiver Off Hook (ROH) Tone	1400+2067+2467+2600 Hz	0.1 – 0.1	-21 dBm
Message Waiting Indicator Tone	425 Hz * 25	0.1 – 0.04, repeated during 10 seconds	-18 dBm
Reorder Tone	425 Hz	2.5 – 0.5	-18 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	400 Hz	0.375 – 0.375	-18 dBm
Intercept Tone	425 Hz	CONTINUOUS	-18 dBm
Preemption Tone	425 Hz	0.8	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 2.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-6 dBr

Austria

The following parameters apply if you have selected Austria as location.

Austria 1

The following parameters apply if you have selected Austria1 as location.

Table 156: Austria Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	CONTINUOUS	-20 dBm
Busy Tone	450 Hz	0.3 – 0.3	-20 dBm
Ringback Tone	450 Hz	1.0 – 5.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Stutter Dial Tone	450 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-20 dBm
Confirmation Tone	450 Hz	(0.1 – 0.1) x 3 End	-20 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	450 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-20 dBm
Reorder Tone	450 Hz	0.3 – 0.3	-20 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	450 Hz	0.3 – 0.3	-20 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	1.0 – 5.0	
Input Impedance	270 Ω + 750 Ω // 150 nF		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr

Austria 2

The following parameters apply if you have selected Austria2 as location.

Table 157: Austria 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	420 Hz	CONTINUOUS	-20 dBm
Busy Tone	420 Hz	0.4 – 0.4	-20 dBm
Ringback Tone	420 Hz	1.0 – 5.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Stutter Dial Tone	380 + 420 Hz	CONTINUOUS	-20 dBm
Confirmation Tone	420 Hz	(0.1 – 0.1) x 3 End	-20 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	420 Hz	(0.1 – 0.1) x 10 CONTINUOUS	-20 dBm
Reorder Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	420 Hz 440 Hz 440 Hz 440 Hz	0.04 – 1.95 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-20 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	420 Hz	0.2 – 0.2	-20 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	1.0 – 5.0	
Input Impedance	270 Ω + 750 Ω // 150 nF		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr

China

The following parameters apply if you have selected China as location.

Table 158: China Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	CONTINUOUS	-10 dBm
Busy Tone	450 Hz	0.35 – 0.35	-10 dBm
Ringback Tone	450 Hz	1.0 – 4.0	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-10 dBm
Stutter Dial Tone	450 Hz	0.4 – 0.04	-10 dBm
Confirmation Tone	450 Hz	(0.1 – 0.1) x 3, End	-10 dBm
Receiver Off Hook (ROH) Tone	950 Hz 950 Hz 950 Hz 950 Hz	15.0 – 15.0 – 15.0 15.0 – 15.0 – 15.0 15.0 – 15.0 – 15.0 15.0 – 15.0 – 15.0 – CONTINUOUS	-25 dBm -16 dBm -8 dBm -6 dBm
Message Waiting Indicator Tone	450 Hz	0.4 – 0.04	-10 dBm
Reorder Tone	450 Hz	0.1 – 0.1, 0.1 – 0.1, 0.1 – 0.1, 0.4 – 0.4	-10 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	450 Hz	0.7 – 0.7	-10 dBm
Intercept Tone	450 Hz	0.2 – 0.2, 0.2 – 0.6	-20 dBm
Preemption Tone	450 Hz	0.2 – 0.2, 0.2 – 0.6	-20 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

France

The following parameters apply if you have selected France as location.

Table 159: France Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	440 Hz	CONTINUOUS	-16.9 dBm
Busy Tone	440 Hz	0.5 – 0.5	-19.9 dBm
Ringback Tone	440 Hz	1.5 – 3.5	-19.9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	(3 x 0.3 – 2 x 0.03) – 1.0	-19.9 dBm
Stutter Dial Tone	440 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-16.9 dBm
Confirmation Tone	440 Hz	(0.1 – 0.1) x 3, End	-16.9 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	440 Hz	(0.1 – 0.1) x 10	-16.9 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	440 Hz	0.25 – 0.25	-19.9 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	1.5 – 3.5	
Input Impedance	215 Ω + 1000 Ω // 137 nF		
FXS Line Attenuation (Input)			+1.9 dBr
FXS Line Attenuation (Output)			-8.9 dBr

Germany

The following parameters apply if you have selected Germany as location.

Germany 1

The following parameters apply if you have selected Germany 1 as location.

Table 160: Germany 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-16 dBm
Busy Tone	425 Hz	0.48 – 0.48	-16 dBm
Ringback Tone	425 Hz	1.0 – 5.0	-16 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-16 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-16 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10	-16 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.24 – 0.24	-16 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr

Germany 2

The following parameters apply if you have selected Germany 2 as location.

Table 161: Germany 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-16 dBm
Busy Tone	425 Hz	0.48 – 0.48	-16 dBm
Ringback Tone	425 Hz	1.0 – 5.0	-16 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-16 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-16 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10	-13 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.24 – 0.24	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Hong Kong

The following parameters apply if you have selected Hong Kong as location.

Table 162: Hong Kong Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350 + 440 Hz	CONTINUOUS	-13 dBm
Busy Tone	480 + 620 Hz	0.5 – 0.5	-13 dBm
Ringback Tone	440 + 480 Hz	0.4 – 0.2, 0.4 – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-16 dBm
Stutter Dial Tone	350 + 440 Hz	(0.1 – 0.1) x 20, CONTINUOUS	-16 dBm
Confirmation Tone	350 + 440 Hz	0.1 – 0.1, 0.3 – End	-16 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	350 + 440 Hz	(0.2 – 0.2, 0.5 – 0.2) x 4, CONTINUOUS	-16 dBm
Reorder Tone	480 + 620 Hz	CONTINUOUS	-13 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	480 + 620 Hz	0.25 – 0.25	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 3.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Indonesia

The following parameters apply if you have selected Indonesia as location.

Table 163: Indonesia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-9 dBm
Busy Tone	425 Hz	0.5 – 0.5	-9 dBm
Ringback Tone	425 Hz	1.0 – 4.0	-9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 – 0.03, 0.33 – 0.03, 0.33 – 1.0	-9 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-9 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-9 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	950 Hz	0.33 – 0.03	-9 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.25 – 0.25	-9 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr

Israel

The following parameters apply if you have selected Israel as location.

Table 164: Israel Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	CONTINUOUS	-15 dBm
Busy Tone	400 Hz	0.5 – 0.5	-15 dBm
Ringback Tone	400 Hz	1.0 – 3.0	-15 dBm
Special Information Tone	975 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-15 dBm
Stutter Dial Tone	400 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-15 dBm
Confirmation Tone	400 Hz	0.17 – 0.14, 0.34	-15 dBm
Receiver Off Hook (ROH) Tone	1440+2060+2452+2600 Hz	0.12 – 0.88	-20 dBm
Message Waiting Indicator Tone	400 Hz	(0.16 – 0.16) x 10, CONTINUOUS	-15 dBm
Reorder Tone	1000 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-15 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	400 Hz	0.25 – 0.25	-15 dBm
Preemption Tone	400 Hz	0.1 – 0.1, 0.1 – 0.1, 0.6 – 3.0	-15 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 3.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Italy

The following parameters apply if you have selected Italy as location.

Table 165: Italy Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	0.2 – 0.2, 0.6 – 1.0	-13 dBm
Busy Tone	425 Hz	0.2 – 0.2	-13 dBm
Ringback Tone	425 Hz	1.0 – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, 0.2 – 0.2, 0.6 – 1.0	-13 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10, 0.2 – 0.2, 0.6 – 1.0	-13 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.2 – 0.2	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	180 Ω + 630 Ω // 60 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Japan

The following parameters apply if you have selected Japan as location.

Table 166: Japan Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	CONTINUOUS	-13 dBm
Busy Tone	400 Hz	0.5 – 0.5	-13 dBm
Ringback Tone	400 Hz * 16	1.0 – 2.0	-16 dBm
Special Information Tone	400 Hz	0.1 – 0.1	-13 dBm
Stutter Dial Tone	400 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-13 dBm
Confirmation Tone	400 Hz	(0.1 – 0.1) x 3, End	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	400 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-13 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	400 Hz	0.5 – 0.5	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	1.0 – 2.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Malaysia

The following parameters apply if you have selected Malaysia as location.

Table 167: Malaysia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-14 dBm
Busy Tone	425 Hz	0.5 – 0.5	-18 dBm
Ringback Tone	425 Hz	0.4 – 0.2, 0.4 – 2.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	1.0 1.0 1.0 – 1.0	-14 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-14 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3 End	-14 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-14 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0. – 0.25	-18 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 2.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Netherlands

The following parameters apply if you have selected Netherlands as location.

Table 168: Netherlands Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-17 dBm
Busy Tone	425 Hz	0.5 – 0.5	-17 dBm
Ringback Tone	425 Hz	1.0 – 4.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-17 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-17 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10 CONTINUOUS	-17 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.25 – 0.25	-17 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	270 Ω + 750 Ω // 150 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

North America

The following parameters apply if you have selected North America as location.

North America 1

The following parameters apply if you have selected North America 1 as location.

Table 169: North America 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	CONTINUOUS	-17 dBm
Busy Tone	480+620 Hz	0.5 – 0.5	-21 dBm
Ringback Tone	440+480 Hz	2.0 – 4.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-14 dBm
Stutter Dial Tone	350+440 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-17 dBm
Confirmation Tone	350+440 Hz	(0.1 – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	350+440 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-17 dBm
Reorder Tone	480+620 Hz	0.3 – 0.2	-21 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	480+620 Hz	0.25 – 0.25	-21 dBm
Intercept Tone	440 Hz 620 Hz	0.25 – 0.25 0.5 – 0.5	-14 dBm -14 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	2.0 – 4.0	
Input Impedance	600 Ω		
Tbri-Impedance ^a	600 Ω		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr

a. TBRL-Impedance for “on-premise” or short loop ports.

North America 2

The following parameters apply if you have selected North America 2 as location.

Table 170: North America 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	CONTINUOUS	-17 dBm
Busy Tone	480+620 Hz	0.5 – 0.5	-21 dBm
Ringback Tone	440+480 Hz	2.0 – 4.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-14 dBm
Stutter Dial Tone	350+440 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-17 dBm
Confirmation Tone	350+440 Hz	(0.1 – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	350+440 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-17 dBm
Reorder Tone	480+620 Hz	0.3 – 0.2	-21 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	480+620 Hz	0.25 – 0.25	-21 dBm
Intercept Tone	440 Hz 620 Hz	0.25 – 0.25 0.5 – 0.5	-14 dBm -14 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	2.0 – 4.0	
Input Impedance	600 Ω		
Tbri-Impedance ^a	350 Ω + 1000 Ω // 210 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			0 dBr

a. TBRL-Impedance for “off-premise” or long loop ports (wire length longer than 2.5 km).

Russia

The following parameters apply if you have selected Russia as location.

Table 171: Russia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-10 dBm
Busy Tone	425 Hz	0.4 – 0.4	-10 dBm
Ringback Tone	425 Hz	0.8 – 3.2	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-17 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, End	-10 dBm
Confirmation Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	0.1 – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Receiver Off Hook (ROH) Tone	425 Hz	3 x (0.1 – 0.1), CONTINUOUS	-10 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10 CONTINUOUS	-10 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.2 – 0.2	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	0.8 – 3.2	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			+2 dBr
FXS Line Attenuation (Output)			-2 dBr

Spain

The following parameters apply if you have selected Spain as location.

Table 172: Spain Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-10 dBm
Busy Tone	425 Hz	0.2 – 0.2	-13 dBm
Ringback Tone	425 Hz	1.5 – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-10 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-10 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-10 dBm
Reorder Tone	425 Hz	0.2 – 0.2, 0.2 – 0.2, 0.2 – 0.6	-13 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.2 – 0.2, 0.2 – 0.2, 0.2 – 0.6	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.5 – 3.0	
Input Impedance	220 Ω + 820 Ω // 120 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Sweden

The following parameters apply if you have selected Sweden as location.

Table 173: Sweden Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-12.5 dBm
Busy Tone	425 Hz	0.25 – 0.25	-12.5 dBm
Ringback Tone	425 Hz	1.0 – 5.0	-12.5 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-22 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-12.5 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-12.5 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-12.5 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.25 – 0.75	-12.5 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 5.0	
Input Impedance	200 Ω + 1000 Ω // 100 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-5 dBr

Switzerland

The following parameters apply if you have selected Switzerland as location.

Table 174: Switzerland Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-8 dBm
Busy Tone	425 Hz	0.5 – 0.5	-13 dBm
Ringback Tone	425 Hz	1.0 – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.333 0.333 0.333 – 1.0	-13 dBm
Stutter Dial Tone	425 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-8 dBm
Confirmation Tone	425 Hz	(0.1 – 0.1) x 3, End	-8 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	425 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-8 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	425 Hz	0.2 – 0.2	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6.5 dBr

Thailand

The following parameters apply if you have selected Thailand as location.

Table 175: Thailand Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 * 50 Hz	CONTINUOUS	-16 dBm
Busy Tone	400 Hz	0.5 – 0.5	-10 dBm
Ringback Tone	400 Hz	1.0 – 4.0	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-15 dBm
Stutter Dial Tone	400 * 50 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-16 dBm
Confirmation Tone	400 * 50 Hz	(0.1 – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	400 * 50 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-16 dBm
Reorder Tone	400 Hz	0.3 – 0.3	-10 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	400 Hz	0.3 – 0.3	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr

United Arab Emirates

The following parameters apply if you have selected the United Arab Emirates 2 as location.

Table 176: United Arab Emirates 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	CONTINUOUS	-13 dBm
Busy Tone	400 Hz	0.375 – 0.375	-13 dBm
Ringback Tone	425 Hz	0.4 – 0.2, 0.4 – 2.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-15 dBm -15 dBm -15 dBm
Stutter Dial Tone	350+440 Hz	(0.4 – 0.04) x 5, CONTINUOUS	-13 dBm
Confirmation Tone	400 Hz	(0.1 – 0.1) x 3 End	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	(0.1 – 0.1)	-19 dBm
Message Waiting Indicator Tone	350+440 Hz	(0.1 – 0.1) x 10 CONTINUOUS	-16 dBm
Reorder Tone	400 Hz	CONTINUOUS	-13 dBm
Call Waiting Tone	425 Hz	0.2 – 12) x 3	-13 dBm
Alternative Call Waiting Tone			
Network Congestion Tone	400 Hz	0.4 – 0.35, 0.225 – 0.525	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 2.0	
Input Impedance	600 Ω		
FXS Line Attenuation (Input)			3 dBr
FXS Line Attenuation (Output)			-3 dBr

UK

The following parameters apply if you have selected the United Kingdom as location.

Table 177: UK Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	CONTINUOUS	-22 dBm
Busy Tone	400 Hz	0.375 – 0.375	-19 dBm
Ringback Tone	400+450 Hz	0.4 – 0.2, 0.4 – 2.0	-22 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-19 dBm
Stutter Dial Tone	350+440 Hz	(0.1 – 0.1) x 3, CONTINUOUS	-22 dBm
Confirmation Tone	350+440 Hz	(0.1 – 0.1) x 3, End	-22 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	0.1 – 0.1	-19 dBm
Message Waiting Indicator Tone	350+440 Hz	(0.1 – 0.1) x 10, CONTINUOUS	-22 dBm
Reorder Tone	400 Hz	0.4 – 0.35, 0.225 – 0.525	-19 dBm
Call Waiting Tone	440 Hz	0.3	-17 dBm
Alternative Call Waiting Tone	440 Hz 440 Hz 440 Hz 440 Hz	0.3 0.1 – 0.1, 0.1 0.1 – 0.1, 0.1 – 0.1, 0.1 0.1 – 0.1, 0.3 – 0.1, 0.1	-17 dBm -17 dBm -17 dBm -17 dBm
Network Congestion Tone	400 Hz	0.4 – 0.35, 0.225 – 0.525	-19 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 2.0	
Input Impedance	300 Ω + 1000 Ω // 220 nF		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-9 dBr

10 BaseT

An Ethernet local area network that works on twisted pair wiring.

100 BaseT

A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

Access Device

Device capable of sending or receiving data over a data communications channel.

A-Law

The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (μ)-law standard. See also *mu (μ)-law*.

Access Concentrator

A device that merges many data transmission signals onto a single shared channel in such a way that all the data channels can be active at the same time. The access concentrator supports dial-up modem calls, ISDN connections, frame relay traffic and multiprotocol routing.

Analog Display Services Interface (ADSI)

Telecommunications protocol standard that enables alternate voice and data capability over the existing analog telephone network. This means that in addition to the familiar voice response audio interface (where you listen to voice recordings and make menu selections using the telephone keypad), you can now see the menu and information on the screen display and make selections using soft keys. To use ADSI, you would need an ADSI capable device (as you would if you want the caller ID service).

Area Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line. In North America, an area code has three digits and is used with a NXX (office code) number. For instance, in the North American telephone number 561-955-1212, the numbers are defined as follows:

Table 178: North American Numbering Plan

No.	Description
561	Area Code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the area code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is xZABPQ 12 34, where:

Table 179: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.

Table 179: France Numbering Plan (Continued)

No.	Description
Z	Geographical (regional) zone of the number (in France, there are five zones). It has two digits.
ABPQ	First four digits corresponding to a local zone defined by central offices.
12 34	Unique number to reach a specific destination.

In this context, the area code corresponds to the Z portion of the numbering plan. Because virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an area code for the location of your communication unit.

Cable Modem

A device that connects a computer to a local cable television line and receives data at about 1.5 Mbps. This data rate far exceeds that of the prevalent 28.8 and 56 Kbps telephone modems and the up to 128 Kbps of Integrated Services Digital Network (ISDN). It is about the data rate available to subscribers of Digital Subscriber Line (DSL) telephone service. A cable modem can be added to or integrated with a set-top box that provides your TV set with channels for Internet access. In most cases, cable modems are furnished as part of the cable access service and are not purchased directly and installed by the subscriber.

Call Agent (Connection Manager)

Manages the connection state of the Mediatrix 4102. The Connection Manager provides Basic Call Processing and MGCP Gateway Support.

Country Code (CC)

In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Custom Local Area Signalling Services (CLASS)

One of an identified group of network-provided enhanced services. A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.

Digital Signal Processor (DSP)

Specialized computer chip designed to perform speedy and complex operations on digitized waveforms. Useful in processing sound (like voice phone calls) and video.

Digital Subscriber Lines (DSL)

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL.

Domain Name Server (DNS)

Internet service that translates domain names into IP addresses. To use a domain name, a DNS service must translate the name into the corresponding IP address. For instance, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF)

In telephone systems, multi-frequency signalling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “*”, the “*” being reserved for special purposes.

Dynamic Host Configuration Protocol (DHCP)

TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

Echo Cancellation

Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.

Far End Disconnect

Refers to methods for detecting that a remote party has hung up. This is also known as Hangup Supervision. There are several methods that may be used by a PBX/ACD/CO to signal that the remote party has hung up, including cleardown tone, or a wink.

Federal Communications Commission (FCC)

U.S. government regulatory body for radio, television, interstate telecommunications services, and international services originating in the United States.

Foreign Exchange Service/Station (FXS)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., "foreign", exchange, rather than the local exchange area's central office. This is the station (telephone) end of an FX circuit. An FXS port will provide dial tone and ring voltage.

G.711

ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48 kbps, 56 kbps, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.726

Nn implementation of ITU-T G.726 standard for conversion linear or A-law or μ -law PCM to and from a 40, 32, 24 or 16 kbit/s channel.

G.729

A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).

Gateway

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

International Telecommunication Union (ITU)

Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

Internet-Drafts

Internet-Drafts are working documents of the IETF, its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet Protocol (IP)

A standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

Jitter

A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

Layer 2

Layer 2 refers to the Data Link Layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Data Link Layer is concerned with moving data across the physical links in the network.

The Data-Link Layer contains two sublayers that are described in the IEEE-802 LAN standards:

- ▶ Media Access Control (MAC)
- ▶ Logical Link Control (LLC)

Layer 3

Layer 3 refers to the Network layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Network Layer is concerned with knowing the address of the neighbouring nodes in the network, selecting routes and quality of service, and recognizing and forwarding to the transport layer incoming messages for local host domains.

Light Emitting Diode (LED)

A semiconductor diode that emits light when a current is passed through it.

Local Area Network (LAN)

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also WAN.

Management Information Base (MIB)

Specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

Management Server

Includes a web-based provisioning client, provisioning server, and SNMP proxy server used to manage all agents connected to the system. The Management Server provides Gateway provisioning, Monitoring, and Numbering Plan.

Media Access Control (MAC) Address

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

Media Gateway Control Protocol (MGCP)

An application programming interface and a protocol for controlling Voice over IP (VoIP) Gateways from external call control elements, where the intelligence is.

Mu (μ)-Law

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Network

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Network-based Call Signalling (NCS)

NCS is a profile of the Media Gateway Control Protocol (MGCP). The scope of NCS is currently only embedded Voice-Over-IP client devices.

Off-hook

A line condition caused when a telephone handset is removed from its cradle.

On-hook

A line condition caused when a telephone handset is resting in its cradle.

Packet

Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection. The structure of a packet depends on the protocol.

Plain Old Telephone System (POTS)

Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

Point to Point Protocol over Ethernet (PPPoE)

A proposal specifying how a host personal computer interacts with a broadband modem (i.e., DSL, cable, wireless, etc.) to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dialup Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

Port

Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Portable Operating System Interface (POSIX)

POSIX is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturer's computer systems without having to be recoded.

POST

The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.

Private Branch Exchange (PBX)

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Programmable Read-Only Memory (PROM)

A memory chip where data is written only once as it remains there forever. Unlike RAM, PROMs retain their contents when the computer is turned off.

Protocol

A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between application programs.

Public Switched Telephone Network (PSTN)

The local telephone company network that carries voice data over analog telephone lines.

Quality of Service (QoS)

Measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).

Real Time Control Protocol (RTCP)

RTCP is the control protocol designed to work in conjunction with RTP. It is standardized in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

Realtime Transport Protocol (RTP)

An IETF standard for streaming realtime multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.

Request for Comment (RFC)

A Request for Comments (RFC) is a formal document from the IETF that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

Restart in Progress (RSIP)

The RSIP command is used by the gateway to signal that an endpoint, or a group of endpoints, is put in-service or out-of-service.

Router

A specialized switching device which allows customers to link different geographically dispersed local area networks and computer systems. This is achieved even though it encompasses different types of traffic under different protocols, creating a single, more efficient, enterprise-wide network.

Switched Circuit Network (SCN)

A communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

Server

A computer or device on a network that works in conjunction with a client to perform some operation.

Session Description Protocol (SDP)

Describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation. SDP communicates the existence of a session and conveys sufficient information to enable participation in the session. SDP is described in RFC 2327.

Simple Network Management Protocol (SNMP)

A standard of network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol / Internet Protocol (TCP/IP) suite and defined in RFC 1157.

Simple Network Time Protocol (SNTP)

SNTP, which is an adaptation of the Network Time Protocol (NTP), is widely used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronization source and network paths.

Stack

A set of network protocol layers that work together. The OSI Reference Model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the Internet.

Subnet

An efficient means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks.

T.38

An ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

Telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Trivial File Transfer Protocol (TFTP)

A simplified version of FTP that transfers files but does not provide password protection, directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP)

An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Voice Over IP (VoIP)

The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN)

A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

List of Acronyms

AC	Access Concentrator
ADSI	Analog Display Services Interface
CE	Cummunauté européenne (French)
CHAP	Challenge Handshake Authentication Protocol
CNG	Comfort Noise Generator
CS-ACELP	Conjugate Structure-Algebraic Code Excited Linear Prediction
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Lines
DTMF	Dual Tone Multi-Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
Hz	Hertz
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
Mb/s	Megabits Per Second
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MTU	Maximum Transmission Unit
NCS	Network-based Call Signalling
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PBX	Private Branch eXchange
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol Over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service

RSIP	Restart in Progress
RTCP	Real Time Control Protocol
SCN	Switched Circuit Network
SDP	Session Description Protocol
SME	Small and Medium-sized Enterprise
SMI	Structure of Management Information
STUN	Simple Traversal of User Datagram Protocol (UDP) through Network Address Transla-
tion (NAT)	
TAS	Transparent Address Sharing
TBRL	Terminal Balance Return Loss
TCP/IP	Transmission Control Protocol/Internet Protocol
TPE	Twisted-Pair Ethernet
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
UTP	Unshielded Twisted pair
VAD	Voice Activity Detection
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	eXtensible Markup Language



List of MIB Parameters

A

analogScnGwDtmfDuration	109
analogScnGwInterDigitDialDelay	109

C

checkTcpIpStackForSuccessfulBoot	24
configFileAutoUpdateOnRestartEnable	139
configFileAutoUpdatePeriod	140
configFileAutoUpdatePeriodicEnable	141
configFileAutoUpdateTimeRange	140
configFileAutoUpdateTimeUnit	140
configFileFetchingConfigSource	22
configFileFetchingDhcpSiteSpecificCode	63, 132
configFileFetchingFileLocation	133
configFileFetchingFileName	133
configFileFetchingHost	63, 132
configFileFetchingPort	63, 132
configFileFetchingSelectConfigSource	63, 132
configFileFetchingSpecificFileName	134
configFileFetchingStaticHost	63, 132
configFileFetchingStaticPort	63, 132
configFilePrivacyEnable	136
configFilePrivacyGenericSecret	136
configFilePrivacySpecificSecret	136
configFileTransferPassword	138, 139, 140
configFileTransferProtocol	137, 138, 139, 140
configFileTransferUsername	138, 139, 140

D

dataIcfClearChannelCodecPreferred	183
dataIcfCodecMediaTypeIdImageEnable	182
dataIcfCodecT38Enable	183, 185
dataIcfCodecT38ProtectionLevel	185
dataIcfT38BasePort	123
dataIcfT38NoSignalEnable	185
dataIcfT38NoSignalTimeout	185

F

fxsFlashHookDetectionDelayMax	164
fxsFlashHookDetectionDelayMin	164
fxsLoopCurrent	165
fxsMeterPauseDuration	89
fxsMeterPulseDuration	89
fxsMeterPulseFreq	89

G

groupAdminState	138, 156, 157
groupReset	23
groupSetAdmin	23, 137, 138, 156, 157

H

httpServerAccess	26
httpServerEnable	25
httpServerPort	25

I

IfAdminInitialAdminState	164
ifAdminSetAdmin	163
imageAutoUpdateEnable	158, 160
imageAutoUpdateOnRestartEnable	158
imageAutoUpdatePeriod	159
imageAutoUpdateTimeRange	159
imageAutoUpdateTimeUnit	159
imageConfigSource	22
imageDhcpPrimarySiteSpecificCode	61, 150
imageDhcpSecondarySiteSpecificCode	62, 150
imageLocation	152, 153
imageLocationProvisionSource	152
imagePrimaryHost	22, 61, 150
imagePrimaryPort	22, 61, 150
imageSecondaryHost	22, 62, 150
imageSecondaryPort	22, 62, 150
imageSelectConfigSource	61, 150
imageSelectionFileLocation	152, 153
imageStaticPrimaryHost	151
imageStaticPrimaryPort	151
imageStaticSecondaryHost	151
imageStaticSecondaryPort	151
imageTransferPassword	157, 158, 159
imageTransferProtocol	156, 157, 158, 159
imageTransferUsername	157, 158, 159
ipAddressConfigLanInterface	120
ipRoutingDhcpServerLeaseTime	122
ipRoutingEnable	122, 129
ipRoutingMacAddress	122
ipRoutingMacSpoofAddress	121
ipRoutingMacSpoofEnable	122
ipRoutingQosDiffServSubstitution	120
ipRoutingQosDiffServSubstitutionEnable	120

L

lanStaticAddress	59, 66
lanStaticNetworkMask	59, 66, 121
localHostAddress	22, 58, 118
localHostConfigSource	22
localHostDefaultRouter	22, 58
localHostDhcpServer	58
localHostDnsOverrideEnable	61
localHostFqdn	59
localHostFqdnConfigSource	59
localHostFqdnSelectConfigSource	59
localHostNetworkMask	121
localHostPrimaryDns	22, 58
localHostSecondaryDns	22, 58
localHostSelectConfigSource	15, 57, 116
LocalHostSnmpPort	60
localHostSnmpPort	22, 60
localHostStaticDefaultRouter	116

localHostStaticFqdn	59
localHostStaticPrimaryDns	16, 59
localHostStaticSecondaryDns	16, 59
localHostStaticSnmpPort	60
localHostStaticSubnetMask	16
localHostStaticWanAddress	58
localHostSubnetMask	22, 58
LocalHostWanAddress	59
localHostWanAddress	118
localHostWanAddressSelectConfigSource	58, 118

M

mgcpAddPtimeIfPresentInLCO	80
mgcpCADhcpSiteSpecificCode	64, 76
mgcpCAHost	64, 76
mgcpCAPort	64, 76
mgcpCAsSelectConfigSource	64, 76
mgcpCAsStaticHost	77
mgcpCAsStaticPort	77
mgcpDefaultDigitMap	80
mgcpDefaultPackage	84
mgcpDtmfPackageLDuration	85
mgcpDtmfPackageTCriticalDuration	85
mgcpDtmfPackageTPartialDuration	85
mgcpEndpointIdListIncludeNotStarted	80
mgcpEndpointIdTerm1	81
mgcpEndpointIdTerm2	81
mgcpFwKeepAliveEnable	92
mgcpFwKeepAliveTimeout	92
mgcpGenericMediaPackageRbkDuration	85
mgcpGenericMediaPackageRtDuration	84
mgcpLinePackageBzDuration	85
mgcpLinePackageDIDuration	86
mgcpLinePackageHdPersistent	86
mgcpLinePackageHfPersistent	87
mgcpLinePackageHuPersistent	87
mgcpLinePackageMwiDuration	86
mgcpLinePackageOsiDuration	86
mgcpLinePackageOtDuration	86
mgcpLinePackageRgDuration	86
mgcpLinePackageRoDuration	86
mgcpLinePackageSIDuration	86
mgcpLinePackageWtDuration	86
mgcpncsAnswerStreamFormat	94
mgcpncsBracketsAroundIpAddressInDomainNameEnable	98
mgcpncsConnectRtpSockets	95
mgcpncsFakeRfc3407Recognition	97
mgcpncsG729AnnexBNegotiation	178
mgcpncsImmediateModemToneReporting	96
mgcpncsMakeOsiSignalBrief	96
mgcpncsMultipleFaxToneDetection	95
mgcpncsOriginLineSessionIDAndVersionMaxLength	94
mgcpncsPolarityReversalOnCallingCardServiceToneEnable	98
mgcpncsRtpUdpChecksumEnable	95
mgcpncsT38CapabilitiesUsingAudioCodec98	96
mgcpncsUseltuT38Format	97
mgcpncsValidateOfferAnswerModel	93
mgcpPiggyBackingEnable	80
mgcpPort	80

mgcpRestartLevel	80
mgcpRetransmissionAlgorithm	82
mgcpRetransmissionDisconnectInitialWaitingPeriod	83
mgcpRetransmissionDisconnectMaxWaitingPeriod	83
mgcpRetransmissionDisconnectMinWaitingPeriod	83
mgcpRetransmissionDisconnectThreshold	83
mgcpRetransmissionDisconnectThresholdDnsQuery	83
mgcpRetransmissionDisconnectTimeout	82
mgcpRetransmissionHistoryTimeout	83
mgcpRetransmissionInitialPeriod	82
mgcpRetransmissionMaxPeriod	82
mgcpRetransmissionMaxWaitingDelay	83
mgcpRetransmissionSuspicionThreshold	82
mgcpRetransmissionSuspicionThresholdDnsQuery	83
mgcpXPPackageIrfDuration	88
msConfigSource	22
msDhcpSiteSpecificCode	62, 194
msEnable	193
msHost	22, 62, 193
msSelectConfigSource	62, 193
msStaticHost	62, 194
msStaticPort	62
msStaticTrapPort	62, 194
msTrapConfigInformation	144
msTrapPort	22, 62, 193
msTrapRetransmissionPeriod	193
msTrapRetransmissionRetryCount	193
mxDebugPcmCaptureEnable	214
mxDebugPcmCaptureEndpointNumber	214
mxDebugPcmCaptureIrfAddress	214

N

ncsCADhcpSiteSpecificCode	64, 100
ncsCAHost	64
ncsCaHost	100
ncsCAPort	64, 100
ncsCASelectConfigSource	64, 100
ncsCAStaticHost	101
ncsCAStaticPort	101
ncsCompatibilityRtpPayloadType18EncodingName	106
ncsCompatibilityVersion	107
ncsDefaultDigitMap	101
ncsEndpointIdListIncludeNotStarted	102
ncsEndpointIdTerm1	102
ncsEndpointIdTerm2	102
ncsLinePackageBzDuration	105
ncsLinePackageDIDuration	105
ncsLinePackageLDuration	105
ncsLinePackageMwiDuration	105
ncsLinePackageOtDuration	105
ncsLinePackageRbkDuration	105
ncsLinePackageRgDuration	105
ncsLinePackageRoDuration	105
ncsLinePackageRtDuration	105
ncsLinePackageSIDuration	106
ncsLinePackageTCriticalDuration	106
ncsLinePackageTPartialDuration	106
ncsPiggyBackingEnable	102
ncsPort	101

ncsRestartLevel	101
ncsRetransmissionAlgorithm	103
ncsRetransmissionDisconnectInitialWaitingPeriod	104
ncsRetransmissionDisconnectMaxWaitingPeriod	104
ncsRetransmissionDisconnectMinWaitingPeriod	104
ncsRetransmissionDisconnectThreshold	104
ncsRetransmissionDisconnectThresholdDnsQuery	104
ncsRetransmissionDisconnectTimeout	103
ncsRetransmissionHistoryTimeout	104
ncsRetransmissionInitialPeriod	103
ncsRetransmissionMaxPeriod	103
ncsRetransmissionMaxWaitingDelay	104
ncsRetransmissionSuspicionThreshold	103
ncsRetransmissionSuspicionThresholdDnsQuery	104

P

pppoeAcName	116
pppoeEnable	117
pppoeServiceName	117
pppSecuritySecretsIdentity	117
pppSecuritySecretsSecret	117

Q

qosSignalingDiffServ	195
qosSignalingIeee8021qEnable	196
qosSignalingIeee8021qUserPriority	196
qosT38FaxDiffServ	196
qosT38FaxIeee8021qEnable	129, 196
qosT38FaxIeee8021qUserPriority	129, 196
qosVlanIeee8021qDefaultUserPriority	197
qosVlanIeee8021qSubstitutionEnable	198, 199
qosVlanIeee8021qSubstitutionFiltering	199
qosVlanIeee8021qSubstitutionUserPriority	198
qosVlanIeee8021qSubstitutionVlanID	198
qosVlanIeee8021qTaggingEnable	197
qosVlanIeee8021qVirtualLanID	197
qosVoiceDiffServ	196
qosVoiceIeee8021qEnable	129, 196
qosVoiceIeee8021qUserPriority	129, 196

R

rtpConfigBasePort	124
-------------------------	-----

S

snmpAgentAccess	52
sntpConfigSource	22
sntpEnable	189
sntpHost	65, 190
sntpPort	65, 190
sntpSelectConfigSource	65, 190
sntpStaticHost	190
sntpStaticPort	190
sntpSynchronizationPeriod	189
sntpSynchronizationPeriodOnError	189
sntpTimeZoneString	140, 159, 191
stunEnable	188
stunKeepAliveInterval	188

stunQueryCacheDuration	188
stunQueryTimeout	188
stunStaticHost	188
stunStaticPort	188
sysAdminCommand	57, 156, 157
sysAdminDefaultSettingsEnable	23
sysAdminDownloadConfigFileStatus	134, 144
sysConfigCommand	137, 138
sysConfigComputerEthernetSpeed	73
sysConfigDownloadConfigFile	139, 141, 144
sysConfigDownloadConfigMode	144
sysConfigMaxDynamicPort	123
sysConfigMinDynamicPort	123
sysConfigNetworkEthernetSpeed	73
sysConfigStatsNumberPeriods	206
sysConfigStatsPeriodLength	206
syslogConfigSource	22
syslogDhcpSiteSpecificCode	63, 202
syslogHost	22, 63, 202
syslogMsgDisplayLocalHost	203
syslogMsgDisplayMacAddress	203
syslogMsgDisplayTime	203
syslogMsgDisplayTimeFormat	203
syslogMsgLocalMaxNbr	204
syslogMsgLocalMaxSeverity	204
syslogMsgMaxSeverity	201
syslogPort	22, 63, 202
syslogSelectConfigSource	63, 202
syslogStaticHost	202
syslogStaticPort	202
sysMacAddress	9, 66
sysMibVersion	52

T

telephonyCountrySelection	111
telephonyDnsOverrideEnable	61
telephonyIpSignalingProtocolSelection	53, 75, 99

V

voicelfAdaptativeJitterBufferEnable	213
voicelfCodecG72616kbpsEnable	169
voicelfCodecG72616kbpsMaxPTime	171
voicelfCodecG72616kbpsMinPTime	171
voicelfCodecG72616kbpsPayloadType	169
voicelfCodecG72624kbpsEnable	169
voicelfCodecG72624kbpsMaxPTime	171
voicelfCodecG72624kbpsMinPTime	171
voicelfCodecG72624kbpsPayloadType	169
voicelfCodecG72632kbpsEnable	169
voicelfCodecG72632kbpsMaxPTime	171
voicelfCodecG72632kbpsMinPTime	171
voicelfCodecG72632kbpsPayloadType	170
voicelfCodecG72640kbpsEnable	169
voicelfCodecG72640kbpsMaxPTime	171
voicelfCodecG72640kbpsMinPTime	171
voicelfCodecG72640kbpsPayloadType	170
voicelfCodecG729Enable	169
voicelfCodecG729MaxPTime	172
voicelfCodecG729MinPTime	172

voicelfCodecPcmaEnable	169
voicelfCodecPcmaMaxPTime	170
voicelfCodecPcmaMinPTime	170
voicelfCodecPcmuEnable	169
voicelfCodecPcmuMaxPTime	170
voicelfCodecPcmuMinPTime	170
voicelfCodecPreferred	169
voicelfDtmfDetectionRiseTimeCriteria	175
voicelfDtmfDetectionUnitBreakPowerThreshold	175
voicelfDtmfDetectionUnitMaxPowerThreshold	174
voicelfDtmfDetectionUnitMinPowerThreshold	174
voicelfDtmfDetectionUnitNegativeTwist	175
voicelfDtmfDetectionUnitPositiveTwist	175
voicelfDtmfPayloadType	173
voicelfDtmfTransport	170, 172, 173
voicelfG711ComfortNoiseGenerationEnable	179
voicelfG711VoiceActivityDetectionEnable	177
voicelfG729VoiceActivityDetectionEnable	177
voicelfMaxJitterBufferLength	176, 213
voicelfTargetJitterBufferLength	176, 213
voicelfUserInputGainOffset	179
voicelfUserOutputGainOffset	179

Index

Numerics

- 10 BaseT [6](#), [9](#), [10](#), [12](#), [13](#), [73](#)
 - defined [267](#)
 - see also *cabling*
- 100 BaseT [6](#), [9](#), [10](#), [12](#), [13](#), [73](#)
 - defined [267](#)
 - see also *cabling*
- 802.1q, in QoS [196](#)

A

- access concentrator, defined [267](#)
- acronyms [275](#)
- ADSI
 - caller ID [110](#)
 - defined [267](#)
- A-Law [167](#)
 - defined [267](#)
- analog modem, feature [167](#)
- area code, defined [267](#)
- audience, intended [xiii](#)
- auto MDI/MDIX [9](#)
- automatic
 - configuration update [139](#)
 - software update [158](#)

B

- brackets around domain name, in MGCP/NCS [98](#)
- brief OSI signal, in MGCP/NCS [96](#)
- broadcast storm, behaviour when restarting [24](#)

C

- cabling
 - RJ-11 [237](#)
 - RJ-45
 - crossover [236](#)
 - pin name [236](#)
 - pinout information [235](#)
 - straight through [235](#)
 - see also *10 BaseT*
 - see also *100 BaseT*
- call, placing [4](#)
- call agent
 - defined [268](#)
 - setting [76](#), [100](#)
- caller ID
 - ADSI [110](#)
 - country-specific, selecting [111](#)
 - DTMF signalling [109](#)
 - ETSI 300 659-1 January 2001 (Annex B) [109](#)
 - STD 220-250-713 Issue 01. November 1993 [109](#)
 - TDK-TS 900 301-1 January 2003 [109](#)
 - FSK generation [110](#)
 - Bellcore GR-30-CORE [110](#)
 - British Telecom (BT) SIN227, SIN242 [110](#)
 - ETSI 300 659-1 [110](#)
 - UK CCA specification TW/P&E/312 [110](#)
 - generation [109](#)
- clear channel fax
 - enabling [182](#)
 - preferred codec [183](#)

- clear channel fax (continued)
 - setting [181](#)
- codec
 - data
 - clear channel fax [181](#)
 - enabling [182](#)
 - preferred [183](#)
 - enabling [181](#)
 - T.38 [183](#), [185](#)
 - voice
 - defined [167](#)
 - DTMF detection [173](#)
 - DTMF transport type [172](#), [173](#)
 - enabling [169](#)
 - packetization time [170](#)
 - preferred [169](#)
- comfort noise [178](#)
- compliance to standards. see *standards compliance*
- conference mode, feature [89](#)
- configuration
 - file [52](#)
 - using a GUI [49](#)
 - web interface
 - configuration file upload [33](#)
 - enabling [25](#)
 - LAN [31](#)
 - LAN interface [31](#)
 - MAC address spoofing [31](#)
 - password
 - modify [34](#)
 - reset [34](#)
 - PPP password [30](#)
 - PPP user name [30](#)
 - static information [30](#)
 - STUN [32](#)
 - system log [36](#)
 - user name, modify [34](#)
 - WAN [29](#)
 - WAN connection type [30](#)
 - web interface. see *web interface*
- configuration file
 - automatic update [139](#)
 - download server [131](#)
 - configuration source [131](#)
 - DHCP information, using [132](#)
 - HTTP server, configuring [131](#)
 - IP address [131](#)
 - SNTP server, configuring [131](#)
 - static information, using [132](#)
 - TFTP server, configuring [131](#)
 - download, setting [133](#)
- encryption
 - decrypting generic [136](#)
 - decrypting specific [136](#)
 - defined [136](#)
- example [147](#)
- HTTP, downloading via [138](#)
- management server, downloading from [144](#)
- syslog messages [135](#)
- TFTP, downloading via [137](#)
- uploading via web interface [33](#)

configuration sources, setting all to static [57](#)

- configuring the software
 - configuration file [52](#)
 - DHCP (dynamic), using [56](#)
 - MIB. *see* [SNMP](#)
 - static
 - setting configuration sources to [57](#)
 - using [57](#)
- connecting the unit [9](#)
- connectors
 - LAN [6](#)
 - Phone-Fax 1 [6](#)
 - Phone-Fax 2 [6](#)
 - Reset/Default [6](#)
 - universal power supply unit [6](#)
 - WAN [6](#)
- country-specific parameters [239](#)
 - caller ID, selecting [111](#)
 - setting [110](#)
- crossover cable. *see* [cabling](#)
- customer services [xviii](#)

D

- default router, setting [30](#), [58](#)
- Default Settings
 - factory reset procedure [22](#)
 - disabling [23](#)
 - in recovery mode [21](#)
- DHCP information
 - configuration file download server [132](#)
 - Image [150](#)
 - management server [193](#)
 - MGCP call agent [76](#)
 - NCS call agent [100](#)
 - SNTP [190](#)
 - syslog daemon [202](#)
 - see also* [static information](#)
- DHCP server
 - configuring [66](#)
 - defined [269](#)
 - FQDN, entering [70](#)
 - IP address of, setting [58](#)
 - IP addresses, entering [69](#)
 - network configuration [67](#)
 - requirement [3](#)
 - site specific option [68](#)
 - vendor class ID [67](#)
 - vendor specific option [67](#)
- Differentiated Services (DS) Field, in QoS [195](#)
 - substituting configured value [120](#)
- disabling lines [163](#)
- DNS
 - defined [268](#)
 - primary [30](#), [58](#)
 - static [60](#)
 - requirement [3](#)
 - secondary [30](#), [58](#)
 - static [60](#)
- documentation
 - Media5 download portal [xvii](#)
 - Mediatrix download portal [xvii](#)
- domain name, brackets around [98](#)
- downgrading software, procedure [160](#)
- downloading software
 - automatic update [158](#)
 - configuration source [150](#)

- downloading software (continued)
 - emergency download [160](#)
 - HTTP server, configuring [149](#)
 - HTTP, via [157](#)
 - Image path [152](#)
 - LED states [155](#)
 - SNTP server, configuring [149](#)
 - TFTP server, configuring [149](#)
 - TFTP, via [156](#)
 - troubleshooting [216](#)
 - zip file [152](#)
- DTMF
 - defined [268](#)
 - detection [173](#)
 - out-of-band [172](#)
 - signalling, caller ID [109](#)
 - transport type [172](#)
 - payload type [173](#)

E

- echo cancellation [178](#)
- emergency software download [160](#)
- enabling lines [163](#)
- encryption, of configuration files
 - decrypt generic [136](#)
 - decrypt specific [136](#)
 - defined [136](#)
- end user technical support [xviii](#)
- endpoint. *See* [lines](#)
- Ethernet connection, setting speed of [73](#)

F

- factory reset
 - disabling [23](#)
 - reverting to [22](#)
 - see also* [recovery mode](#)
- fake RFC 3407 recognition, in MGCP/NCS [97](#)
- far end disconnect, signalling [165](#)
- fax
 - clear channel [181](#)
 - multiple tone detection [95](#)
 - T.38 [183](#)
 - no-signal [185](#)
 - user gain vs communication quality [179](#)
- features, conference mode [89](#)
- firewall, traversal [92](#)
- flash hook, setting [164](#)
- Foreign Exchange Service/Station (FXS)
 - defined [269](#)
 - see also* [lines](#)
- FQDN, entering [70](#)
- FSK generation, caller ID [110](#)

G

- g a cable modem [116](#)
- G.711 [167](#)
 - comfort noise [178](#)
 - defined [269](#)
 - voice activity detection [176](#)
- G.726 [168](#)
 - comfort noise [178](#)
 - defined [269](#)
 - payload type [169](#)

- G.726 168 (continued)
 - voice activity detection [176](#)
- G.729 [168](#)
 - Annex B negotiation [177](#)
 - defined [269](#)
 - voice activity detection [177](#)
- GUI, using a [49](#)

H

- hardware
 - cleaning [8](#)
 - condensation [8](#)
 - front indicators [5](#)
 - proper location [7](#)
 - rear connections [6](#)
- HTTP
 - configuration file download [138](#)
 - server
 - configuring [131](#), [149](#)
 - requirement [3](#)
 - software download via [157](#)
- humidity level [7](#)

I

- IEEE 802.1q, in QoS [196](#)
- IGMP, in router service [115](#)
- Image server
 - DHCP information, using [150](#)
 - static information, using [151](#)
- immediate modem tone reporting, in MGCP/NCS [96](#)
- indicators of the hardware [5](#)
- installation
 - before proceeding [9](#)
 - connecting the hardware [9](#)
 - free standing unit [8](#)
 - package contents [3](#)
 - provisioning sequence in DHCP [15](#)
 - provisioning sequence in PPPoE or PPPoA [15](#)
 - requirements [3](#)
 - reserving IP address [9](#)
 - router, with a [12](#)
 - safety recommendations [3](#)
 - selecting site for [7](#)
 - setting up the unit for the first time [13](#)
 - single computer, with a [10](#)
 - verifying [24](#)
 - wall-mounting [8](#)
- intended audience [xiii](#)
- IP address
 - default router [30](#), [58](#)
 - defining
 - decimal [55](#)
 - hexadecimal [55](#)
 - octal [55](#)
 - DHCP server [58](#)
 - DHCP, using [56](#)
 - DNS, primary [30](#), [58](#)
 - static [60](#)
 - DNS, secondary [30](#), [58](#)
 - static [60](#)
 - download server [131](#)
 - entering [69](#)
 - Image server [150](#)
 - LAN connector, static [65](#)

- IP address (continued)
 - locating [55](#)
 - Management Server [193](#)
 - MGCP call agent [76](#)
 - NCS call agent [100](#)
 - of unit [30](#), [58](#)
 - SNTP server [190](#)
 - static
 - setting configuration sources to [57](#)
 - using [57](#)
 - subnet mask [30](#), [58](#)
 - syslog daemon [202](#)
 - WAN [118](#)

J

- jitter
 - buffer protection [175](#)
 - defined [270](#)

L

- LAN
 - cable [24](#)
 - configuration via web interface [31](#)
 - defined [270](#)
 - interface, configuring in transparent address sharing [120](#)
 - via web interface [31](#)
- LEDs
 - behaviour
 - in download mode [155](#)
 - in starting mode [16](#)
 - defined [270](#)
 - ETH [17](#)
 - In Use [17](#)
 - patterns
 - AdminMode [17](#), [19](#)
 - Booting [17](#), [18](#)
 - DefaultSettings ending [18](#)
 - DiagFailed [18](#)
 - ImageDownloadError [18](#)
 - ImageDownloadInProgress [18](#)
 - InitFailed [18](#)
 - NormalMode [17](#), [19](#)
 - RebootPending [17](#)
 - RecoveryMode [17](#), [20](#)
 - RecoveryModePending [17](#)
 - ResetPending [17](#)
 - Power [17](#)
 - Ready [16](#)
 - states [16](#)
- lines
 - comfort noise [178](#)
 - data codecs [181](#)
 - clear channel fax [181](#)
 - clear channel, enabling [182](#)
 - clear channel, preferred [183](#)
 - enabling [181](#)
 - T.38 [183](#), [185](#)
 - echo cancellation [178](#)
 - far end disconnect, signalling [165](#)
 - jitter buffer protection [175](#)
 - locking/unlocking [163](#)
 - multiple connections on [164](#)
 - user gain [179](#)
 - voice activity detection [176](#)

- lines (continued)
 - voice codecs
 - defined [167](#)
 - DTMF detection [173](#)
 - DTMF transport type [172](#), [173](#)
 - enabling [169](#)
 - packetization time [170](#)
 - preferred codec [169](#)
- local
 - host, in customized syslog messages [203](#)
 - IP address, setting [30](#), [58](#)
 - time, in customized syslog messages [203](#)
- location
 - caller ID, selecting [111](#)
 - country, setting [110](#)
- locking lines [163](#)
- loop current, setting [165](#)

M

- MAC address [9](#)
 - defined [270](#)
 - in customized syslog messages [203](#)
 - spoofing [121](#)
 - via web interface [31](#)
- Management Server
 - defined [270](#)
 - DHCP information, using [193](#)
 - in configuration file download [144](#)
 - static information, using [194](#)
 - using [193](#)
- MDI/MDIX, auto [9](#)
- Media5 download portal [xvii](#)
- Mediatrix download portal [xvii](#)
- meter pulse, setting [89](#)
- MGCP, setting
 - brackets around domain name [98](#)
 - brief OSI signal [96](#)
 - call agent [76](#)
 - DHCP information, using [76](#)
 - static information, using [77](#)
 - configuration [75](#)
 - connect RTP sockets [95](#)
 - endpoints [81](#)
 - fake RFC 3407 recognition [97](#)
 - firewall traversal [92](#)
 - immediate modem tone reporting [96](#)
 - meter pulse [89](#)
 - multiple fax tone detection [95](#)
 - Offer/Answer model [93](#)
 - offered stream format [94](#)
 - packages
 - DTMF [85](#)
 - Generic Media [84](#)
 - Line [85](#)
 - XL [87](#)
 - X-P [88](#)
 - polarity reversal on calling card service tone [98](#)
 - retransmission [82](#)
 - services [75](#)
 - session ID/version [94](#)
 - switching to [75](#)
 - T.38 capabilities using audio codec [98](#) [96](#)
 - T.38 negotiation syntax [97](#)
 - UDP checksum [95](#)

- MIB
 - defined [39](#)
 - in SNMP protocol [39](#)
 - see also *parameters*
- MIB structure
 - changing a parameter value [49](#)
 - conformance [48](#)
 - description
 - mediatrixAdmin [47](#)
 - mediatrixConfig [47](#)
 - mediatrixExperimental [47](#)
 - mediatrixIplTelephonySignaling [47](#)
 - mediatrixMgmt [47](#)
 - mediatrixModules [47](#)
 - mediatrixProducts [47](#)
 - events [48](#)
 - introduction [39](#)
 - objects [48](#)
 - OID, defined [39](#)
 - persistent parameters [49](#)
 - SMI, defined [39](#)
 - SNMP messages. see *SNMP*
 - tables
 - defined [50](#)
 - generic [50](#)
 - groupAdmin [51](#)
 - ifAdmin [51](#)
 - textual conventions [48](#)
 - volatile parameters [49](#)
- mounting, on a wall [8](#)
- MTU, requirements [209](#)
- Mu (μ)-Law [167](#)
 - defined [270](#)
- multicast, in router service [115](#)

N

- NAT
 - in configuration file download [137](#)
 - see also *STUN*
- NCS, setting
 - brackets around domain name [98](#)
 - brief OSI signal [96](#)
 - call agents [100](#)
 - DHCP information, using [100](#)
 - static information, using [101](#)
 - compatibility version [107](#)
 - configuration [99](#)
 - connect RTP sockets [95](#)
 - endpoints [102](#)
 - fake RFC 3407 recognition [97](#)
 - immediate modem tone reporting [96](#)
 - Line package [105](#)
 - multiple fax tone detection [95](#)
 - Offer/Answer model [93](#)
 - offered stream format [94](#)
 - polarity reversal on calling card service tone [98](#)
 - retransmission [103](#)
 - RTP Payload Type 18 [106](#)
 - services [99](#)
 - session ID/version [94](#)
 - switching to [99](#)
 - T.38 capabilities using audio codec [98](#) [96](#)
 - T.38 negotiation syntax [97](#)
 - UDP checksum [95](#)
- no-signal, in T.38 [185](#)

O

Offer/Answer model [93](#)
 OID, defined [39](#)
 operating temperature [7](#)
 out-of-band DTMF [172](#)
 overview of the product [4](#)

P

package contents [3](#)
 packetization time, setting for voice codecs [170](#)
 parameters
 changing value of [49](#)
 using a GUI [49](#)
 PCM traces, enabling [214](#)
 persistent parameters, defined [49](#)
 placing a call [4](#)
 polarity reversal on calling card service tone, in MGCP/NCS [98](#)
 port number
 configuration file fetching [63](#)
 configuration file server [131](#)
 DHCP setting [69](#)
 image server [61](#), [150](#)
 management server [62](#), [193](#)
 MGCP [80](#)
 MGCP call agent [64](#), [76](#)
 NCS [101](#)
 NCS call agent [64](#), [100](#)
 RTCP, setting range of [124](#)
 RTP, setting range of [124](#)
 SNMP agent [60](#)
 SNMP trap [60](#)
 syslog [63](#), [202](#)
 T.38, setting range of [123](#)
 TCP, setting range of [123](#)
 UDP, setting range of [123](#)
 PPPoA service
 password, setting [30](#)
 user name, setting [30](#)
 PPPoE service
 connection
 authentication phase [126](#)
 discovery phase [126](#)
 network-layer protocol phase [126](#)
 defined [116](#)
 enabling [116](#)
 error handling [127](#)
 identity [117](#)
 password, setting [30](#), [117](#)
 RFCs supported [116](#)
 secret [117](#)
 setting [116](#)
 user name, setting [30](#), [117](#)
 primary DNS, setting [30](#)
 product overview [4](#)
 protocol, switching [53](#)
 provisioning
 configuration file [52](#)
 MIB files [52](#)

Q

QoS
 802.1q [196](#)
 defined [272](#)

QoS (continued)

 Differentiated Services (DS) Field [195](#)
 substituting configured value [120](#)
 VLAN [197](#)
 substitution values [198](#)

R

rear connections [6](#)
 recovery mode
 LED patterns [20](#)
 resetting in [21](#)
 see also *factory reset*
 related documentation [xiii](#)
 requirements [3](#)
 restart
 behaviour in case of broadcast storm [24](#)
 software-initiated [23](#)
 unit [28](#)

RFC

RFC 1027 [113](#)
 RFC 1332 [116](#)
 RFC 1334 [116](#), [229](#)
 RFC 1350 [229](#)
 RFC 1362 [229](#)
 RFC 1471 [116](#), [229](#)
 RFC 1472 [116](#), [229](#)
 RFC 1473 [116](#), [229](#)
 RFC 1661 [116](#), [229](#)
 RFC 1769 [189](#)
 RFC 1877 [116](#), [229](#)
 RFC 1889 [229](#)
 RFC 1890 [173](#), [229](#)
 RFC 1945 [229](#)
 RFC 1994 [116](#), [229](#)
 RFC 2131 [66](#), [125](#), [229](#)
 RFC 2132 [66](#), [67](#), [68](#), [125](#), [229](#)
 RFC 2347 [229](#)
 RFC 2348 [229](#)
 RFC 2349 [229](#)
 RFC 2475 [195](#)
 RFC 2516 [116](#), [229](#)
 RFC 2616 [25](#), [229](#)
 RFC 2617 [34](#), [229](#)
 RFC 2833 [172](#), [229](#)
 RFC 3164 [201](#), [229](#)
 RFC 3264 [93](#)
 RFC 3389 [178](#), [229](#)
 RFC 3435 [75](#), [229](#)
 RFC 3489 [32](#), [187](#), [230](#)

RJ-11. see *cabling*

RJ-45. see *cabling*

router, installing with a [12](#)

router service

 IGMP [115](#)
 multicast [115](#)

RTCP [195](#)

 base port range [124](#)

RTP

 base port range [124](#)
 Payload Type 18 [106](#)

S

safety
 recommendations [3](#), [228](#)

safety (continued)

warnings

- Circuit Breaker (20A) [227](#)
- ETH, FXS1 and FXS2 Connectors [227](#)
- LAN Connector [228](#)
- No. 26 AWG [227](#)
- Product Disposal [227](#)
- Socket Outlet [228](#)
- TN Power [227](#)

secondary DNS, setting [30](#)signaling protocol, MGCP. see *MGCP, setting*site specific information, DHCP setting [68](#)site, selecting for unit [7](#)SMI, defined [39](#)

SNMP

- access limitation [52](#)
- behaviour [41](#)
 - non-secure management mode [42](#)
 - secure management mode [42](#)
- configuring [60](#)
- messages [40](#)
- MIB [39](#)
- SNMP configuration file [43](#)
- versions [40](#)

SNTP

- defined [272](#)
- DHCP information, using [190](#)
- enabling [189](#)
- server, configuring [131](#), [149](#)
- static information, using [190](#)
- time zone, defining custom [191](#)

software

- downgrading, procedure [160](#)
- downloading
 - automatic update [158](#)
 - configuration source [150](#)
 - emergency procedure [160](#)
 - HTTP server, configuring [149](#)
 - HTTP, via [157](#)
 - Image path [152](#)
 - LED states [155](#)
 - SNTP server, configuring [149](#)
 - syslog messages [154](#)
 - TFTP server, configuring [149](#)
 - TFTP, via [156](#)
 - troubleshooting [216](#)
 - zip file [152](#)
 - see also *downgrading*

standards compliance

- agency approvals [223](#)
- CE marking [224](#)
- emissions [223](#)
- FCC Part 15 disclaimer [224](#)
- immunity [223](#)
- RoHS China [225](#)
- safety standards [223](#)

standards supported *xvi*

caller ID

- Bellcore GR-30-CORE [110](#)
- British Telecom (BT) SIN227, SIN242 [110](#)
- ETSI 300 659-1 [110](#)
- ETSI 300 659-1 January 2001 (Annex B) [109](#)
- STD 220-250-713 Issue 01. November 1993 [109](#)
- TDK-TS 900 301-1 January 2003 [109](#)
- UK CCA specification TW/P&E/312 [110](#)
- ITU-T Q.24 [172](#)

standards supported *xvi* (continued)

- PKT-SP-EC-MGCP-I01-990312 [229](#)
- Recommendation ITU T.38 version 0 [183](#)
- Recommendation ITU-T T.38, section D.2.3 [97](#)
- RFC 1027 [113](#)
- RFC 1332 [116](#)
- RFC 1334 [116](#), [229](#)
- RFC 1350 [229](#)
- RFC 1362 [229](#)
- RFC 1471 [116](#), [229](#)
- RFC 1472 [116](#), [229](#)
- RFC 1473 [116](#), [229](#)
- RFC 1661 [116](#), [229](#)
- RFC 1769 [189](#)
- RFC 1877 [116](#), [229](#)
- RFC 1889 [229](#)
- RFC 1890 [173](#), [229](#)
- RFC 1945 [229](#)
- RFC 1994 [116](#), [229](#)
- RFC 2131 [66](#), [125](#), [229](#)
- RFC 2132 [66](#), [67](#), [68](#), [125](#), [229](#)
- RFC 2347 [229](#)
- RFC 2348 [229](#)
- RFC 2349 [229](#)
- RFC 2475 [195](#)
- RFC 2516 [116](#), [229](#)
- RFC 2616 [25](#), [229](#)
- RFC 2617 [34](#), [229](#)
- RFC 2833 [172](#), [229](#)
- RFC 3164 [201](#), [229](#)
- RFC 3264 [93](#)
- RFC 3389 [178](#), [229](#)
- RFC 3435 [75](#), [229](#)
- RFC 3489 [32](#), [187](#), [230](#)

static

- LAN connector IP address [65](#)
- setting DNS address as [60](#)

static information

- configuration file download server [132](#)
- Image [151](#)
- management server [194](#)
- MGCP call agent [77](#)
- NCS call agent [101](#)
- setting all configuration sources to [57](#)
- SNTP [190](#)
- syslog daemon [202](#)
- see also *DHCP information*

statistics

- MGCP [205](#)
- NCS [205](#)
- resetting [206](#)
- RTP [205](#)
- setting how to collect [206](#)
- viewing [205](#)

straight through cable. see *cabling*

STUN

- configuration via web interface [32](#)
- configuring [188](#)
- defined [187](#)

subnet mask, setting [30](#), [58](#)support services *xviii*switching protocol [53](#)

syslog

- daemon
 - configuring the application [203](#)
 - customizing messages

- local host [203](#)
- local time [203](#)
- MAC address [203](#)
- defined [201](#)
- DHCP information, using [202](#)
- enabling [201](#)
- messages examples [201](#)
- requirement [3](#)
- static information, using [202](#)
- local [204](#)
- messages examples [204](#)
- messages
 - configuration file [135](#)
 - examples [201](#), [204](#)
 - software download [154](#)

T

- T.38
 - base port range [123](#)
 - defined [273](#)
 - enabling [185](#)
 - negotiation syntax in MGCP/NCS [97](#)
 - not supported by other endpoint [215](#)
 - number of redundancy packets [185](#)
 - protection level [185](#)
- T.38 capabilities using audio codec 98, in MGCP/NCS [96](#)
- tables
 - defined [50](#)
 - generic [50](#)
 - groupAdmin [51](#)
 - ifAdmin [51](#)
- TCP, port range [123](#)
- technical support for end user [xviii](#)
- temperature, operating [7](#)
- textual conventions, in MIB structure [48](#)
- TFTP
 - configuration file download [137](#)
 - server
 - configuring [131](#), [149](#)
 - defined [273](#)
 - requirement [3](#)
 - software download via [156](#)
- time zone, defining custom [191](#)
- TPE. see *cabling*
- translated warning definition [226](#)
- transparent address sharing
 - defined [113](#)
 - enabling [119](#)
 - LAN interface [120](#)
 - PPPoE service
 - connection [126](#)
 - enabling [116](#)
 - error handling [127](#)
 - password, setting [117](#)
 - RFCs supported [116](#)
 - setting [116](#)
 - user name, setting [117](#)
 - QoS substitution value [120](#)
 - routing mechanism [128](#)
 - RTCP base port range [124](#)
 - RTP base port range [124](#)
 - T.38 base port range [123](#)
 - TCP port range [123](#)
 - UDP port range [123](#)
 - WAN IP address [118](#)
- troubleshooting
 - call
 - cannot establish to endpoint [215](#)
 - cannot make [214](#)
 - cannot disable adaptive jitter buffer [213](#)
 - cannot register to IGMP services [212](#)
 - DHCP unreachable [212](#)
 - fax
 - poor line condition during transmission [215](#)
 - unable to send in clear channel [215](#)
 - unable to send in T.38 [215](#)
 - voice does not switch back to codec after clear channel fax [216](#)
 - LAN web page, unable to access [213](#)
 - LEDs, all off [211](#)
 - long delay when starting unit [211](#)
 - PC has limited web access in time [212](#)
 - PCM traces, enabling [214](#)
 - SNMP
 - cannot set a variable [218](#)
 - MIB variable empty after downgrade [218](#)
 - network manager cannot access unit [217](#)
 - no response when trying to access unit [217](#)
 - SNMPv3 variables contents [219](#)
 - traps not received by network manager [218](#)
 - when viewing table, unit does not respond [218](#)
 - wrong value error message [218](#)
 - software download
 - cannot communicate with image server [216](#)
 - long time to perform [217](#)
 - path not recognized [217](#)
 - transfer problems [216](#)
 - unable to reach unit after changing Ethernet speed [212](#)
 - value not accepted [213](#)
 - WINS server not forwarded to the PC [212](#)

U

- UDP
 - checksum [95](#)
 - port range [123](#)
- unit, restarting [28](#)
- Unit Manager Network product
 - as management server [3](#), [60](#), [62](#), [193](#)
 - defined [xvii](#)
 - using [49](#), [55](#), [57](#), [149](#)
- unlocking lines [163](#)
- using this manual [xvi](#)
- UTP. see *cabling*

V

- vendor specific information, DHCP setting [67](#)
- verifying the installation [24](#)
- viewing statistics and performances [205](#)
- VLAN, in QoS [197](#)
 - substitution values [198](#)
- voice activity detection [176](#)
- volatile parameters, defined [49](#)

W

- wall-mounting the unit [8](#)
- WAN
 - configuration via web interface [29](#)
 - IP address, in transparent address sharing [118](#)

web interface

- access limitation [25](#)
- choosing suitable web browser [25](#)
- configuration file upload [33](#)
- enabling [25](#)
- LAN [31](#)
 - LAN interface [31](#)
 - MAC address spoofing [31](#)
- password
 - modify [34](#)
 - reset [34](#)
- status, system [27](#)
- STUN [32](#)
- system log [36](#)
- user name, modify [34](#)
- WAN [29](#)
 - connection type [30](#)
 - default router [30](#)
 - local IP address [30](#)
 - PPP password [30](#)
 - PPP user name [30](#)
 - primary DNS [30](#)
 - secondary DNS [30](#)
 - static information [30](#)
 - subnet mask [30](#)