media5 corporation

Discover the Power of 5

Reference Manual

Mediatrix® 4100 Series

Mediatrix 4108 / 4116 / 4124 (FXS)

MGCP/NCS Version

Product Version 5.0

Document Revision 08

November 30, 2011

RoHS COMPLIANT 2002/95/EC

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

Mediatrix® 4100 Series Reference Manual

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® 4100 Series 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 xiv
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

Chapter 1

Installation 3

Requirements 3
Safety Recommendations 3
Package Contents 3
Overview 4
About the Mediatrix 4100 4
Placing a Call 4
Panels 6
Front Indicators 6
Rear Connectors 8
Choosing a Suitable Installation Site 8
Location 8
Rack-Mounting 9
Condensation 9
Cleaning 9
Hardware Connection 9
Reserving an IP Address 9
Connecting Cables – Mediatrix 4108/4116 Models 10
Connecting Cables – Mediatrix 4124 Model 11
Starting the Mediatrix 4100 for the First Time 12
IP Address Discovery or Configuration 12
Initial Provisioning Sequence 13
LED Behaviour in Starting Mode 13

LED Indicators 14
Ready LED 14
In Use LED 14
LAN LED 14
Power LED 14
LED Patterns 14
Booting LED Pattern Description 16
NormalMode LED Pattern Description 16
AdminMode LED Pattern Description 16
Recovery Mode LED Patterns 17
Reset / Default Switch 18
At Run-Time 18
At Start-Time 18
Recovery Mode 18
Factory Reset 20
Software Restart 21
Restart Behaviour 21
Verifying the Installation 21

SNMP Configuration

Chapter 2

MIB Structure and SNMP 25

SNMP Overview 25
Definitions 25
SNMP Versions 26
SNMP Behaviour 27
SNMPv3 Special Behaviour 28
SNMP Configuration via a Configuration File 29
MIB Structure 33
Textual Conventions 34
Objects, Conformance, and Events 34
IP Addresses 35
Persistence 35
Changing a Parameter Value 35
Tables 36
Generic Variables 36
Variables for Administrative Commands 37
SNMP Access Limitation 38
Current MIB Version 38
Sending Configuration Data to the Mediatrix 4100 38
Configuration File 38
Management Information Base – MIB 38
Switching Protocols 39

Chapter 3

IP Address and Network Configuration 41

IP Addresses 41
IP Addresses Formats in the DHCP Server 41
Provisioning Source 42

Services 42
Configuration Source 42
Local Host 43
Static DNS 46
Image 47
Management Server 48
Configuration File Fetching 48
Syslog 49
MGCP Call Agent 50
NCS Call Agent 50
SNTP 51
ETH2 Connector Static IP Address 51
DHCP Server Configuration 52
Connection to the DHCP Behaviour 52
Network Configuration 53
Vendor and Site Specific DHCP Options 53
Vendor Specific Options 53
Site Specific Options 54
Option Codes 55
Entering IP Addresses 55
Entering FQDNs 56
Settings Example 57
Error Handling 58
DHCP Server Failures 58
Vendor/Site Specific Option Missing 58
DNS Failures 58
Ethernet Connection Speed 59
Speed and Duplex Detection Issues 59

Chapter 4

MGCP Protocol Features 61

Introduction 61
MGCP Information 61
Services Provided 61
Call Agent Information 62
Configuration Source 62
Establishing a MGCP Session 64
MGCP Commands 65
MGCP Responses 65
Basic Information 66
Endpoints 67
Retransmission Parameters 68
Packages 70
Setting the Default Package 70
Dynamic Timeout Values 70
Generic Media Package 70
DTMF Package 71
Line Package 71
Extended Analog Line (XL) Package 73
X-P Package 74
Redirecting to a Different Call Agent 75
Meter Pulse 75
MGCP Conference Mode 75
Firewall Traversal 78
Interoperability Configuration 79
Offer/Answer Model 79

Offered Stream Format 80
Session ID and Session Version 80
Multiple Fax Tone Detection 81
Connected RTP Sockets 81
UDP Checksum 81
T.38 Capabilities Using Audio Codec 98 82
Immediate Modem Tone Reporting 82
Brief OSI Signal 82
Fake RFC 3407 Recognition 83
T.38 Negotiation Syntax 83
Brackets Around IP Address in Domain Name 84
Polarity Reversal on Calling Card Service Tone 84

Chapter 5

NCS Protocol Features 85

Introduction 85
NCS Information 85
Services Provided 85
Call Agent Information 86
Configuration Source 86
Basic Information 87
Endpoints 88
Retransmission Parameters 89
Line Package 91
Encoding Name of the Payload Type 18 92
Compatibility Version 93
Interoperability Configuration 93

Chapter 6

Country-Specific Configuration 95

Caller ID Information 95
Caller ID Generation 95
ADSI 96
Setting the Location (Country) 96
Caller ID Selection 97

Chapter 7

Configuration File Download 99

Configuration File Download Server 99
Configuring the TFTP Server 99
Configuring the SNTP Server 99
Configuring the HTTP Server 99
Configuration File Server Settings 99
Setting up the Configuration File Download 101
Configuration Update Status 102
Configuration Files Encryption 103
Configuration Download via TFTP 104
Configuration Download via HTTP 105
Automatic Configuration Update 106
Error Handling 108
Management Server 111

Management Server Configuration 111
Downloading from the Management Server 111
Error Handling 112
Syslog Messages 113
Configuration File Example 114
Supported Characters 114

Chapter 8

Software Download 115

Before Downloading 115
Configuring the TFTP Server 115
Configuring the SNTP Server 115
Configuring the HTTP Server 115
Software Servers Configuration 116
DHCP Configuration 116
Static Configuration 117
Download Procedure 118
Extracting the Zip File 118
Setting up the Image Path 118
Software Download Status 120
Download via TFTP 122
Download via HTTP 123
Automatic Software Update 124
Software Downgrade 126
Emergency Software Procedure 126
Using the Emergency Software 126

Chapter 9

Line Configuration 129

Lines Administrative State 129
Temporary Administrative State 129
Permanent Administrative State 130
Multiple Connections on Endpoints (Lines) 130
Flash Hook Detection 130
Loop Current 131

Chapter 10

Voice Transmissions 133

Codec Descriptions 133
G.711 PCMA and PCMU 133
G.726 134
G.723.1 134
G.729 135
Preferred Codec 135
Enabling Individual Codecs 136
Packetization Time 137
DTMF Transport Type 139
DTMF Payload Type 140
DTMF Detection 140
DTMF Frequencies 140
DTMF Detection Configuration 140

Adaptative Jitter Buffer 142
About Changing Jitter Buffer Values 143
Voice Activity Detection 143
G.711 and G.726 VAD 143
G.729 VAD 144
Echo Cancellation....145
Comfort Noise....145
User Gain....146

Chapter 11

Fax Transmission....147

Introduction....147
Clear Channel Fax....148
T.38 Fax....149
T.38 No-Signal 151

Chapter 12

Bypass Configuration....153

Bypass Connector Settings 153
Standard Bypass 153

Chapter 13

STUN Configuration....155

What is STUN?....155
Restrictions on the Media5 STUN Implementation 155
STUN Client Configuration 156

Chapter 14

SNTP Settings....157

Enabling the SNTP Client....157
Configuration Source....158
DHCP Configuration.... 158
Static Configuration 158
Defining a Custom Time Zone 159
STD / DST 159
OFFSET 159
START / END 159
Example 160

Chapter 15

Management Server Configuration....161

Using the Management Server 161
Configuration Source.... 161

Chapter 16

Quality of Service (QoS) 163

Differentiated Services (DS) Field 163
IEEE 802.1q 164
VLAN 165

Chapter 17

Syslog Daemon 167

Syslog Daemon Configuration 167
Configuration Source 168
Customizing Syslog Messages 169
Configuring the Syslog Daemon Application 169

Chapter 18

Statistics 171

MGCP / NCS Statistics 171
RTP Statistics 171
Statistics Buffers 171
How are Statistics Collected? 172
Example 172

Chapter 19

Maximum Transmission Unit (MTU) 175

What is MTU? 175
Mediatrix 4100 MTU 175
Possible Hardware Problem 175

Chapter 20

Troubleshooting 177

General Operation Issues 177
Calling Issues 180
Fax Issues 180
Software Upgrade Issues 181
SNMP Management Software Issues 183

Appendices

Appendix A

Standards Compliance and Safety Information 187

Standards Supported 187

Disclaimers 188
Federal Communications Commission (FCC) Part 15 188
Federal Communications Commission (FCC) Part 68 188
Industry Canada 189
CE Marking 189
RoHS China 190
Translated Warning Definition 191
Safety Warnings 192
Circuit Breaker (15A) Warning 192
TN Power Warning 192
Product Disposal Warning 192
No. 26 AWG Warning 192
LAN anf FXS Ports Connectors Warning 192
Socket Outlet Warning 192
Safety Recommendations 193

Appendix B

Standard Hardware Information 195

Industry Standard Protocols 195
Hardware Features 195
Display 195
Interfaces 196
Power 196
Casing / Installation 196
Product Architecture Details 196
Real Time Fax Router Technical Specifications 196
Analog Line Interface (FXS) 197
Audio Specifications 197
DTMF Tone Detection 197
DTMF Tone Generation 198
MTBF Value 198
Power Consumption 198
Measurements at the DC input 198
Operating Environment 198
Dimensions and Weight 199
Warranty 199

Appendix C

Cabling Considerations 201

RJ-45 Cable 201
Straight Through Cable 201
Crossover Cable 202
RJ21X Connector (Mediatrix 4124) 203
Creating a RJ21X Cable 203
RJ21X Pinout 203
RJ-11 (Telephone) Cable 205
Wiring Conventions 205
Loop Current vs Cable Length 206

Appendix D

Country-Specific Parameters 207

Definitions 207
Supported MGCP/NCS Signals 208
Conventions 208
Australia 210
Australia 1 210
Australia 2 211
Austria 212
Austria 1 212
Austria 2 213
China 214
France 215
Germany 216
Germany 1 216
Germany 2 217
Hong Kong 218
Indonesia 219
Israel 220
Italy 221
Japan 222
Malaysia 223
Netherlands 224
North America 225
North America 1 225
North America 2 226
Russia 227
Spain 228
Sweden 229
Switzerland 230
Thailand 231
United Arab Emirates 232
UK 233

Appendix E

Glossary 235

Appendix F

List of Acronyms 243

Appendix G

List of MIB Parameters 245

PREFACE

P

About this Manual

Thank you for purchasing the Mediatrix 4100 Series from Media5.

The Mediatrix 4100 Series FXS VoIP Integrated Access Devices are telephony adaptors that connect up to 24 conventional analog telephones or fax machines to a LAN or a WAN with access to an IP Packet Network to permit high-quality, full duplex, audio/fax communications. The Mediatrix 4100 Series are available in the following models:

Table 1: Mediatrix 4100 Series Models

Model	Interfaces
Mediatrix 4108	8 FXS ports
Mediatrix 4116	16 FXS ports
Mediatrix 4124	24 FXS ports

To ensure maximum flexibility, the Mediatrix 4100 can:

- dynamically detect the most commonly used IP Telephony codecs and fax protocols, including T.38
- be auto-provisioned and remotely managed and upgraded
- provide a connection directly to the SCN via an automatic Bypass function in the event of an IP network failure or power outage.

Document Objectives

The *Mediatrix 4100 Reference Manual* provides technical information for the Mediatrix 4100.

Use the *Mediatrix 4100 Reference Manual* in conjunction with the appropriate publications listed in "Related Documentation" on page xiv.

Note: There are many flavours of the Mediatrix 4100 unit. Because of this, some of the information provided may not apply to your particular Mediatrix 4100 unit model.

Intended Audience

This manual provides all the technical information needed to install and manage the Mediatrix 4100. 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. Some installation procedures also require a qualified telephony technician. See "RJ21X Connector (Mediatrix 4124)" on page 203 for more details.

From the perspective of the LAN administrator, a Mediatrix 4100 presents itself like another device to add to the LAN. It requires the same kind of TCP/IP addressing. The Mediatrix 4100 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 4100 document set includes the following:

- *MIB Reference Manual*

  Lists and explains all parameters in the MIB structure.
- *Mediatrix 4100 Quick Start Guide*

  This printed booklet allows you to quickly setup and work with the Mediatrix 4100.
- *Third Party Software Copyright Information*

  This document lists the third-party software modules used in the Mediatrix 4100 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 4100 Reference Manual has three parts:

- "Installation" on page 1. This part describes the installation scenarios of the Mediatrix 4100.
- "SNMP Configuration" on page 23. This part describes all SNMP-related parameters of the Mediatrix 4100.
- "Appendices" on page 185: This part contains supplemental information useful to the reader.

The Mediatrix 4100 Reference Manual contains the following information.

Table 2: Mediatrix 4100 Reference Manual Chapter/Appendices

Title	Summary
Installation	
"Chapter 1 - Installation" on page 3	Describes the installation of the Mediatrix 4100. Also presents the possible states and LED patterns of the Mediatrix 4100, as seen from an operator perspective.
SNMP Configuration	
"Chapter 2 - MIB Structure and SNMP" on page 25	Describes how the Mediatrix 4100 uses the SNMP protocol for its configuration.
"Chapter 3 - IP Address and Network Configuration" on page 41	Describes how to set IP information in the Mediatrix 4100 and how to configure a DHCP server.
"Chapter 4 - MGCP Protocol Features" on page 61	Describes how to set information exclusive to the Media Gateway Control Protocol (MGCP).
"Chapter 5 - NCS Protocol Features" on page 85	Describes how to set information exclusive to the Network-based Call Signalling (NCS) protocol.
"Chapter 6 - Country-Specific Configuration" on page 95	Describes how to set the Mediatrix 4100 with the proper country settings.
"Chapter 7 - Configuration File Download" on page 99	Describes how to use the configuration file download feature to update the Mediatrix 4100 configuration.
"Chapter 8 - Software Download" on page 115	Describes how to download a software version available on the designated software server into the Mediatrix 4100.

Table 2: Mediatrix 4100 Reference Manual Chapter/Appendices (Continued)

Title	Summary
“Chapter 9 - Line Configuration” on page 129	Describes the features available on the lines connected to the Mediatrix 4100.
“Chapter 10 - Voice Transmissions” on page 133	Describes the various codecs the Mediatrix 4100 supports for transmitting audio signals.
“Chapter 11 - Fax Transmission” on page 147	Describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 4100.
“Chapter 12 - Bypass Configuration” on page 153	Describes the Bypass feature that can be used in the event of a power failure or network failure.
“Chapter 13 - STUN Configuration” on page 155	Describes how to configure the STUN client of the Mediatrix 4100.
“Chapter 14 - SNTP Settings” on page 157	Describes how to configure the Mediatrix 4100 to enable the notion of time (date, month, time) into it.
“Chapter 15 - Management Server Configuration” on page 161	Describes how to configure the Mediatrix 4100 to connect to a module or software that is used to remotely set up Mediatrix units.
“Chapter 16 - Quality of Service (QoS)” on page 163	Defines the QoS (Quality of Service) features available on the Mediatrix 4100.
“Chapter 17 - Syslog Daemon” on page 167	Describes how to configure and use the Syslog daemon.
“Chapter 18 - Statistics” on page 171	Defines the statistics the Mediatrix 4100 can collect.
“Chapter 19 - Maximum Transmission Unit (MTU)” on page 175	Describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 4100.
“Chapter 20 - Troubleshooting” on page 177	Examines some of the problems you may experience when connecting the Mediatrix 4100 to the network and provides possible solutions.
Appendices	
“Appendix A - Standards Compliance and Safety Information” on page 187	Lists the various standards compliance of the Mediatrix 4100.
“Appendix B - Standard Hardware Information” on page 195	Lists the technical hardware information of the Mediatrix 4100.
“Appendix C - Cabling Considerations” on page 201	Describes the pin-to-pin connections for cables used with the Mediatrix 4100.
“Appendix D - Country-Specific Parameters” on page 207	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 4100 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 187.

This Appendix describes the international agency compliance and safety information for the Mediatrix 4100. 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 4100'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 4100 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

Page Left Intentionally Blank

CHAPTER 1

Installation

This chapter describes the installation and initial provisioning of the Mediatrix 4100.

Requirements

The Mediatrix 4100 requires the following items to work properly:

Table 3: Required Items

Item	Description
Analog lines (Mediatrix 4124 only)	Standard analog lines wired into a RJ21X cable. This cable may be directly connected to the Key Service Unit (KSU) or PBX Main Distribution Frame. See "RJ21X Connector (Mediatrix 4124)" on page 203 for more details.
DHCP Server (optional)	Supplies network parameters to the Mediatrix 4100.
DNS Server (optional)	Translates domain names into IP addresses.
Call Agent	Manages the active calls of the Mediatrix 4100.
Management Server (optional)	Module or software used to remotely manage and configure the Mediatrix 4100. 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 4100.

Safety Recommendations

To ensure general safety, follow these guidelines:

- Do not open or disassemble the Mediatrix 4100.
- Do not get the Mediatrix 4100 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 4100 package contains the following items:

- the Mediatrix 4100 unit
- two rack-mounting brackets
- a power cord for the country in which you are using the Mediatrix 4100
- a printed Flyer

You also need a 10/100 BaseT Ethernet RJ-45 cable.

Overview

The Mediatrix 4100 is a standalone Internet telephony access device that connects to virtually any business telephone system supporting standard analog lines.

The Mediatrix 4100 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.

This version of the Mediatrix 4100 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 39.

About the Mediatrix 4100

The Mediatrix 4100:

- 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.723.1A
    - 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 802.1q user priority tagging

Placing a Call

You can place a call from a telephone or fax connected to:

- a port of the Mediatrix 4100 (Mediatrix 4108/4116)
- the analog line plugged into the Mediatrix 4100 (Mediatrix 4124)

The unit automatically detects if the call originates from a voice or fax transmission and acts accordingly.

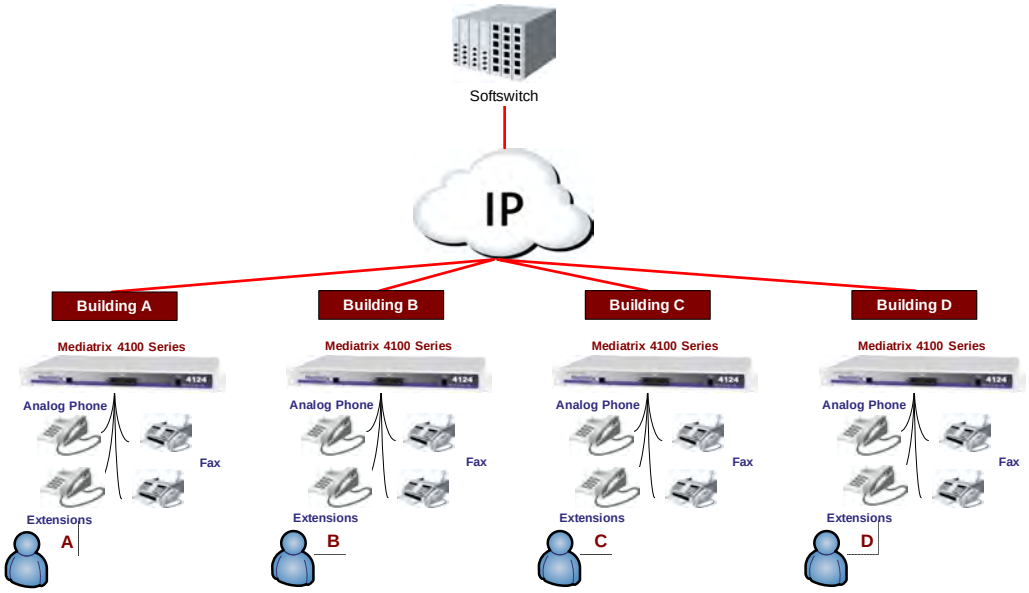
When placing a call, the Mediatrix 4100 collects the DTMF digits dialed and sends a message to the Call Agent. The Call Agent sends back a list of contacts where the dialed number could be located.

You can dial on a telephone/fax machine connected to the Mediatrix 4100 as you normally do.

Multi-Tenant / Multi-Dwelling Units (MTU/MDU) IP Telephony

The Mediatrix 4100 can be used as a service unit for large buildings such as an apartment building. The analog lines of the building are directly connected to the Mediatrix 4100, which allows you to send voice or fax communication on an IP network such as a LAN, WAN or the public Internet.

Figure 1: MTU/MDU IP Telephony Solution



For more information on this scenario, please refer to *Configuration Notes 251: Configuring A Mediatrix 41xx FXS Gateway with a MGCP Call Agent* available on the Mediatrix Support Portal.

Panels

This section provides an overview of the front and rear panels of the Mediatrix 4100.

Front Indicators

Figure 2 shows the visual indicators and various connectors located on the front of the Mediatrix 4100.

Figure 2: Front Panel Indicators and Connectors

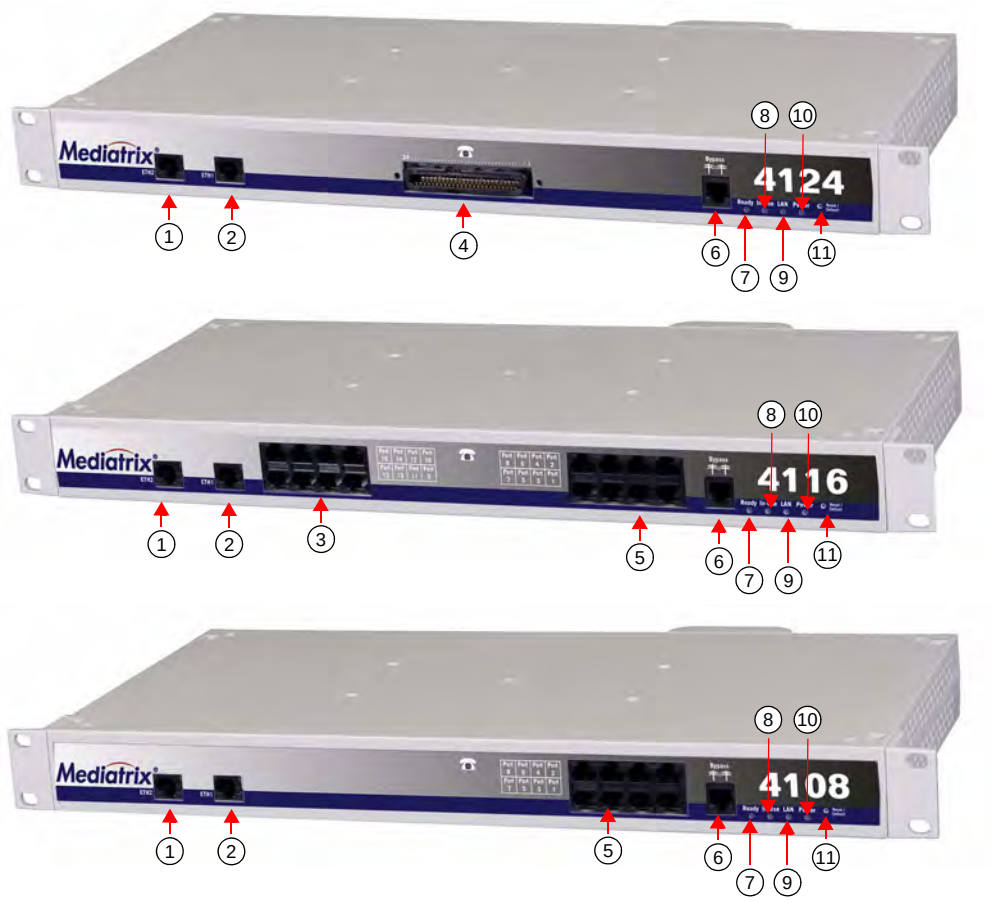


Table 4 describes the LEDs and connectors on the front panel of the Mediatrix 4100.

Table 4: Front Connectors and LEDs

	Connector / LED	Description
1.	ETH2	A 10/100 BaseT Ethernet RJ-45 connector that can be connected into the network card of a computer. This connector may not be available on older models.
2.	ETH1	RJ-45 connector for 100 BaseT Ethernet access to a LAN.
3.	FXS connectors	Eight RJ-11 connectors to attach conventional telephones or G3 fax machines. These connectors are available on the Mediatrix 4116 only.
4.	Analog Lines	A RJ21X connector with 24 RJ-11 Teladapt connectors to provide line cord connection to analog phones, faxes and modems. This connector is available on the Mediatrix 4124 only. See "RJ21X Connector (Mediatrix 4124)" on page 203 for more details.

Table 4: Front Connectors and LEDs (Continued)

	Connector / LED	Description
5.	FXS connectors	Eight RJ-11 connectors to attach conventional telephones or G3 fax machines. These connectors are available on the Mediatrix 4108 and Mediatrix 4116 only.
6.	Bypass	Permits users to make and receive calls even when the Mediatrix 4100 is not operating.
7.	Ready LED	When lit, at least one of the FXS lines configured to be registered with a Call Agent is properly and successfully registered.
8.	In Use LED	When lit, at least one of the FXS lines is in use.
9.	LAN LED	Provides the state of the network connected to the *ETH1* and *ETH2* connectors
10.	Power LED	When lit, power is applied to the Mediatrix 4100.
11.	Reset / Default button	Resets configuration parameters of the Mediatrix 4100 to default (known) values. It can be used to reconfigure the unit. See "Reset / Default Switch" on page 18 for more details.

See "LED Indicators" on page 14 for a detailed description of the LED patterns the Mediatrix 4100 may have and the states they represent.

Port Numbering Convention (Mediatrix 4108/4116)

The following describes the port numbering conventions of the FXS connectors available on the Mediatrix 4108 and Mediatrix 4116. Note that the connectors in the left section are available only on the Mediatrix 4116 model.

Figure 3: FXS Connectors Port Numbering Convention (Mediatrix 4108/4116)

Analog Lines Numbering Convention (Mediatrix 4124)

The following describes the numbering conventions of the FXS analog lines available on the Mediatrix 4124.

Figure 4: Analog Lines Numbering Convention (Mediatrix 4124)

Rear Connectors

The Mediatrix 4100 has several connections that must be properly set. Figure 5 shows the back panel of the Mediatrix 4100.

Figure 5: Back Panel Connector

Table 5 describes the back panel connections.

Table 5: Back Connections of the Mediatrix 4100

Connection	Description
Power connector	IEC320-C14 Power Cord Receptacle. This power cord supplies an internal Switching Mode Power Supply (SMPS) Universal input. The power supply range is 100 – 240 VAC; 50/60 Hz; 1.6 A.

Choosing a Suitable Installation Site

Warning: The analog lines of the Mediatrix 4100 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 4100 is suitable for use in an office environment where it can be placed in the same room or cabinet where the PBX/telephony equipment is located. The unit can be mounted on a standard 48.26 cm (19 in.) equipment rack.

Location

Install the Mediatrix 4100 in a well-ventilated location where it will not be exposed to high temperature or humidity. Do not install the Mediatrix 4100 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 4100, ensure that:

- The Mediatrix 4100 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 4100.
- The airflow is not restricted around the Mediatrix 4100 or through the vents in the side and back of the unit. The unit requires a minimum of 25 mm (1 in.) clearance.
- The fan on the Mediatrix 4100 is not blocked or that the back of the unit is not too close to the wall.

- The operating temperature is between 0°C and 40°C.
- The humidity is not over 85% and is non-condensing.

Rack-Mounting

The Mediatrix 4100 is 4.4 cm (1.74 in.) high. It meets the EIA-310-D and ETS 300 119 standards.

To rack-mount the Mediatrix 4100:

1. Disconnect all of the cables from the Mediatrix 4100.
2. Insert the Mediatrix 4100 into the rack and secure with suitable screws (not provided). Be sure that the ventilation holes are not obstructed.
3. Proceed to "Hardware Connection" on page 9.

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 4100, wipe with a soft dry cloth. Do not use volatile liquids such as benzine 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

This section describes how to set the connectors of the Mediatrix 4100.

Warning: Do not connect the Mediatrix 4100 directly to Telecommunication Systems.

Caution: The Mediatrix 4100 must be installed on a circuit equipped with a breaker so that you can easily power the unit off if required.

See "Appendix C - Cabling Considerations" on page 201 for more details on the cables the Mediatrix 4100 uses.

Reserving an IP Address

Before connecting the Mediatrix 4100 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 4100 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.

Connecting Cables – Mediatrix 4108/4116 Models

The following describes how to connect the various cables to the Mediatrix 4108 or Mediatrix 4116.

Figure 6: Mediatrix 4108/4116 Hardware Installation

▶ **To install the cables:**

1. Before you begin, be sure that the Mediatrix 4100 is powered off.
2. Connect the power cord to its connector on the back of the unit.
3. Connect analog telephones or fax machines into the phone/fax connectors

   The Mediatrix 4108 has 8 connectors, while the Mediatrix has 16 connectors.

   Use a standard telecommunication cord with a minimum of 26 AWG wire size.

Note: The Mediatrix 4100 telephone line interface has been designed to interface with a conventional telephone or fax machine. Connections to FXS ports of third party devices such as a PBX / Key System could damage the Mediatrix 4100.

4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *ETH1* connector of the Mediatrix 4100; connect the other end to a compatible Ethernet interface that supplies TCP/IP network access (e.g., router, switch, hub or computer).

   Use a standard telecommunication cord with a minimum of 26 AWG wire size.
5. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *ETH2* connector of the Mediatrix 4100 and connect the other end to the network card of a computer.

   This connector may not be available on older models.

   Use a standard telecommunication cord with a minimum of 26 AWG wire size. You can either use a crossover or straight Ethernet cable because it performs automatic MDI / MDIX detection. See "RJ-45 Cable" on page 201 for more details.
6. Connect a SCN line into the *Bypass* connector of the Mediatrix 4100 (optional).

   Use a standard telecommunication cord with a minimum of 26 AWG wire size.
7. Connect the other end of the power cord to an electrical outlet.

Warning: The electrical outlet must be installed near the Mediatrix 4100 so that it is easily accessible.

Connecting Cables – Mediatrix 4124 Model

The following describes how to connect the various cables to the Mediatrix 4124.

Figure 7: Mediatrix 4124 Hardware Installation

▶ **To install the cables:**

1. Before you begin, be sure that the Mediatrix 4124 is powered off.
2. Connect the power cord to its connector on the back of the unit.
3. Connect a RJ21X cable into the RJ21X receptacle of the Mediatrix 4124.

   The RJ21X cable contains the connections for the 24 analog lines to connect to the Mediatrix 4124. See "RJ21X Connector (Mediatrix 4124)" on page 203 for more details.
4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *ETH1* connector of the Mediatrix 4124; connect the other end to a compatible Ethernet interface that supplies TCP/IP network access (e.g., router, switch, hub or computer).

   Use a standard telecommunication cord with a minimum of 26 AWG wire size.
5. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *ETH2* connector of the Mediatrix 4100 and connect the other end to the network card of a computer.

   This connector may not be available on older models.

   Use a standard telecommunication cord with a minimum of 26 AWG wire size. You can either use a crossover or straight Ethernet cable because it performs automatic MDI / MDIX detection. See "RJ-45 Cable" on page 201 for more details.
6. Connect a SCN line into the *Bypass* connector of the Mediatrix 4124 (optional).

   Use a standard telecommunication cord with a minimum of 26 AWG wire size.
7. Connect the other end of the power cord to an electrical outlet.

Warning: The electrical outlet must be installed near the Mediatrix 4124 so that it is easily accessible.

Starting the Mediatrix 4100 for the First Time

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 3 - IP Address and Network Configuration" on page 41 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 18.

IP Address Discovery or Configuration

Note: This section applies to the IP configuration of the **ETH1** port.

Once the physical connection is complete and the Mediatrix 4100 is powered up, the first thing to do is find out the IP address the Mediatrix 4100 is using. The Mediatrix 4100's IP address can be set either dynamically or statically. The default behaviour of the Mediatrix 4100 is to try to obtain a dynamic IP address through a DHCP server.

Caution: If you set a Mediatrix 4100 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 4100 is 192.168.0.10.

Dynamic IP Address Discovery

Before connecting the Mediatrix 4100 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 4100 by either:

- consulting your DHCP server's logs to find out details on the DHCP lease that was given to the Mediatrix 4100.
- using a network packet sniffer (e.g., Wireshark) to examine the DHCP messages exchanged between the Mediatrix 4100 and your DHCP server while the Mediatrix 4100 boots up.

To start the Mediatrix 4100 with a dynamic IP address:

1. If you need to discover the IP address of the Mediatrix 4100, install and start your network packet sniffer.
2. Power on the Mediatrix 4100 by connecting the other end of the power cord to an electrical outlet. The electrical outlet must be installed near the Mediatrix 4100 so that it is easily accessible.

Note: If the *Power* LED is always blinking and never turns on, this means that the Mediatrix 4100 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 12.

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 4100 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 *ETH1* connector of the Mediatrix 4100 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 4100 by connecting the other end of the power cord to an electrical outlet. The electrical outlet must be installed near the Mediatrix 4100 so that it is easily accessible.
4. Insert a small, unbent paper clip into the *Reset / Default* switch hole located at the front of the Mediatrix 4100. 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 4100 uses the default IP address 192.168.0.1. Refer to "Recovery Mode" on page 18 for details on the recovery mode procedure.

   You must perform the recovery mode in a closed network and perform it on only one Mediatrix 4100 at a time, since the default IP address is the same on every unit.

Initial Provisioning Sequence

When starting the Mediatrix 4100 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 4100 hardware as per "Hardware Connection" on page 9.

The Mediatrix 4100 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 4100 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.

▶ **Initial provisioning sequence:**

1. When the Mediatrix 4100 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 4100 IP address.

   The following are some of the network parameters assigned via DHCP:
   - Mediatrix 4100 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 4100 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.

LED Behaviour in Starting Mode

When the Mediatrix 4100 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 18 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 *LAN* LED.

Ready LED

The *Ready* LED provides an “at-a-glance” view of the Mediatrix 4100 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 8 on page 16.

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 8 on page 16.

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

LAN LED

The *LAN* LED provides the Link and Heartbeat status of the network connected to the *ETH1* and *ETH2* connectors. 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 LAN is loaded. Patterns and meanings of the *LAN* LED are described in Table 8 on page 16.

Power LED

The *Power* LED indicates whether or not the Mediatrix 4100 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 8 on page 16.

LED Patterns

Table 6 describes the different states a Mediatrix unit can have and their associated LED patterns.

Table 6: States and LED Patterns

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
Booting	Follows a hardware start or a reset.	See “Booting LED Pattern Description” on page 16			
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 16			
AdminMode	Calls are not permitted and maintenance actions can be performed.	See “AdminMode LED Pattern Description” on page 16			

Table 6: States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	**In Use**	**LAN**	**Power**
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 *Reset / Default* switch is pressed and held for at least 2 seconds.	Off	Off	Off	Blink 1 Hz 50%
Reboot Pending	Triggered when the *Reset / Default* switch is pressed in either the *ResetPending* or *RecoveryMode Pending* states. The unit prepares for a physical shutdown and restart.	Off	Off	Off	Off
Recovery Mode Pending	Triggered when the *Reset / Default* 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%
Default Settings Pending	Triggered when the *Reset / Default* switch is not released while in *RecoveryModePending* state. At run time, if the *Reset / Default* 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 *Reset / Default* 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%, *one at a time*, 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 *Booting* 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 16.

Booting LED Pattern Description

While in the *Booting* state, the LEDs of the Mediatrix 4100 behave independently; the following table indicates the behaviour for each LED.

Table 7: LED Patterns in Booting Mode

LED	Pattern	Meaning
Ready	Steady Off	Not Ready.
In Use	Steady Off	Cannot be in use.
LAN (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected or hardware control not activated.
	Blinking (variable rate)	Ethernet activity detected.
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 4100 behave independently; the following table indicates the behaviour for each LED.

Table 8: 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.
LAN (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 4100 behave independently; the following table indicates the behaviour for each LED.

Table 9: LED Patterns in AdminMode

LED	Pattern	Meaning
Ready	Blinking 1 Hz 75%	*Ready* and *Power* LEDs blink off phase at 180 degrees.
In Use	Steady Off	All analog lines are not available.

Table 9: LED Patterns in AdminMode (Continued)

LED	Pattern	Meaning
LAN (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected.
	Blinking (variable rate)	Ethernet activity detected.
Power	Blinking 1 Hz 75%	*Ready* and *Power* LEDs blink off phase at 180 degrees.

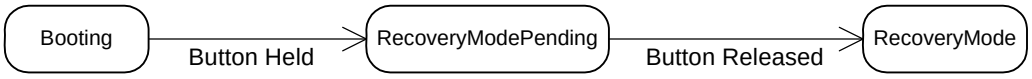
Recovery Mode LED Patterns

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:

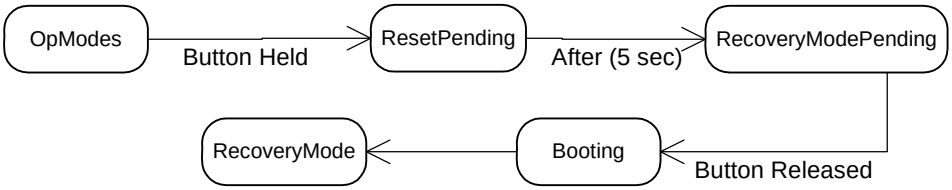
Figure 8: LED Pattern at Start-Time



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 4100 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 4100 is running without powering the unit off. Table 10 describes the actions you can perform in this case.

Table 10: Reset / Default Switch Interaction

Reset / Default Switch Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	LAN	Power
2 to 5 seconds	Restarts the Mediatrix 4100	No changes are made to the Mediatrix 4100 settings.	Off	Off	Off	Blink
5 to 10 seconds	Restarts the Mediatrix 4100 in Recovery Mode	Sets the Mediatrix 4100 IP address to its default value in the MIB and restarts the unit.	Blink	Blink	Blink	Blink[a]
10 to 15 seconds[b]	Restarts the Mediatrix 4100 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 20 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 4100 in "Recovery Mode". Note that this can take up to 40 seconds.
- 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 4100 back to its default factory settings.

See "LED Indicators" on page 14 for a detailed description of the LED patterns related to the *Reset / Default* switch.

Recovery Mode

The recovery mode restarts the Mediatrix 4100 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 4100 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 *ETH1* connector of the Mediatrix 4100 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 *ETH1* connector of the Mediatrix 4100 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 front of the Mediatrix 4100.

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
   - sntpConfigSource

   All the persistent MIB values are kept.

   In this mode, MGCP/NCS is deactivated. Only SNMP 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 4100 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 4100 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 35 for more details.

Note: The recovery mode does not alter any persistent configuration data of the Mediatrix 4100.

Factory Reset

The Factory reset reverts the Mediatrix 4100 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 Factory reset creates a new configuration file with the default factory values. It should be performed with the Mediatrix 4100 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 20 for more details.

To trigger the Factory Reset:

1. Insert a small, unbent paper clip into the *Reset / Default* switch hole of the Mediatrix 4100.

   Do not depress before all the LEDs stop blinking and are steadily ON.

2. Release the paper clip.

   The Mediatrix 4100 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 4100 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 4100.

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 4100 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 18 for more details.

Software Restart

You can initiate a software restart of the Mediatrix 4100 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 4100 restarts.

Restart Behaviour

This feature affects the behaviour of the Mediatrix 4100 when it restarts.

You can instruct the Mediatrix 4100 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 4100 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 4100 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 4100 you want to verify. If the Mediatrix 4100 does not respond, do the following:

- Verify that the LAN cable is securely connected to the Mediatrix 4100 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 *LAN* LED should be ON or blinking).
- Verify that the call agent is operational.

SNMP Configuration

Page Left Intentionally Blank

CHAPTER 2

MIB Structure and SNMP

This chapter describes how the Mediatrix 4100 uses the SNMP protocol for its configuration.

SNMP Overview

The Mediatrix 4100 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 4100 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 11: 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 12: SNMPv2 Message Type

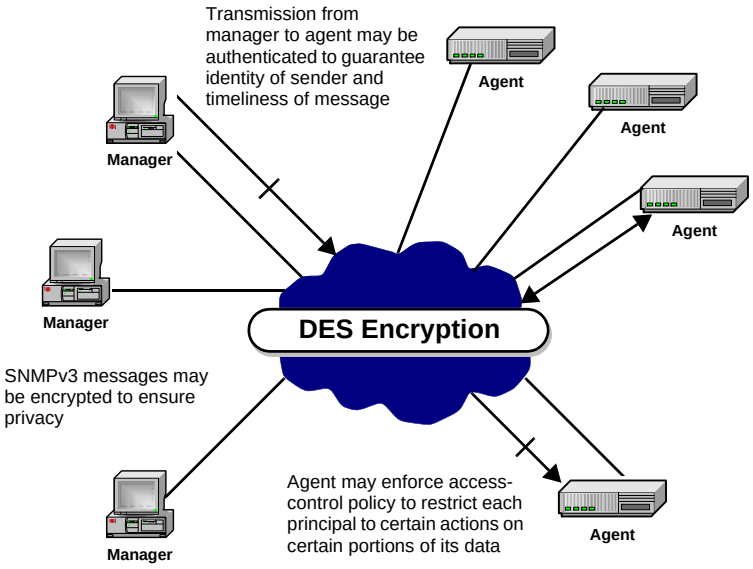
Operator	Description
get-bulk	Uses BULK Requests to query for a tree of information about a network entity. A variable put in command line specifies which portion of the object identifier space will be searched using BULK Requests. All variables in the subtree below the given variable are queried as 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 10). 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 10: 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 20 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 20 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 4100 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 4100 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 4100 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 4100, see "Chapter 7 - Configuration File Download" on page 99.

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 *SnmpGenericTemplate.xml* file located under *Unit Manager Network 3.2\UnitManager\DefaultCfgFile* folder. The contents of the *SnmpGenericTemplate.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 4100, 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 11: SNMP Agent Section Example

```
<SnmpAgentConfig>
 <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"/>
```

```
      <vacmAccessContextMatch ValueType="UINT32" Value="1"/>
      <vacmAccessReadViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <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"/>
      <vacmAccessWriteViewName ValueType="OCTET_STRING" Value="PublicView"/>
      <vacmAccessNotifyViewName ValueType="OCTET_STRING" Value="PrivateView"/>
      <vacmAccessStorageType ValueType="UINT32" Value="4"/>
      <vacmAccessStatus ValueType="UINT32" Value="1"/>
     </g>
    </vacmAccessTable>
   </vacmMIBObjects>
  </snmpVacmMIB>
 </snmpModules>
</snmpV2>
</SnmpAgentConfig>
```

Enable/Disable SNMPv3
Enable/Disable SNMPv3
Enable/Disable SNMPv3
Enable/Disable SNMPv3
Enable/Disable SNMPv3
Enable/Disable SNMPv3
Enable/Disable SNMPv1
Enable/Disable SNMPv1
Enable/Disable SNMPv1
Enable/Disable SNMPv1
Enable/Disable SNMPv2
Enable/Disable SNMPv2
Enable/Disable SNMPv2
Enable/Disable SNMPv2

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 11 on page 29 with the following icon: ← **Enable/Disable SNMPv*x***.

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 11 on page 29 with the following icon: ← **Enable/Disable SNMPv*x***.

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 11 on page 29 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 11 on page 29 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 11 on page 29 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 13: 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 *mediatrixExperimental* 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 14: 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 3 - IP Address and Network Configuration” on page 41 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 fore more details.

Objects, Conformance, and Events

Each MIB may have three types of data.

Table 15: 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 3 - IP Address and Network Configuration" on page 41 for more details.

Persistence

A variable may either be persistent or volatile.

Table 16: Storage Clauses

Clause	Definition
Persistent	*Persistent* parameters are saved into the unit's memory and restored when it restarts. All the variables with the *Access = Read Write* attribute are persistent, except the variables representing commands (such as *sysAdminCommand*).
Volatile	*Volatile* 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. *Statistics* are also volatile parameters that are lost every time the unit restarts.

Changing a Parameter Value

The Mediatrix 4100 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 4100. 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 4100. 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 4100 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.

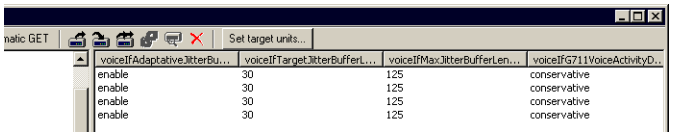
Table 17 gives an example of the *ifTable*.

Table 17: 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 12 shows a table built in the Unit Manager Network from the *voiceifTable* parameters.

Figure 12: voiceIftable Example



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 18: 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 (*groupAdminIndex*), taken from this table (*groupAdminTable*), 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 19: 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 4100 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 4100 can be accessed via SNMP in the *snmpAgentAccess* variable.

   You have the following choices:

Table 20: SNMP Access Limitation Parameters

Access	Description
lanOnly	SNMP connections are only permitted on the LAN side, which is usually associated with the *ETH2* connector. The LAN IP address is provisioned by the *lanStaticAddress* variable.
wanOnly	SNMP connections are only permitted on the WAN side, which is usually associated with the *ETH1* connector. However, if the WAN interface is down and the unit reverts to its LAN configuration, the SNMP agent can access the Mediatrix 4100 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 4100.

1. In the *sysMgmtMIB*, locate the *sysMibVersion* variable.

   This variable displays the current version of the MIB.

Sending Configuration Data to the Mediatrix 4100

The configuration data can be provisioned into the Mediatrix 4100 in two ways:

- as a configuration file sent from the Management Server to the Mediatrix 4100 via TFTP
- as a MIB sent from the Management Server to the Mediatrix 4100 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 13 for more details).

For more information on how to use a configuration file for updating the Mediatrix 4100, see "Chapter 7 - Configuration File Download" on page 99.

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 4100 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 4100 unit.

   After the unit restarts, it uses the selected protocol. See:

   - “Chapter 4 - MGCP Protocol Features” on page 61
   - “Chapter 5 - NCS Protocol Features” on page 85

CHAPTER 3

IP Address and Network Configuration

The Mediatrix 4100 must be provisioned with various IP addresses and network parameters to be fully functional. This occurs each time the Mediatrix 4100 is started or when an IP address value is changed in the MIB. The Mediatrix 4100 can use static network parameters as well as parameters provided by a DHCP server 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 2 - MIB Structure and SNMP" on page 25 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 21: 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 *ipAddressStatus* folder.

IP Addresses Formats in the DHCP Server

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

Table 22: 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 4100 IP information may come from a variety of sources.

Table 23: IP Address Provisioning Sources

Source	Description
Static	You manually enter the value and it remains the same every time the Mediatrix 4100 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 4100 is used. See “Site Specific Options” on page 54 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 53 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.

Services

This section describes the services the Mediatrix 4100 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 52 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 4100 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 4100 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 52 for more details.

The Mediatrix 4100 can receive numerous information from the DHCP server, including the vendor or site specific information. Note that the Mediatrix 4100 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.

Verifying the DHCP-Assigned IP Addresses

You can query the MIB structure to see the IP addresses that have been assigned to the Mediatrix 4100. 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 4100 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 4100 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 4100 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 4100 needs to work properly. This group is vital to the proper operation of the Mediatrix 4100. If a variable of this group is not properly set, the Mediatrix 4100 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 24: 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 181 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* variable is enabled, the primary and secondary DNS addresses are set with static values. See "Static DNS" on page 46 for more details.

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

3. Restart the Mediatrix 4100 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 Mediatrix 4100. 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 25: WAN IP Address Source Settings

Option[a]	Description
localAddress	The WAN address is the one that is set in the *localHostAddress* variable, whereas the *localHostStaticWanAddress* is ignored.
static	The Mediatrix 4100 has a static WAN address. The address is configured in the *localHostStaticWanAddress* variable. Note that this setting allows a limited NAT traversal scheme.

a. pppoe is not available on the Mediatrix 4100.

Table 26: WAN IP Address Source

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

2. Restart the Mediatrix 4100 so that the changes may take effect.

FQDN Configuration Source

You can select where to get the Fully Qualified Domain Name (FQDN) of the gateway. The Mediatrix 4100 uses the FQDN to register to the MGCP/NCS call agent.

▶ **To select the FQDN configuration source:**

1. 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 4100 FQDN information.

   Table 27: FQDN Configuration Source

Source	Comment
static	Set the *localHostStaticFqdn* variable in the *ipAddressConfigLocalHostStatic* group.
dhcp	The DHCP-provided “host name” (option number 12) is used. No site specific code is provided. The Mediatrix 4100 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 *localHostStaticPrimaryDns* or *localHostStaticSecondaryDns* 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 4100 in the read-only variable *localHostFqdn* (*ipAddressStatus LocalHost* group).

2. Restart the Mediatrix 4100 so that the changes may take effect.

SNMP Configuration

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

Table 28: 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 4100 uses the SNMP protocol for software configuration. Set the following SNMP-related variable to properly use the protocol.

Table 29: 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 4100 receives 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 DHCP.

However, you can set static values for the primary and secondary DNS IP addresses, even when the Mediatrix 4100 is set by DHCP. These static values can thus override DHCP provisioning

The Mediatrix 4100 may receive DNS addresses from two sources:

- from an ISP via DHCP
- from the static local host DNS IP addresses

Table 30 explains how DNS addresses are attributed to the Mediatrix 4100.

Table 30: DNS Addresses Possibilities

Configuration Source	localHostDns OverrideEnable	DNS address of Mediatrix 4100
DHCP	disabled	DHCP DNS
DHCP	enabled	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.

2. Restart the Mediatrix 4100 so that the changes may take effect.

Image

The *ipAddressConfigImage* group provides the configuration necessary to download applications into the Mediatrix 4100. 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 31: Image Information Source

Variable	Default Static Value	DHCP Source
imagePrimaryHost	“192.168.0.10”	Use option specified in variable *imageDhcpPrimarySiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 117, bytes 0-3.
imagePrimaryPort	69[a]	Use option specified in variable *imageDhcpPrimarySiteSpecificCode*, 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.
imageSecondaryHost	“192.168.0.10”	Use option specified in variable *imageDhcpSecondarySiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 118, bytes 0-3.
imageSecondaryPort	69[a]	Use option specified in variable *imageDhcpSecondarySiteSpecificCode*, 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.

3. Restart the Mediatrix 4100 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:**

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

Table 32: Management Server Source

Variable	Default Static Value	DHCP Source
msHost	N/A	Use option specified in variable *msDhcpSiteSpecificCode*, 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 *msDhcpSiteSpecificCode*, 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.

3. Restart the Mediatrix 4100 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 33: Configuration File Fetching Source

Variable	Default Static Value	DHCP Source
configFileFetching Host	N/A	Use option specified in variable *configFileFetchingDhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 201, bytes 0-3.

Table 33: Configuration File Fetching Source (Continued)

Variable	Default Static Value	DHCP Source
configFileFetching Port	N/A	Use option specified in variable *configFileFetchingDhcpSiteSpecificCode*, 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 4100 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 34: Syslog Source

Variable	Default Static Value	DHCP Source
syslogHost	“192.168.0.10”	Use option specified in variable *syslogDhcpSiteSpecificCode*, 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 4100 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 *mgcpCASelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 35: MGCP Call Agent Source

Variable	Default Static Value	DHCP Source
mgcpCAHost	“192.168.0.10”	Use option specified in variable *mgcpCADhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 207, bytes 0-3.
mgcpCAPort	2727	Use option specified in variable *mgcpCADhcpSiteSpecificCode*, 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 4100 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 *ncsCASelectConfigSource* variable (under the *ipAddressConfigNcsCallAgent* group).
2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

Table 36: NCS Call Agent Source

Variable	Default Static Value	DHCP Source
ncsCAHost	“192.168.0.10”	Use option specified in variable *ncsCADhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 210, bytes 0-3.
ncsCAPort	2727	Use option specified in variable *ncsCADhcpSiteSpecificCode*, 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 4100 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 14 - SNTP Settings" on page 157 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 4100 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 37: 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.

ETH2 Connector Static IP Address

You can use the *ETH2* connector of the Mediatrix 4100 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 *ETH2* connector and use this LAN static IP address according to the VLAN substitution or always enabled configuration.

▶ **To set the *ETH2* connector static IP address:**

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

Table 38: LAN Connector Static IP Address

Parameter	Description
ipRouting	To set the *lanStaticAddress* variable as the Local Area Network (LAN) IP address used by the Mediatrix 4100's *ETH2* interface, set the variable *ipRoutingEnable* to **enable**.
always	Sets the *lanStaticAddress* as the Local Area Network (LAN) IP address used by the Mediatrix 4100's *ETH2* interface.

2. In the *ipAddressConfig* folder, set the static *ETH2* connector information as follows:

Table 39: LAN Interface Source

Variable	Default Static Value	Description
lanStaticAddress	192.168.10.1	LAN IP address used by the unit's *ETH2* interface.
lanStaticNetworkMask	255.255.255.0	LAN subnet mask used by the unit's *ETH2* 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 4100 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

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 4100 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 4100 on the network.

Connection to the DHCP Behaviour

When the Mediatrix 4100 restarts, it requests a DHCP offer to get its IP addresses and network information. The Mediatrix 4100 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 4100 stops broadcasting as soon as it receives at least one reply. If the offer is valid, the Mediatrix 4100 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 4100 makes its DHCP request that will be released immediately.

Network Configuration

Table 40 lists some of the network options to configure in the DHCP server:

Table 40: 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

This section briefly describes vendor and site specific DHCP options.

Most of the MIB variables described in "Services" on page 42 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 57 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 41 on page 55 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 41 on page 55 for actual codes.

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

Figure 13: General Layout of a Vendor Specific Information Option

43	Len	Data	Data	Data	Data	…

Figure 14: Layout for Encapsulated Vendor Specific Options

43	Len	Code1	Len1	Data1	Data1	…	Code2	Len2	Data2	Data2	…

Figure 15 is an example of a vendor specific option containing an *msHost* IP address (192.168.1.2).

Figure 15: Example of Encapsulated Vendor Specific Option

43	6	200	4	192	168	1	2

Mediatrix 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 55. The layout for storing FQDNs is explained in section "Entering FQDNs" on page 56.

Vendor Class ID

When using the vendor specific option, first define a Vendor Class ID for the Mediatrix 4100 (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 *Mediatrix 4108*, *Mediatrix 4116*, or *Mediatrix 4124*, depending on your unit model.

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 Mediatrix 4100 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 55 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 Mediatrix 4100 is used. You are responsible to allocate an option number (between 128 and 254) for each information element to be stored.

Mediatrix 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 55. The layout for storing FQDNs is explained in section "Entering FQDNs" on page 56.

Figure 16 is an example of site specific option #146, containing address 192.168.0.1.

Figure 16: 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 55 for more details on the syntax to use.

Option Codes

This table lists all vendor specific sub-option codes.

Table 41: 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 41 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 42: 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 17: Example – Short Address String

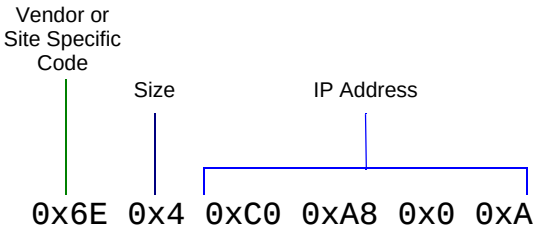
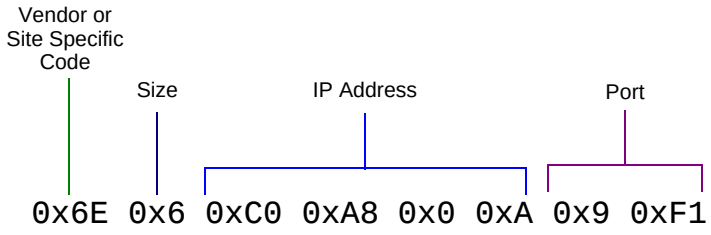


Figure 18: Example – Long Address String



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 55.

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

Figure 19: 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 20: 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 addess 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 addess 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 43: 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 44: 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 45: 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 4100 cannot contact the DHCP server, it performs one of the following actions:

1. Retries contacting the DHCP server until it answers. The Mediatrix 4100 does not restart.
2. Uses the replacement value from Table 45 for all variables that depend on the DHCP.

This assumes that the Mediatrix 4100 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 4100 uses the replacement value from Table 45 for each variable that depends on missing vendor/site specific options.

DNS Failures

If the DNS cannot be contacted, the Mediatrix 4100 performs the following steps:

1. The Mediatrix 4100 sends a first request to the primary DNS server.

2. If the DNS server cannot be contacted within two seconds, the Mediatrix 4100 sends a request to the secondary DNS server.
3. If the secondary DNS server cannot be contacted, the Mediatrix 4100 uses the replacement value from Table 45 for all variables that depend on the DNS.

Ethernet Connection Speed

You can set the speed of the Ethernet connection of the Mediatrix 4100.

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:
   - *ETH1* connector in the *sysConfigNetworkEthernetSpeed* variable
   - *ETH2* 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 4100 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 59 for more details.

2. Restart the Mediatrix 4100 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 4100 has the possibility to force the desired Ethernet link speed and duplex mode by disabling the auto-negotiation and selecting the proper setting (*sysConfigNetworkEthernetSpeed* 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.

CHAPTER 4

MGCP Protocol Features

This chapter describes how to set information exclusive to the Media Gateway Control Protocol (MGCP). It assumes that the Mediatrix 4100 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 4100 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 4100.

   After the unit restarts, it uses the selected protocol.

MGCP Information

The Mediatrix 4100 uses IETF RFC 3435 - Media Gateway Control Protocol (MGCP) Version 1.0. F. Andreasen, 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 4100), are the Slaves and only obey orders given by the Master.

The Mediatrix 4100 is used with any MGCP Call Agent (also known as Connection Manager), which manages calls from and to the Mediatrix 4100.

Services Provided

The Mediatrix 4100 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 4100 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 45 for more details.

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

Configuration Source

The Mediatrix 4100 must know the IP address or FQDN and port number of the Call Agent. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 for more details.

▶ **To use DHCP-assigned information:**

1. In the *ipAddressConfig* folder, locate the *mgcpCASelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).

   This variable defines whether the Mediatrix 4100 must ask for its Call Agent settings through a DHCP server or not.

2. Set the *mgcpCASelectConfigSource* 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 46: MGCP Call Agent DHCP Information

To use a...	Set...
vendor specific code	The *mgcpCADhcpSiteSpecificCode* 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 *mgcpCADhcpSiteSpecificCode* 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 *mgcpCADhcpSiteSpecificCode* variable in the unit's configuration).

   See "Vendor and Site Specific DHCP Options" on page 53 for more details.

4. Restart the Mediatrix 4100 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 *mgcpCASelectConfigSource* variable (under the *ipAddressConfigMgcpCallAgent* group).

   This variable defines whether the Mediatrix 4100 must ask for its Call Agent settings through a DHCP server or not.

2. Set the *mgcpCASelectConfigSource* variable to **static**.

3. Set the following variables:

Table 47: MGCP Call Agent Static Address

Variable	Description
mgcpCAStaticHost	Static MGCP Call Agent IP address or domain name. **Default Value**: 192.168.0.10
mgcpCAStaticPort	Static MGCP Call Agent IP port number. **Default Value**: 2727

4. Restart the Mediatrix 4100 so that the changes may take effect.

Establishing a MGCP Session

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

Figure 21: Layout Example

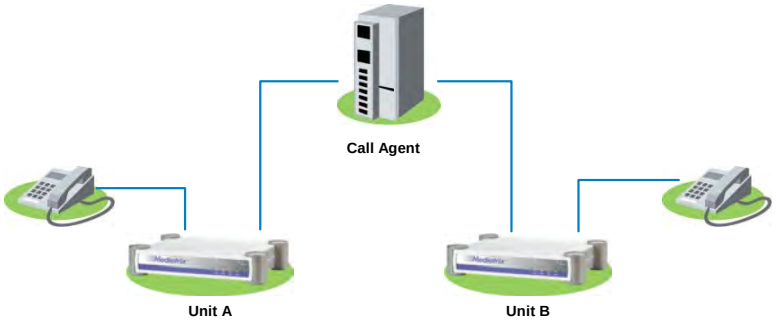
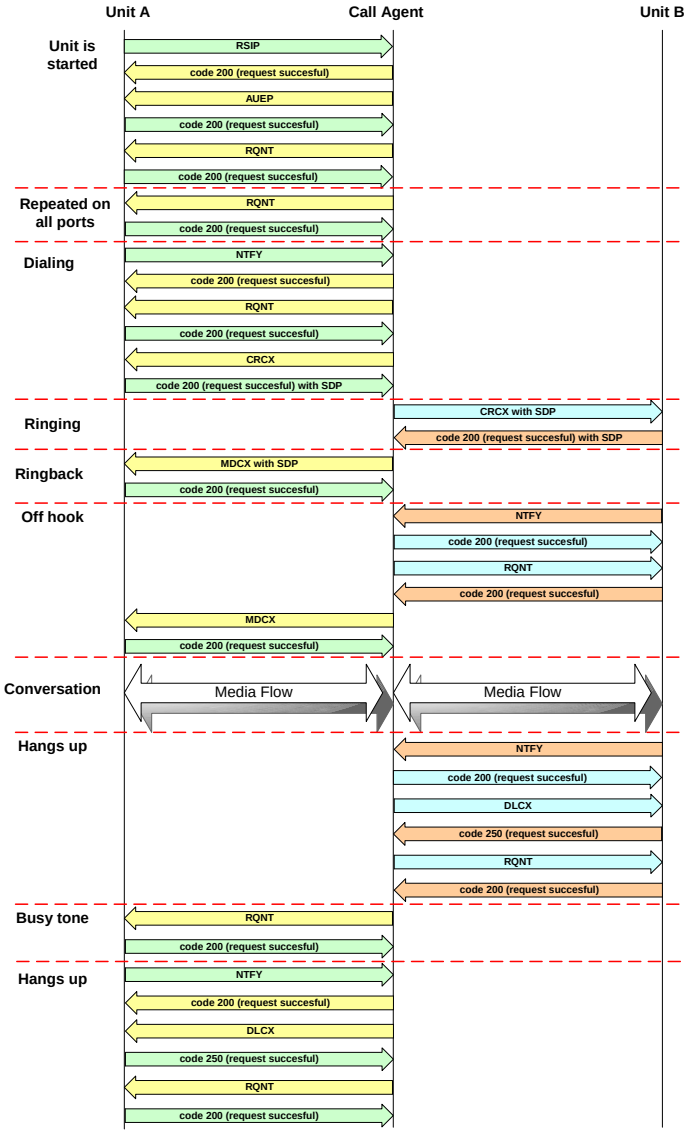


Figure 22: MGCP CAll Flow



MGCP Commands

The following commands are supported.

Table 48: 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 Mediatrix 4100. 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 Mediatrix 4100 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 49: 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 4100 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 50: 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 4100 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 51: 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. Period = (Period x 2) * (Random value (0 to 24) + 88) / 100 Period2 = (Initial period x 2) * (Random value (0 to 24) + 88) / 100 etc.

   The default value is **exponentialWithJitter**.

3. Set the following variables:

Table 52: 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 52: MGCP Retransmission Information (Continued)

Variable	Description
mgcpRetransmissionSuspicion ThresholdDnsQuery	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
mgcpRetransmissionDisconnect Threshold	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
mgcpRetransmissionDisconnect ThresholdDnsQuery	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
mgcpRetransmissionHistory Timeout	Number of milliseconds for which the responses to old transactions must be kept. **Default Value**: 20000
mgcpRetransmissionMaxWaiting Delay	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP (Restart in Progress). **Default Value**: 600000
mgcpRetransmissionDisconnect InitialWaiting Period	Initial waiting delay (in ms) an endpoint must wait before starting the disconnect procedure. **Default Value**: 15000
mgcpRetransmissionDisconnect MinWaitingPeriod	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
mgcpRetransmissionDisconnect MaxWaitingPeriod	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 4100 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 Mediatrix 4100.

▶ **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 Mediatrix 4100 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 Mediatrix 4100 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 207 for more details on country-specific ringback tones.

Table 53: 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 53: 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

3. Restart the Mediatrix 4100 so that the changes may take effect.

DTMF Package

The DTMF package groups variables pertaining to the DTMFs.

▶ **To set DTMF package information:**

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

Table 54: 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

3. Restart the Mediatrix 4100 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:**

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

Table 55: 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 55: MGCP Line Package Information (Continued)

Variable	Description
mgcpLinePackageDlDuration	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
mgcpLinePackageSlDuration	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 55: 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 Mediatrix 4100 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 Mediatrix 4100.

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 Mediatrix 4100 MIB structure.

Limitations to Using Line Reversal

Do not use the XL package in the following situations:

- When an endpoint of the Mediatrix 4100 rings
- When an endpoint of the Mediatrix 4100 uses caller ID
- When an endpoint of the Mediatrix 4100 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 Mediatrix 4100 so that the changes may take effect.

The X-P package offers the following tone definitions:

Table 56: 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 Mediatrix 4100 to indicate the charge display has to be incremented.

b. Initial ring is sent from the media gateway controller to the Mediatrix 4100.

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

Redirecting to a Different Call Agent

The Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 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 33 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 Mediatrix 4100 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 136 for more details.

The following is a call flow of a conference.

Figure 23: Conference Message Flow – Part 1

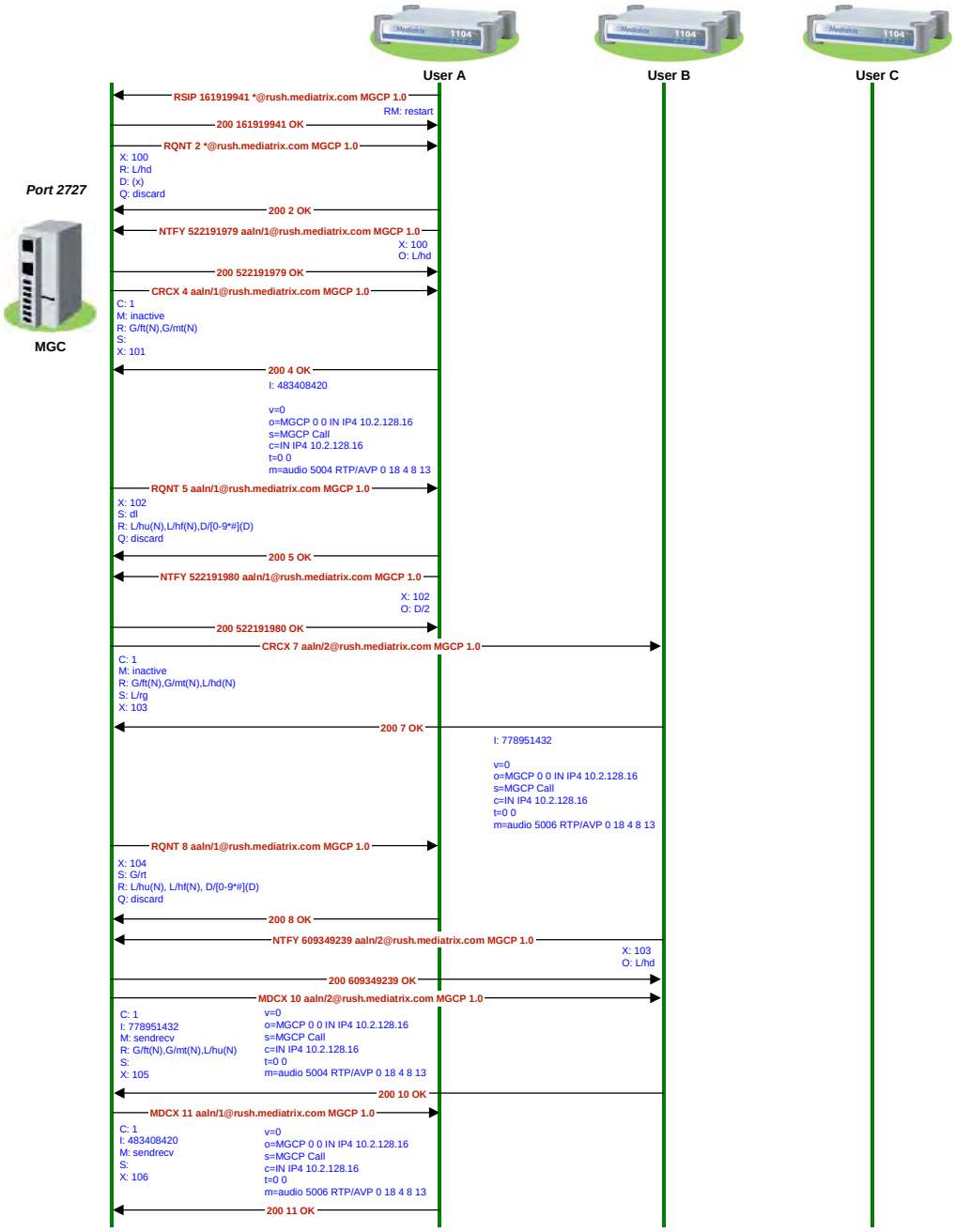


Figure 24: Conference Message Flow – Part 2

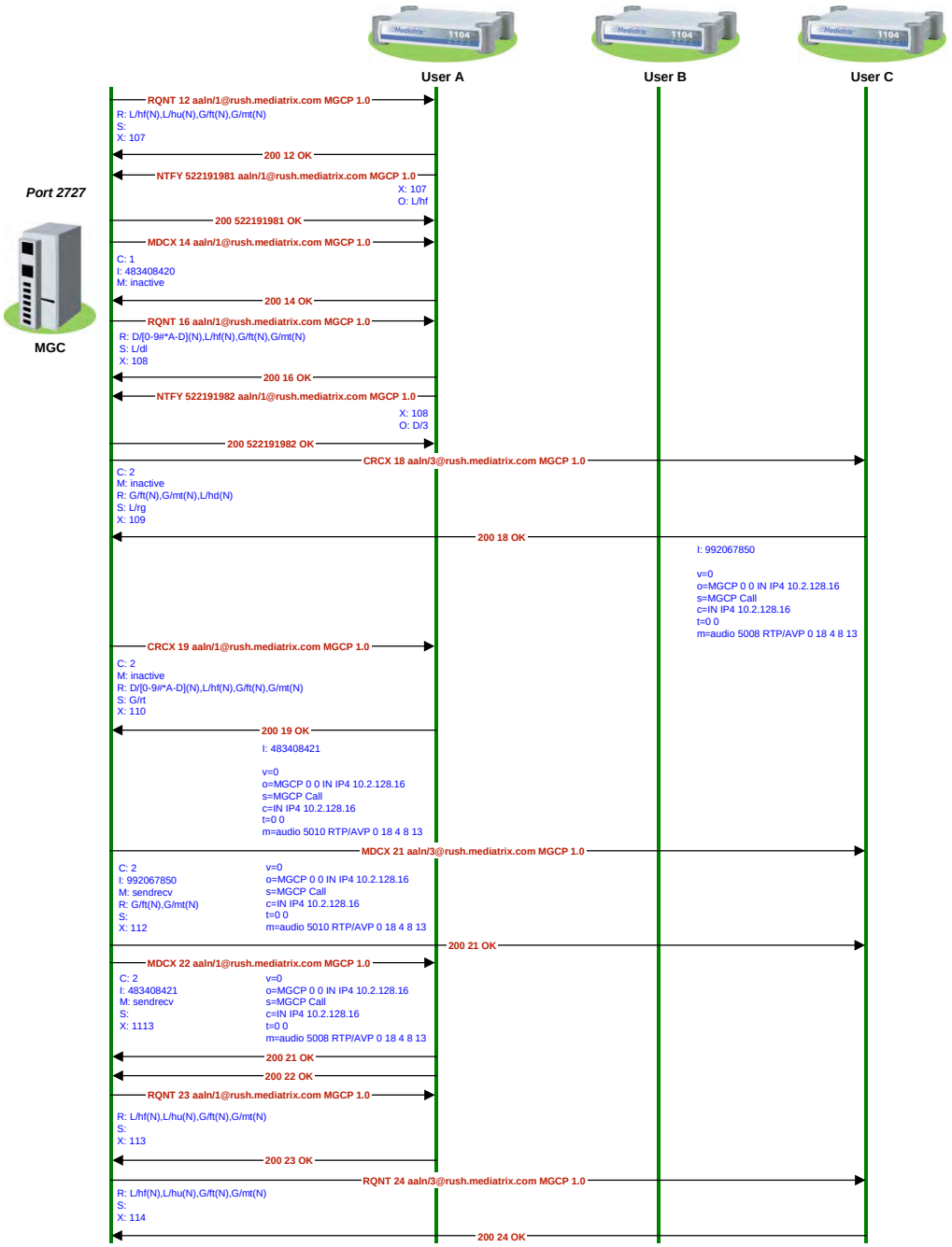
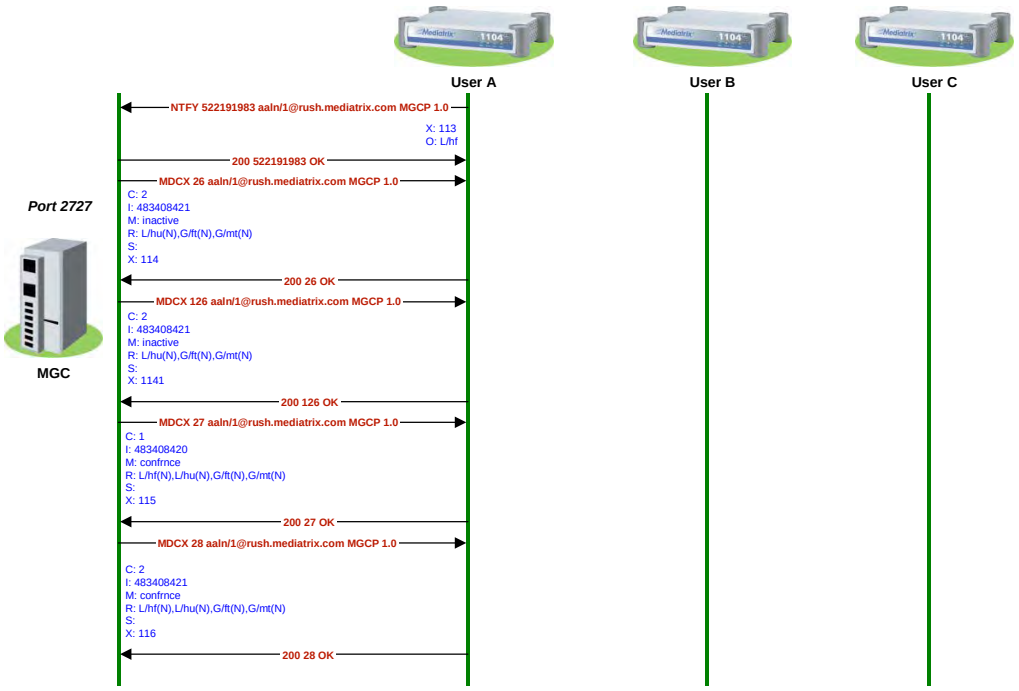


Figure 25: Conference Message Flow – Part 3



Firewall Traversal

The Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 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.

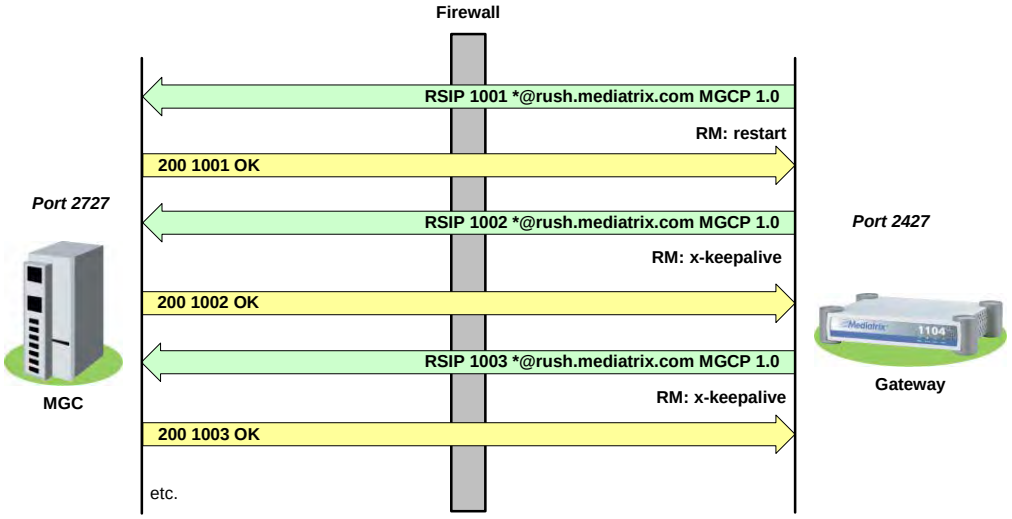
2. Set the *mgcpFwKeepAliveEnable* variable to **enable**.

   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.

Figure 26: Firewall Message Flow



Interoperability Configuration

The following sections describe a few interoperability parameters you can use to impove the way the Mediatrix 4100 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 4100 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 57: 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 Mediatrix 4100, 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 Mediatrix 4100 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 *mgcpncsExperimentalMIB*, set the *mgcpncsAnswerStreamFormat* variable to the proper value.

Table 58: 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 *mgcpncsExperimentalMIB*, set the *mgcpncsOriginLineSessionIDAndVersionMaxLength* variable to the proper value.

Table 59: 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 59: 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 4100 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 *mgcpncsExperimentalMIB*, set the *mgcpncsMultipleFaxToneDetection* variable to **enable**.

   The Mediatrix 4100 will report every occurrence of the fax tone event.

   If you set the variable to **disable**, when establishing a fax call, the Mediatrix 4100 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 *mgcpncsExperimentalMIB*, set the *mgcpncsConnectRtpSockets* 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 4100 uses unconnected sockets and the endpoints will play any RTP packets addressed to them.

2. Restart the Mediatrix 4100 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 checkum:**

1. In the *mgcpncsExperimentalMIB*, set the *mgcpncsRtpUdpChecksumEnable* 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 4100 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 4100 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 4100 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 60: Modem Tone Reporting Parameters

Parameter	Description
enable	The Mediatrix 4100 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 4100 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 61: 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 4100 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 62: 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 *mgcpncsUseItuT38Format* variable with the proper behaviour.

Table 63: 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 *mgcpncsExperimentalMIB*, set the *mgcpncsBracketsAroundIpAddressInDomainNameEnable* variable with the proper behaviour.

Table 64: 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 *mgcpncsExperimentalMIB*, set the *mgcpncsPolarityReversalOnCallingCardServiceToneEnable* variable with the proper behaviour.

Table 65: 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.

CHAPTER 5

NCS Protocol Features

This chapter describes how to set information exclusive to the Network-based Call Signalling (NCS) protocol. It assumes that the Mediatrix 4100 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 4100 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 4100.
   After the unit restarts, it uses the selected protocol.

NCS Information

The Mediatrix 4100 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 4100 is used with any NCS Call Agent (also known as Connection Manager), which manages calls from and to the Mediatrix 4100.

Services Provided

The Mediatrix 4100 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 4100 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 4100 inserted within angle brackets is used instead. See "FQDN Configuration Source" on page 45 for more details.

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

Configuration Source

The Mediatrix 4100 must know the IP address and port number of the Call Agent. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 for more details.

To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *ncsCASelectConfigSource* variable (under the *ipAddressConfigNcsCallAgent* group).

   This variable defines whether the Mediatrix 4100 shall ask for its Call Agent settings through a DHCP server or not.

2. Set the *ncsCASelectConfigSource* 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 66: NCS Call Agent DHCP Information

To use a...	Set...
vendor specific code	The *ncsCADhcpSiteSpecificCode* variable (under the *ipAddressConfigNcsCADhcp* 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 *ncsCADhcpSiteSpecificCode* variable (under the *ipAddressConfigNcsCADhcp* 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 *ncsCADhcpSiteSpecificCode* variable in the unit's configuration).

   See "Vendor and Site Specific DHCP Options" on page 53 for more details.

4. Restart the Mediatrix 4100 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 *ncsCASelectConfig Source* variable (under the *ipAddressConfigNcsCallAgent* group).

   This variable defines whether the Mediatrix 4100 shall ask for its Call Agent settings through a DHCP server or not.

2. Set the *ncsCASelectConfigSource* variable to **static**.

3. Set the following variables:

Table 67: 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 4100 so that the changes may take effect.

Basic Information

You can set general NCS information pertaining to the Mediatrix 4100. 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 4100 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 68: 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 68: 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 4100 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 69: 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 4100 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 70: 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. Period = (Period x 2) * (Random value (0 to 24) + 88) / 100 Period2 = (Initial period x 2) * (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 70: NCS Retransmission Information (Continued)

Variable	Description
ncsRetransmissionSuspicion ThresholdDnsQuery	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
ncsRetransmissionDisconnect Threshold	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
ncsRetransmissionDisconnect ThresholdDnsQuery	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
ncsRetransmissionHistory Timeout	Number of milliseconds for which the responses to old transactions shall be kept. **Default Value**: 20000
ncsRetransmissionMaxWaiting Delay	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP (Restart in Progress). **Default Value**: 600000
ncsRetransmissionDisconnect InitialWaitingPeriod	Initial waiting delay (in ms) an endpoint shall wait before starting the disconnect procedure. **Default Value**: 15000
ncsRetransmissionDisconnect MinWaitingPeriod	Disconnected minimum waiting delay (in ms) that shall have elapsed since the gateway became disconnected before entering the disconnect procedure. **Default Value**: 15000
ncsRetransmissionDisconnect MaxWaitingPeriod	Disconnected maximum waiting delay (in ms) since the gateway became disconnected that an endpoint can wait before starting the disconnect procedure. **Default Value**: 600000

3. Restart the Mediatrix 4100 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 71: NCS Line Package Information

Variable	Description
ncsLinePackageBzDuration	Busy tone timeout value in ms. It indicates the line or equipment is in use, engaged or occupied. **Default Value:** 30000
ncsLinePackageDlDuration	Dial tone timeout value in ms. It indicates the line is ready to receive dialing. **Default Value:** 16000
ncsLinePackageLDuration	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 4100 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
ncsLinePackageMwiDuration	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
ncsLinePackageOtDuration	Off hook warning tone timeout value in ms. It indicates that the telephone is not hung up correctly. **Default Value:** 65535000
ncsLinePackageRbkDuration	Ring back on connection tone timeout value in ms. It is the sound one hears when calling someone else's phone. **Default Value:** 180000
ncsLinePackageRgDuration	Ring tone timeout value in ms. It indicates the called line is ringing out. **Default Value:** 180000
ncsLinePackageRoDuration	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
ncsLinePackageRtDuration	Ring back tone timeout value in ms. **Default Value:** 180000

Table 71: NCS Line Package Information (Continued)

Variable	Description
ncsLinePackageSlDuration	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

3. Restart the Mediatrix 4100 so that the changes may take effect.

Encoding Name of the Payload Type 18

For NCS compatibility, the Mediatrix 4100 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 4100 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 33 for more details.

▶ **To set the encoding name of the RTP Payload Type 18:**

1. In the *ncsCompatibilityMIB*, under *mediatrixExperimental*, locate the *ncsCompatibilityMIBObjects* group.
2. 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
3. Restart the Mediatrix 4100 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 72: 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 *telephonyIpSignalingProtocolSelection* variable is set to **ncs** ("Introduction" on page 85).

Interoperability Configuration

Please refer to "Interoperability Configuration" on page 79 for a few interoperability parameters you can use to impove the way the Mediatrix 4100 interops with other products.

Note: The interoperability parameters apply to units that are either running the MGCP os NCS signalling protocol.

CHAPTER 6

Country-Specific Configuration

This chapter describes how to set the Mediatrix 4100 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.

DTMF Signalling

The data transmission using DTMF signalling is performed during or before ringing depending on the country settings or line configuration. The Mediatrix 4100 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.
- 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 4100 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 4100 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 4100 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 207 for more information on these country-specific settings.

In the *Unit Manager Network Administration Manual*, refer to chapter *Ports Parameters*, section *Port Configuration Window*.t

To set a country location:

1. In the *telephonyMIB,* locate the *telephonyCountrySelection* variable.

   This variable indicates the current country used by the Mediatrix 4100. 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	New Zealand
Austria 2	Australia 3	UAE 2 (United Arab Emirates)
France	Japan	
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 4100 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 73: Caller ID Mappings

Country	Caller ID	*telephonyCountrySelection* 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 95 for more details.

CHAPTER 7

Configuration File Download

The configuration file download feature allows to update the Mediatrix 4100 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 4100. The advantage of having the Mediatrix 4100 as the session initiator is to allow NAT traversal.

Configuration File Download Server

The service allows to download a unique file for each Mediatrix 4100, 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 4100 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 106 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 14 - SNTP Settings" on page 157 for more details on how to configure the Mediatrix 4100 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 4100 must know the IP address and port number of its configuration file server. This server contains the configuration file the Mediatrix 4100 will download. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 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 4100 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 74: Configuration File Server DHCP Information

To use a...	Set...
vendor specific code	The *configFileFetchingDhcpSiteSpecificCode* 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 *configFileFetchingDhcpSiteSpecificCode* 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 *configFileFetchingDhcpSiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 53 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 4100 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 75: Configuration File Server Static Information

Variable	Description
configFileFetchingStaticHost	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
configFileFetchingStaticPort	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 76: 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 4100 (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 4100 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 4100 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 4100 does not download the specific configuration file.

Configuration Update Status

If valid configuration files are successfully downloaded, then the Mediatrix 4100 automatically restarts to apply all the new settings. If the Mediatrix 4100 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 77: 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.

Configuration Files Encryption

You can secure the exchange of configuration files between the server and the Mediatrix 4100. A privacy key allows the unit to decrypt a previously encrypted configuration file. This applies to files downloaded via TFTPor HTTP.

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 4100 unit. Contact your sales representative for more details.

Configuration File Decryption on the Mediatrix 4100

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 78: Decryption Variables

Configuration File	Variable
Generic	configFilePrivacyGenericSecret

Table 78: Decryption Variables (Continued)

Configuration File	Variable
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 4100 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 99.
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.

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.

3. If not already done, set the configuration file path as described in "Setting up the Configuration File Download" on page 101.
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 Mediatrix 4100 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 Mediatrix 4100 immediately downloads the configuration files. It is the initiator of the TFTP sessions.

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 99.

> **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 99 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 101.
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 4100 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 4100 immediately downloads the configuration files. It is the initiator of the HTTP sessions.

Automatic Configuration Update

You can configure the Mediatrix 4100 to automatically update its configuration. This update can be done:

- Every time the Mediatrix 4100 restarts.
- At a specific time interval you can define.

Automatic Update on Restart

The Mediatrix 4100 may download new configuration files each time it restarts.

To set the automatic update every time the Mediatrix 4100 restarts:

1. Set the configuration file server host and port as defined in "Configuration File Server Settings" on page 99.

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 99 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 101.

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 4100 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 4100 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 4100 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 99.

> **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 99 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 101.

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 4100 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 79: Time Unit Parameters

Parameter	Description
minutes	Updates the unit's configuration every *x* minutes. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7).
hours	Updates the unit's configuration every *x* hours. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7).
days	Updates the unit's configuration every *x* days. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7). You can also define the time of day when to perform the update in the *configFileAutoUpdateTimeOfDay* 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 14 - SNTP Settings" on page 157 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 14 - SNTP Settings" on page 157 for more details on how to configure the Mediatrix 4100 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 4100 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 80: 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 80: 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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.

Table 80: 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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.
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 *sysAdminDownloadConfigFileStatus* to *fail*.

Management Server

You can set the Mediatrix 4100 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 15 - Management Server Configuration" on page 161.

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 4100 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 4100.

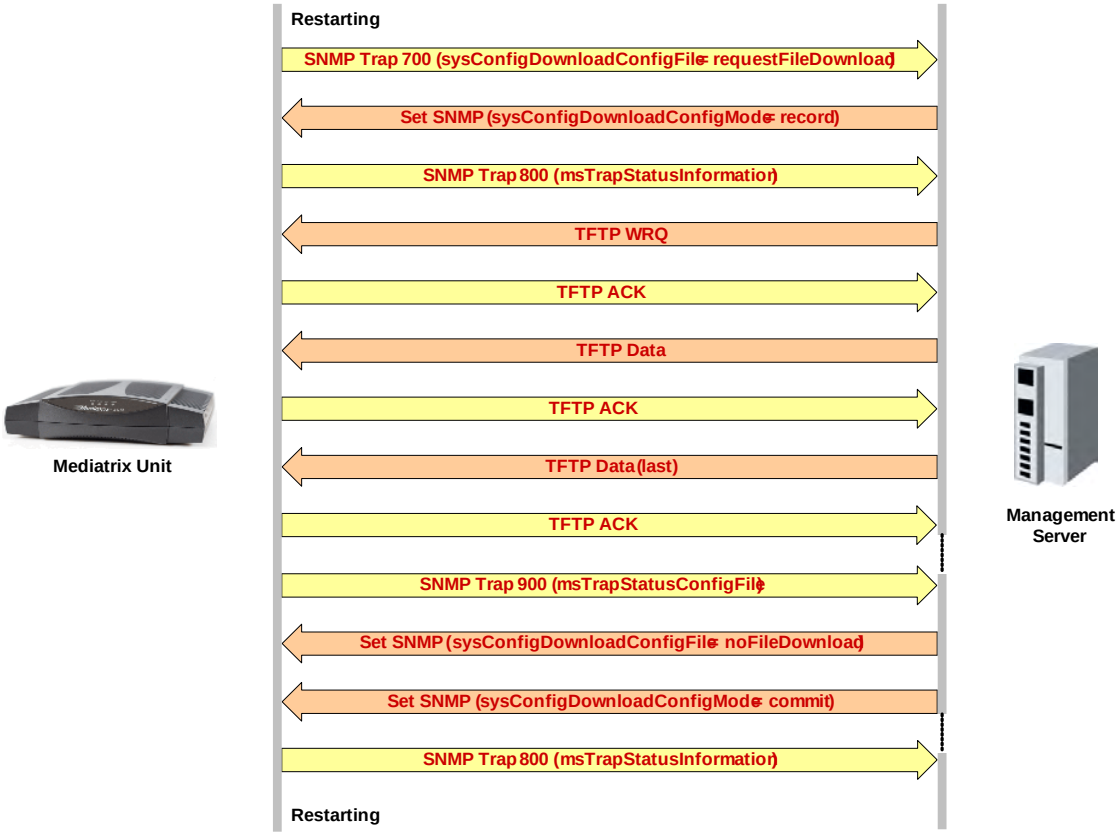
   c. Once the configuration file has been sent, the Unit Manager Network sets the *sysConfigDownloadConfigFile* variable to **noFileDownload**.

   d. The Unit Manager Network sets the *sysConfigDownloadConfigMode* variable to **commit**.

   If a valid configuration file is successfully downloaded, then the Mediatrix 4100 automatically restarts to apply all the new settings. If the Mediatrix 4100 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 27: 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 81: 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 81: 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 *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
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 *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
TFTP transfer aborted	The transfer was aborted while in progress by changing the value of *sysConfigDownload ConfigMode* or *sysConfigDownloadConfigFile*.	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 *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
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 82: Syslog Messages Using the Management Server

Level	Message	Event
Warning	`The notification “XXX” could not be sent to msHost “XXX” and msTrapPort 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.

CHAPTER 8

Software Download

This chapter describes how to download a software version available on the designated software server into the Mediatrix 4100.

You have the choice to perform the software download by using the TFTP or HTTP protocol. You can also configure the Mediatrix 4100 to automatically update its software version.

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 4100 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 4100 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 124 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 14 - SNTP Settings" on page 157 for more details on how to configure the Mediatrix 4100 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 4100 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 4100 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 4100 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 3 - IP Address and Network Configuration" on page 41 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 4100 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 83: Primary Image Server DHCP Information

To use a...	Set...
vendor specific code	The *imageDhcpPrimarySiteSpecificCode* 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 *imageDhcpPrimarySiteSpecificCode* 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 *imageDhcpPrimarySiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 53 for more details.

4. Set how you want to define the Secondary Image server information in the DHCP server.

Table 84: Secondary Image Server DHCP Information

To use a...	Set...
vendor specific code	The *imageDhcpSecondarySiteSpecificCode* variable to **0**. Set the Secondary image server IP address in the DHCP server inside the vendor specific sub-option 118 (hexadecimal 0x76).

Table 84: Secondary Image Server DHCP Information (Continued)

To use a...	Set...
site specific code	The *imageDhcpSecondarySiteSpecificCode* 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 *imageDhcpPrimarySiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 53 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 4100 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 85: 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 4100.

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 126 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 4100 to automatically update its software version.

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

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 4100 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 118 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 115 for more details.

The Mediatrix 4100 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 86: Image Location Parameters

Parameter	Description
static	Uses the directory specified in the *imageLocation* variable (see Step 2).
remoteFile	The image location is defined in a file called "mediatrix4108targetimage.inf" (the 4108 part may be changed to 4116 or 4124 depending on your product). The location of this file is defined in the *imageSelectionFileLocation* 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 4100. 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 “mediatrix4108targetimage.inf” under the server root path.

Note: If you leave the file empty, the Mediatrix 4100 will look for the software download information in the root directory of the image server.

   b. Configure the path of the “mediatrix4108targetimage.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 “mediatrix4108targetimage.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 87: 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 4100 (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 4100 sends:

Table 88: 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 88: 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.

LED States

When the Mediatrix 4100 initiates a software download, the LEDs located on the front panel indicate the status of the process.

Table 89: LED States in Software Download

Event	LED State
Image downloading and writing	*Power*, *LAN*, *In Use* and *Ready* LEDs blink alternately at 1 Hz with 1/4 ON duty cycle. **Warning**: Do not turn the Mediatrix 4100 off while in this state.
Image download failed	*Power*, *LAN*, *In Use* and *Ready* LEDs blink at the same time at 2 Hz with 50% ON duty cycle for 4 seconds.

See “LED Indicators” on page 14 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 115).
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 118.
4. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 116.
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 4100 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 4100 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 129.
8. Initiate the download by setting the *sysAdminCommand* variable (in the *sysAdminMIB*) to **downloadSoftware**.

   This starts the download process.

Caution: Never shutdown the Mediatrix 4100 manually while in the download process, because the image may be partially written and the Mediatrix 4100 is unable to restart.

The software download may take several minutes, depending on your Internet connection, network conditions and servers conditions.

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 115).
2. If not already done, configure the Image path as described in "Setting up the Image Path" on page 118.
3. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 116.

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 116 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 4100 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 4100 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 129.
7. Initiate the download by setting the *sysAdminCommand* variable (in the *sysAdminMIB*) to **downloadSoftware**.

   This starts the download process.

Caution: Never shutdown the Mediatrix 4100 manually while in the download process, because the image may be partially written and the Mediatrix 4100 is unable to restart.

   The software download may take several minutes, depending on your Internet connection, network conditions and servers conditions.

8. Update the MIB browser with the MIB version coming with the software version.

Automatic Software Update

You can configure the Mediatrix 4100 to automatically update its software version. This update can be done:

- Every time the Mediatrix 4100 restarts.
- At a specific time interval you can define.

Automatic Update on Restart

The Mediatrix 4100 may download a new software version each time it restarts.

To set the automatic update every time the Mediatrix 4100 restarts:

1. If not already done, setup the Image server used to download the software (see "Before Downloading" on page 115).
2. If not already done, configure the Image path as described in "Setting up the Image Path" on page 118.
3. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 116.

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 116 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. Set the *imageAutoUpdateOnRestartEnable* variable to **enable**.
7. Set the *imageAutoUpdateEnable* variable to **enable**.

   The automatic software update will be performed each time the Mediatrix 4100 restarts.

Automatic Update at a Specific Time Interval

You can configure the Mediatrix 4100 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 115).
2. If not already done, configure the Image path as described in "Setting up the Image Path" on page 118.

3. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 116.

> **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 116 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 90: Time Unit Parameters

Parameter	Description
minutes	Updates the software every *x* minutes. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7).
hours	Updates the software every *x* hours. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7).
days	Updates the software every *x* days. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7). You can also define the time of day when to perform the update in the *imageAutoUpdateTimeRange* 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 14 - SNTP Settings" on page 157 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 14 - SNTP Settings" on page 157 for more details on how to configure the Mediatrix 4100 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 4100 will perform the download five minutes after both ports are detected on-hook.

Software Downgrade

It is possible to downgrade a Mediatrix 4100 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 4100, 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 4100 with the current application.

   The Mediatrix 4100 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 118.

Emergency Software Procedure

If the software download is suddenly interrupted, it may not be complete. Without any protection against this situation, the Mediatrix 4100 is not functional.

A transfer may be interrupted for the following reasons:

- An electrical shortage.
- The user of the Mediatrix 4100 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 4100 tries to initiate the software download with the primary software server.
2. If the software download fails with the primary software server, the Mediatrix 4100 tries to initiate the software download with the secondary software server.

3. If the primary and the secondary servers cannot be reached, the Mediatrix 4100 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 4100 idles for one minute.

5. After this one minute, the Mediatrix 4100 tries to initiate the software download again.

6. If the software download fails again with the primary, secondary, and default software servers, the Mediatrix 4100 idles for two minutes before attempting to initiate the software download.

7. If the emergency software download still fails, the Mediatrix 4100 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.

CHAPTER 9

Line Configuration

This chapter describes the features available on the lines connected to the Mediatrix 4100.

For information on voice codecs, see "Chapter 10 - Voice Transmissions" on page 133.

For information on data codecs, see "Chapter 11 - Fax Transmission" on page 147.

Lines Administrative State

You can independently set the administrative state of each analog line of your Mediatrix 4100. This state determines how the Mediatrix 4100 processes calls.

For instance, you must properly unlock the analog lines of the Mediatrix 4100 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 4100 restarts.
- Permanent: When the Mediatrix 4100 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 4100 restarts. Once the unit restarts, it uses the permanent state defined for each line. See "Permanent Administrative State" on page 130 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 4100. This state is kept until the unit restarts. It offers the following settings:

Table 91: 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 Mediatrix 4100 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 Mediatrix 4100 restarts. It offers the following settings:

Table 92: 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 Mediatrix 4100 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 Mediatrix 4100 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 93: Flash Hook Parameters

Variable	Description
fxsFlashHookDetectionDelayMin	Minimum time in ms the hook switch must remain pressed to perform a flash hook. **Default Value**: 100
fxsFlashHookDetectionDelayMax	Maximum time in ms the hook switch can remain pressed to perform a flash hook. **Default Value**: 1200

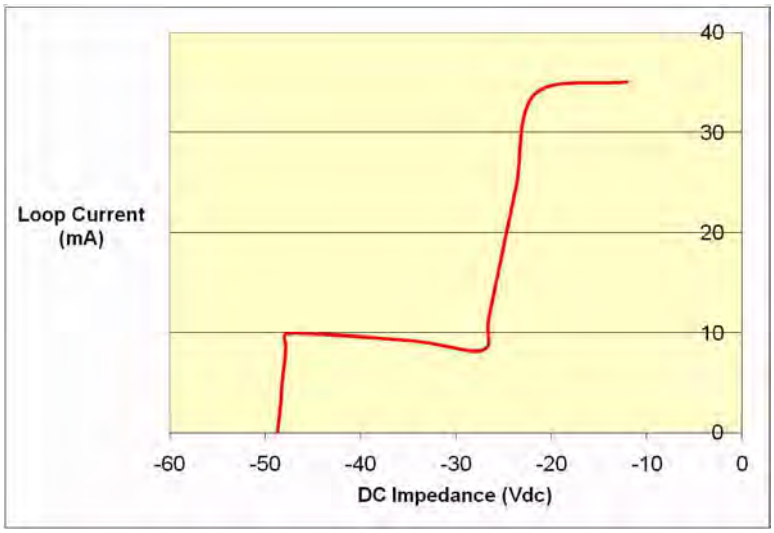
2. Restart the Mediatrix 4100 so that the changes may take effect.

Loop Current

When one of its analog lines goes off-hook, the Mediatrix 4100 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 28 for a loop current of 32 mA.

Figure 28: 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 4100.

2. If you want to set a different loop current value for one or more endpoints, set the following variables:
   - *fxsEpSpecificLoopCurrentOverrideEnable* variable for the specific endpoint you want to configure to **enable**.
   - *fxsEpSpecificLoopCurrentOverride* variable for the specific endpoint you want to configure with the proper loop current value.

3. Restart the Mediatrix 4100 so that the changes may take effect.

When a remote end-user goes on-hook, the Mediatrix 4100 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 4100 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.

CHAPTER 10

Voice Transmissions

This chapter describes the various codecs the Mediatrix 4100 supports for transmitting audio signals.

Codec Descriptions

The lines of the Mediatrix 4100 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 94: Codecs Comparison

	Compression	Voice Quality
G.711	None	Excellent
G.723.1	Highest	Good
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 95: G.711 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. See "Packetization Time" on page 137 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 143 for more details.
Comfort noise	Supports white and custom comfort noise as defined in *RFC 3389*. See "Comfort Noise" on page 145 for more details.

Analog Modem

The Mediatrix 4100 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 4100 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 96: 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 137 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 143 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 145 for more details.

Analog Modem

The Mediatrix 4100 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 Mediatrix 4100 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.723.1

Specified in ITU-T Recommendation G.723.1, dual-rate speech coder for multimedia communications transmitting at 5.3 kbit/s and 6.3 kbit/s. This Recommendation specifies a coded representation that can be used to compress the speech signal component of multi-media services at a very low bit rate. The audio is encoded in 30 ms frames.

A G.723.1 frame can be one of three sizes: 24 octets (6.3 kb/s frame), 20 octets (5.3 kb/s frame), or 4 octets. These 4-octet frames are called SID frames (Silence Insertion Descriptor) and are used to specify comfort noise parameters.

Table 97: G.723.1 Features

Feature	Description
Packetization time	Range of 30 ms to 120 ms with increment of 30 ms. See "Packetization Time" on page 137 for more details.
Voice Activity Detection (VAD)	The Mediatrix 4100 supports the annex A. Annex A is the built-in support of VAD in G.723.1.

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 Mediatrix 4100 supports G.729A and G.729AB for encoding and G.729, G.729A and G.729AB for decoding.

Table 98: G.729 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. See "Packetization Time" on page 137 for more details.
Voice Activity Detection (VAD)	The Mediatrix 4100 supports the annex B. Annex B is the built-in support of VAD in G.729. See "G.729 VAD" on page 144 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 *voiceIfMIB,* locate the *voiceIfCodecPreferred* variable (*voiceIfCodecTable*).
   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
   - g723
   - 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 *voiceIfMIB,* choose the codec you want to use (*voiceIfCodecTable*).

   You have the choice between the following codecs:

Table 99: Enabling Voice Codecs

Codec	Variable	Set to...
PCMU (G.711 u-Law)	voiceIfCodecPcmuEnable	enable
PCMA (G.711 a-Law)	voiceIfCodecPcmaEnable	enable
G.723.1	voiceIfCodecG723Enable	g723-53kbs g723-63kbs
G.726 at 16 kbps	voiceIfCodecG72616kbpsEnable	enable
G.726 at 24 kbps	voiceIfCodecG72624kbpsEnable	enable
G.726 at 32 kbps	voiceIfCodecG72632kbpsEnable	enable
G.726 at 40 kbps	voiceIfCodecG72640kbpsEnable	enable
G.729.A	voiceIfCodecG729Enable	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:
   - voiceIfCodecG72616kbpsPayloadType: The default value is 97.
   - voiceIfCodecG72624kbpsPayloadType: The default value is 98.
   - voiceIfCodecG72632kbpsPayloadType: The default value is 99.
   - voiceIfCodecG72640kbpsPayloadType: 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 *voiceIfDtmfTransport* variable to **outOfBandUsingSignalingProtocol** ("DTMF Transport Type" on page 139), 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 4100 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 *voiceIfMIB,* set the packetization time of the codec(s) as required (*voiceIfCodecTable*). Available values vary from one codec to another.

Table 100: Packetization Time Settings

Variable	Definition	Values (ms)
PCMU (G.711 u-Law)		
voiceIfCodecPcmuMinPTime	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 *voiceIfCodecPcmuMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecPcmuMaxPTime	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 *voiceIfCodecPcmuMinPTime* variable. **Default Value**: 100	10-100, with increments of 10
PCMA (G.711 a-Law)		
voiceIfCodecPcmaMinPTime	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 *voiceIfCodecPcmaMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecPcmaMaxPTime	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 *voiceIfCodecPcmaMinPTime* variable. **Default Value**: 100	10-100, with increments of 10
G.723		
voiceIfCodecG723MinPTime	Shortest packetization period allowed for the G.723 codec. Authorized values start at 30 ms and come in discrete steps of 30 ms up to the one specified by the *voiceIfCodecG723MaxPTime* variable. **Default Value**: 30	30, 60, 90, 120
voiceIfCodecG723MaxPTime	Longest packetization period allowed for the G.723 codec. Authorized values go up to 120 ms, in discrete steps of 30 ms, and start at the one specified by the *voiceIfCodecG723MinPTime* variable. **Default Value**: 120	30, 60, 90, 120

Table 100: Packetization Time Settings (Continued)

Variable	Definition	Values (ms)
G.726		
voiceIfCodecG72616kbpsMinPTime	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 *voiceIfCodecG72616kbpsMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG72616kbpsMaxPTime	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 *voiceIfCodecG72616kbpsMinPTime* variable. **Default Value**: 100	10-100, with increments of 10
voiceIfCodecG72624kbpsMinPTime	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 *voiceIfCodecG72624kbpsMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG72624kbpsMaxPTime	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 *voiceIfCodecG72624kbpsMinPTime* variable. **Default Value**: 100	10-100, with increments of 10
voiceIfCodecG72632kbpsMinPTime	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 *voiceIfCodecG72632kbpsMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG72632kbpsMaxPTime	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 *voiceIfCodecG72632kbpsMinPTime* variable. **Default Value**: 100	10-100, with increments of 10
voiceIfCodecG72640kbpsMinPTime	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 *voiceIfCodecG72640kbpsMaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG72640kbpsMaxPTime	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 *voiceIfCodecG72640kbpsMinPTime* variable. **Default Value**: 100	10-100, with increments of 10

Table 100: Packetization Time Settings (Continued)

Variable	Definition	Values (ms)
G.729		
voiceIfCodecG729MinPTime	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 *voiceIfCodecG729MaxPTime* variable. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG729MaxPTime	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 *voiceIfCodecG729MinPTime* vartiable. **Default Value**: 100	10-100, with increments of 10

2. Restart the Mediatrix 4100 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 *voiceIfMIB,* set the DTMF transport type in the *voiceIfDtmfTransport* variable (*voiceIfDtmfTransportTable* group).

   The following choices are available:

Table 101: DTMF Transport Type Parameters

Transport Parameter	Description
inBand	The DTMFs are transmitted like the voice in the RTP stream.
outOfBandUsingRtp	The DTMFs are transmitted as per RFC 2833 (see "DTMF Payload Type" on page 140 for additional information).

DTMF out-of-band

Certain compression codecs such as G.723.1 and G.729 effectively distort voice because they lose information from the incoming voice stream during the compression and decompression phases. For normal speech this is insignificant and becomes unimportant. In the case of pure tones (such as DTMF) this distortion means the receiver may no longer recognize the tones. The solution is to send this information as a separate packet to the other endpoint, which then plays the DTMF sequence back by re-generating the true tones. Such a mechanism is known as out-of-band DTMF. The Mediatrix 4100 receives and sends out-of-band DTMFs as per ITU Q.24. DTMFs supported are 0-9, A-D, *, #.

Table 101: 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.

2. Restart the Mediatrix 4100 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 139 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:**

1. In the *voiceIfMIB*, set the DTMF transport type in the *voiceIfDtmfTransport* variable (*voiceIfDtmfTransportTable* group) to **outOfBandUsingRtp**.
2. Set the payload type in the *voiceIfDtmfPayloadType* variable.

   Available values range from 96 to 127.

DTMF Detection

The default DTMF detection parameters of the Mediatrix 4100 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.

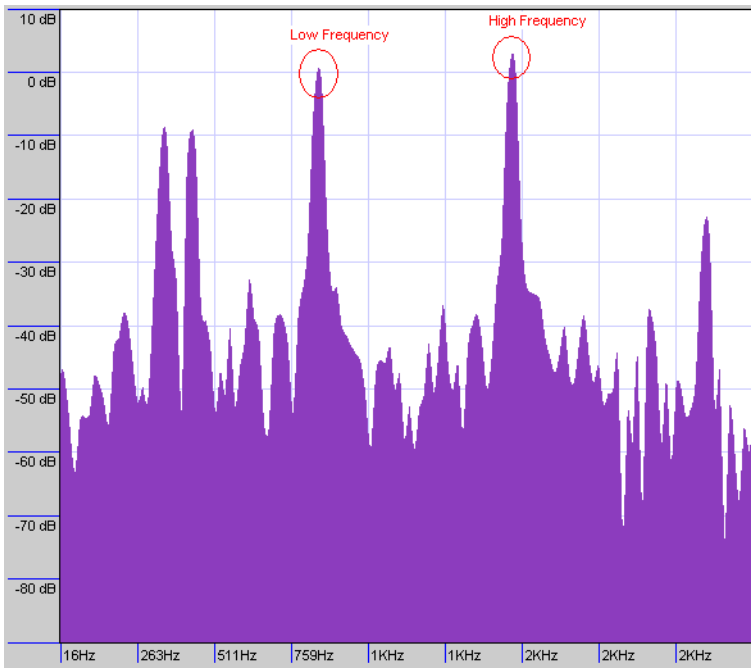
Table 102: DTMF Keypad Frequencies

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 29: DTMF Detection Example



To detect this DTMF, the DSP relies on several parameters. The following table lists the default values that the Mediatrix 4100 uses. You can override any one of these values.

Table 103: 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 *voiceIfMIB*, set the maximum absolute power threshold (dBm0) for the low and high frequencies in a DTMF in the *voiceIfDtmfDetectionUnitMaxPowerThreshold* 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 *voiceIfDtmfDetectionUnitMinPowerThreshold* 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 *voiceIfDtmfDetectionUnitBreakPowerThreshold* 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 *voiceIfDtmfDetectionUnitPositiveTwist* 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 *voiceIfDtmfDetectionUnitNegativeTwist* 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 *voiceIfDtmfDetectionRiseTimeCriteria* variable.

Table 104: 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 4100 is connected suffers from a high level of congestion, the jitter buffer protection level should be higher. If the network to which the Mediatrix 4100 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 *voiceIfTargetJitterBufferLength* and *voiceIfMaxJitterBufferLength* variables.

▶ **To set Jitter Buffer variables:**

1. In the *voiceIfMIB*, locate the *voiceIfTable* group.

2. Define the jitter buffer length in the *voiceIfTargetJitterBufferLength* 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 143 for more details.

3. Define the maximum jitter buffer length in the *voiceIfMaxJitterBufferLength* 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 + 4x20 = 110 ms

   See "About Changing Jitter Buffer Values" on page 143 for more details.

4. Restart the Mediatrix 4100 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 4100 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.

Note: You cannot disable the G.723 VAD.

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 *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the sensitivity of the VAD algorithm to silence periods in the *voiceIfG711VoiceActivityDetectionEnable* variable.

   The following settings are available:

Table 105: 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 Mediatrix 4100 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 *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the *voiceIfG729VoiceActivityDetectionEnable* variable.

   The following settings are available:

Table 106: G.729 VAD Settings

Setting	Description
disable	G.729 uses annex A only. The Mediatrix 4100 does not send G.729 Annex B comfort noise frames.
enable	G.729 annex A is used with annex B. The Mediatrix 4100 sends G.729 Annex B comfort noise frames during silence periods.

See “Enabling Individual Codecs” on page 136 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 *mgcpncsExperimentalMIB*, set the *mgcpncsG729AnnexBNegotiation* variable to the proper value.

   The following values are available:

Table 107: 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 *voiceIfG729VoiceActivityDetectionEnable*. 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 *voiceIfG729VoiceActivityDetectionEnable* 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 *voiceIfG729VoiceActivityDetectionEnable*. 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 4100 processes silence periods information it receives.

Note: Comfort noise only applies to the G.711 and G.726 codecs. G.723 and G.729 CNG is not configurable because it is part of the codec.

During silence periods, the Mediatrix 4100 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 *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the type of comfort noise in the *voiceIfG711ComfortNoiseGenerationEnable* variable.
   The following settings are available:

Table 108: 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 4100 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 4100.

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 4100 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 *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the following variables:
   - *voiceIfUserInputGainOffset*: User input gain offset in dB (from analog to digital).
   - *voiceIfUserOutputGainOffset*: 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 4100 so that the changes may take effect.

CHAPTER 11

Fax Transmission

This chapter describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 4100.

Introduction

The Mediatrix 4100 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.

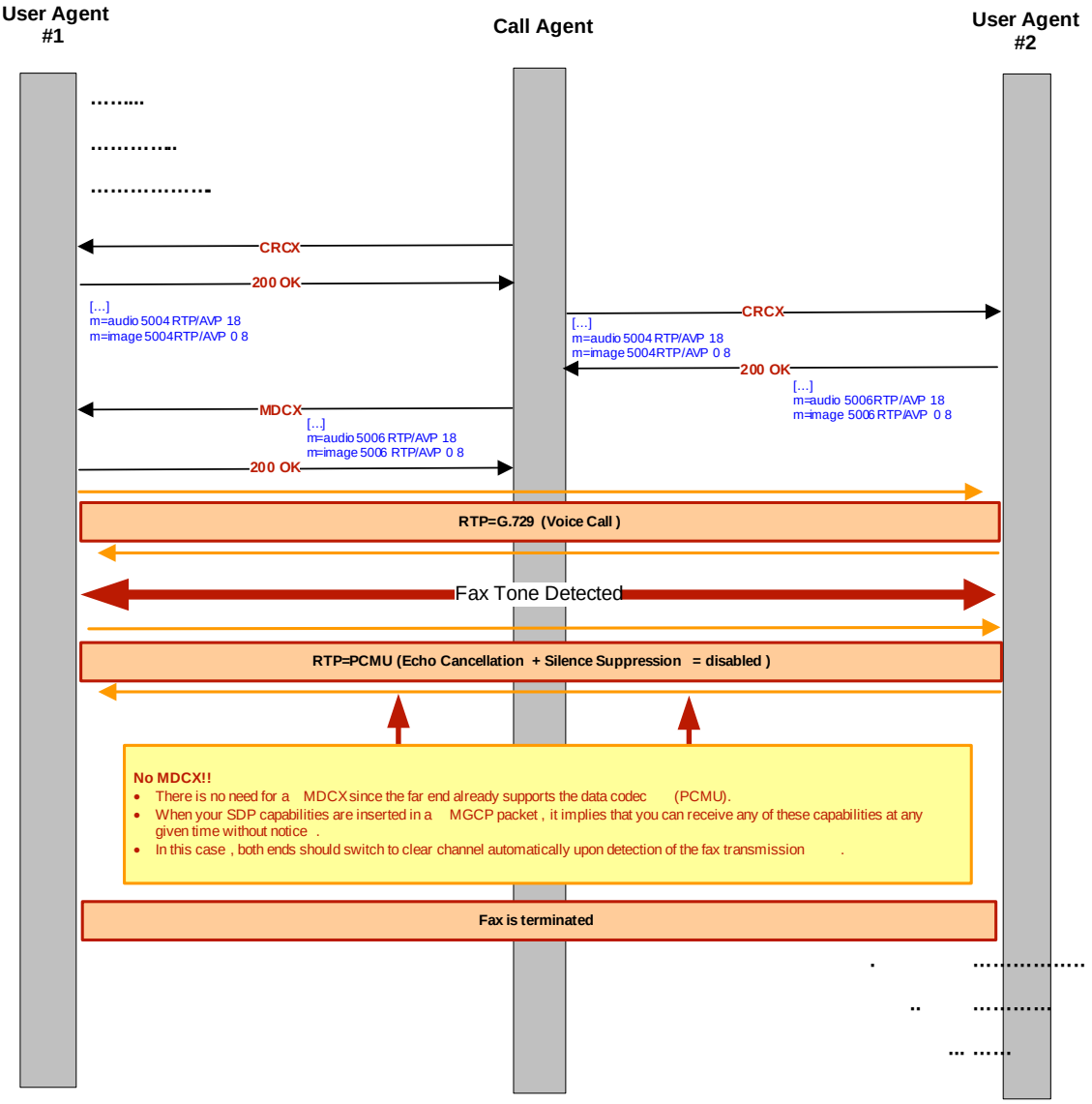
The quality of T.38 fax transmissions depends upon the system configuration, type of call control system used, type of Mediatrix units deployed, as well as the model of fax machines used. Should some of these conditions be unsatisfactory, performance of T.38 fax transmissions may vary and be reduced below expectations.

All lines of the Mediatrix 4100 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 4100 can send faxes in clear channel. The following is a clear channel fax call flow:

Figure 30: 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 109: 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 109: 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 *dataIfCodecT38Enable* variable to **disable**.
2. Set the clear channel codec to use upon detecting a fax tone in the *dataIfClearChannelCodecPreferred* 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 135. Otherwise, the Mediatrix 4100 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 4100 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 *voiceIfCodecPreferred* variable (see "Preferred Codec" on page 135).

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

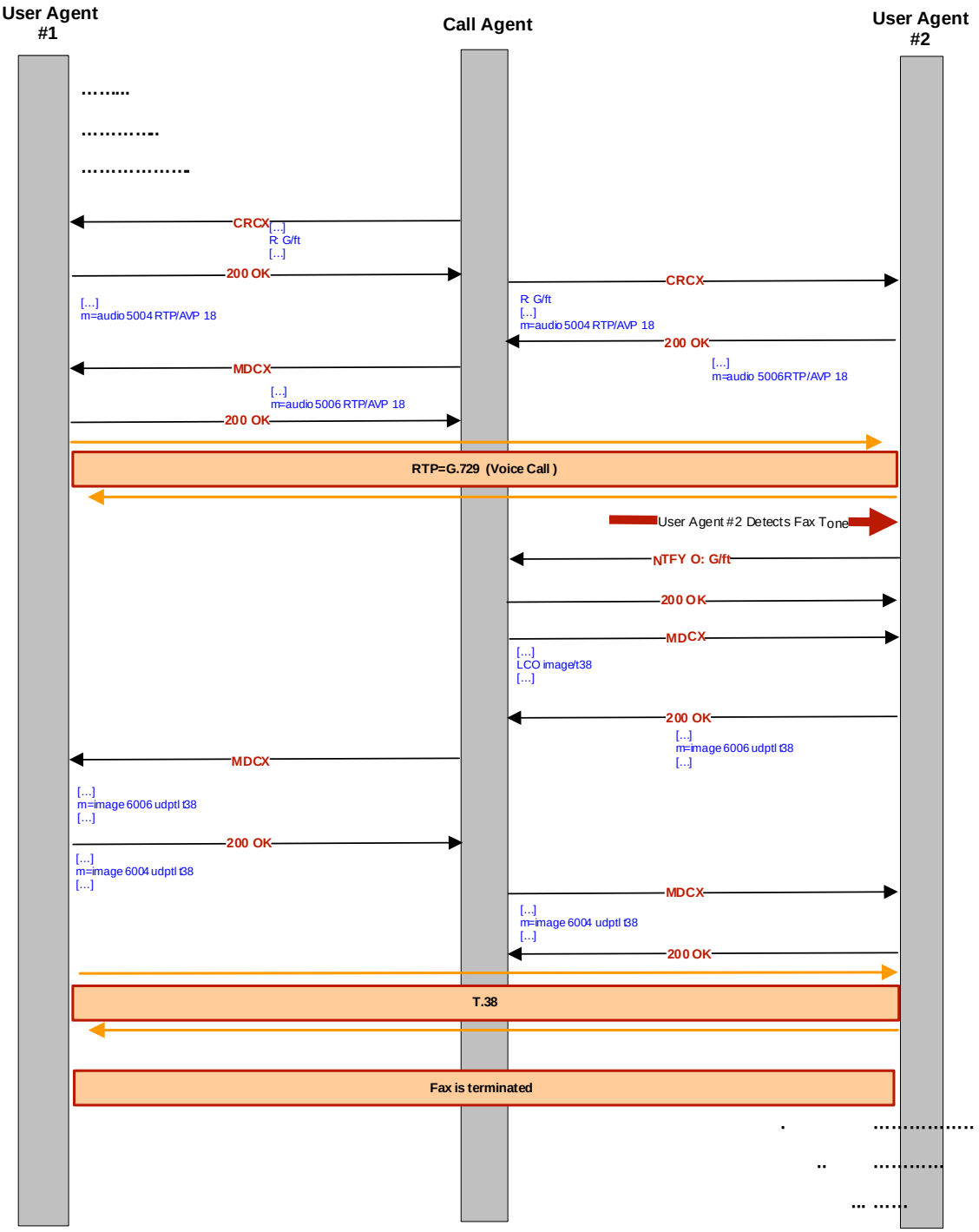
T.38 fax relay is a real-time fax transmission; that is, two fax machines communicating with each other as if there were a direct phone line between the two. T.38 is called a fax relay, which means that instead of sending inband fax signals, which implies a loss of signal quality, it sends those fax signals out-of-band in a T.38 payload, so that the remote end can reproduce the signal locally.

The Mediatrix 4100 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 31: T.38 Fax Call Flow



▶ **To set T.38 fax transmission:**

1. Enable T.38 by setting the *dataIfCodecT38Enable* variable to **enable**.

   If you select the *signalingProtocolDependent* option of the *voiceIfDtmfTransport* variable ("DTMF Transport Type" on page 139), 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 *dataIfCodecT38ProtectionLevel* 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 4100 so that the changes may take effect.

T.38 No-Signal

You can set the Mediatrix 4100 to send no-signal packets during a T.38 fax transmission. The Mediatrix 4100 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 *dataIfT38NoSignalTimeout* 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 *dataIfT38NoSignalEnable* variable to **enable**.

CHAPTER 12

Bypass Configuration

The Mediatrix 4100 may have an optional RJ-11 connector used to connect to a standard SCN line, called *Bypass*. It allows its users to maintain telephone services in the event of a power outage or network failure.

Bypass Connector Settings

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

- When power is removed from the Mediatrix 4100.
- When the IP network is down.

If one of these conditions is met, a phone/fax used on FXS connector 1 (Mediatrix 4108/4116) or analog line 1 (Mediatrix 4124) is directly connected to the SCN Bypass line. FXS connector 1 (Mediatrix 4108/4116) or analog line 1 (Mediatrix 4124) stays in Bypass connection until:

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

Standard Bypass

The following describes how to enable/disable the standard Bypass feature.

To enable the standard Bypass feature:

1. In the *fxsMIB*, locate the *fxsByPassEnable* variable.

   This option enables/disables the bypass service.

Table 110: Bypass Values

Value	Description
disable	The line with the bypass service is never redirected on the bypass line except when there is a power failure.
enable	When the line with the bypass service is unusable (*ifAdminUsageState* is idle-unusable), it is redirected to the bypass line. When this line becomes usable again (*ifAdminUsageState* is idle), the redirection is stopped within 10 seconds if the bypass line is unused or 10 seconds after the termination of the call.

Note: The control of the bypass service is only possible when the unit is powered on. When power is off, the bypass service is always enabled.

The default value is **enable**.

CHAPTER 13

STUN Configuration

This chapter describes how to configure the STUN client of the Mediatrix 4100.

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 4100 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 4100 does not currently support NAT type discovery.
- The Mediatrix 4100 does not currently support STUN NAT binding time to live discovery.
- The Mediatrix 4100 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 Mediatrix 4100 STUN client via SNMP.

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 Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 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 78 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 Mediatrix 4100 so that the changes may take effect.

CHAPTER 14

SNTP Settings

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix 4100. 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 4100 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 111: 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 4100 must know the IP address and port number of the SNTP server. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 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 4100 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 51 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 4100 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 112: 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 4100 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 4100 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:

   `STDOFFSET[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.

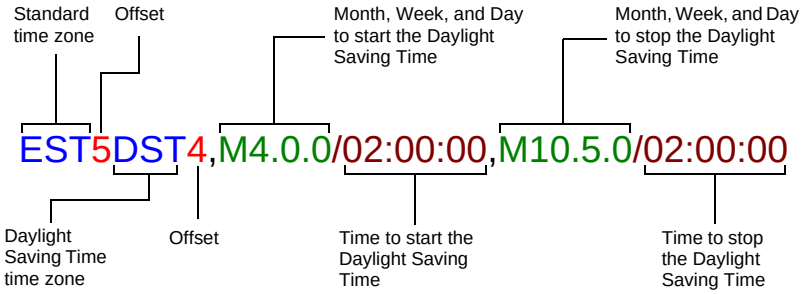
`M10.1.6`

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 113: 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

CHAPTER 15

Management Server Configuration

The Management Server is a generic name for a module or software that is used to remotely set up Mediatrix 4100 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 4100 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 4100.

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 4100 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 4100 must know the IP address and port number of the Management Server. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 for more details.

▶ **To use DHCP-assigned information:**

1. In the *ipAddressConfig* folder, locate the *msSelectConfig Source* variable.

   This variable defines whether the Mediatrix 4100 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 114: Management Server DHCP Information

To use a...	Set...
vendor specific code	The *msDhcpSiteSpecificCode* 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 *msDhcpSiteSpecificCode* 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 *msDhcpSiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 53 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 4100 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 115: 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.

CHAPTER 16

Quality of Service (QoS)

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. The Mediatrix 4100 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 4100 supports the Real Time Control Protocol (RTCP), which is used to send packets to convey feedback on quality of data delivery.

The Mediatrix 4100 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 4100 with standard and correct values.

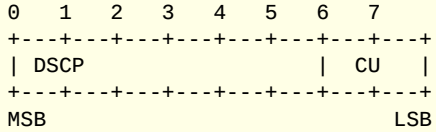
▶ **To enable the DS field configuration:**

1. In the *qosDiffServ* group of the *qosMIB*, locate the following variables:
   - qosSignalingDiffServ
   - qosVoiceDiffServ
   - qosT38FaxDiffServ

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.

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 Mediatrix 4100. 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 Mediatrix 4100 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 Mediatrix 4100 with standard and correct values.

To enable the IEEE 802.1q user priority configuration:

1. In the *qosIeee8021q* 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 *qosIeee8021q* 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.
5. Restart the Mediatrix 4100 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:

1. In the *qosVlanIeee8021q* group of the *qosMIB*, locate the *qosVlanIeee8021qTaggingEnable* variable.
2. Set the value of this parameter to **enable**.

   The VLAN configuration is enabled.
3. Locate the following variables:
   - qosVlanIeee8021qVirtualLanID
   - qosVlanIeee8021qDefaultUserPriority

   You can also use the priorities set in "IEEE 802.1q" on page 164 Step 3 without putting the Mediatrix 4100 in a VLAN. To do so, you must set the *qosVlanIeee8021qTaggingEnable* variable to **enable** and the *qosVlanIeee8021qVirtualLanID* 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.
4. Set the value of these variables.
5. Restart the Mediatrix 4100 so that the changes may take effect.

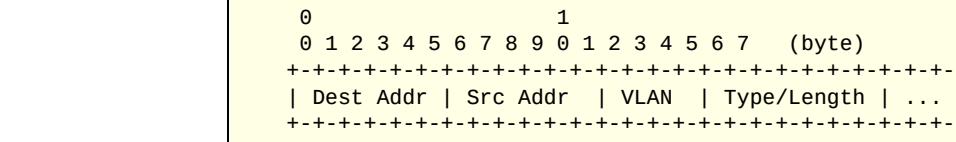
For more information, please refer to the *MIB Reference* manual.

VLANs

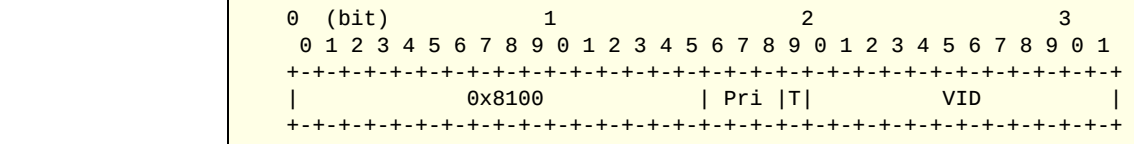
VLANs are created with standard Layer 2 Ethernet. A VLAN Identifier (VID) is associated with each VLAN. VLANs offer the following benefits:

- 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:



The VLAN field is separated as follows:



For both signalling and media packets, the VLAN priority section is configurable independently.

CHAPTER 17

Syslog Daemon

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 4100 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 4100, 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 116: 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 4100 must know the IP address and port number of the Syslog server. You can assign these information to the Mediatrix 4100 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 3 - IP Address and Network Configuration" on page 41 for more details.

▶ **To use DHCP-assigned information:**

1. In the *ipAddressConfig* folder, locate the *syslogSelectConfig Source* variable.

   This variable defines whether the Mediatrix 4100 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 117: Syslog DHCP Information

To use a...	Set...
vendor specific code	The *syslogDhcpSiteSpecificCode* variable (under the *ipAddressConfigSyslogDhcp* 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 *syslogDhcpSiteSpecificCode* variable (under the *ipAddressConfigSyslogDhcp* 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 *syslogDhcpSiteSpecific Code* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 53 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 4100 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 118: Syslog Daemon Static Address

Variable	Description
syslogStaticHost	Syslog server static IP address or domain name. **Default Value**: 192.168.0.10
syslogStaticPort	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 4100 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 4100 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 4100 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 119: Timestamp Format Parameters

Parameter	Description
trueRfcFormat	The timestamp complies with the RFC 3164 format. The timestamp in true RFC 3164 format is *Jan 1 09:05:06*.
pseudoRfcFormat	The timestamp uses a pseudo-RFC 3164 format. The timestamp in pseudo-RFC 3164 format is *Jan 1 9:5:6*.

   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 4100 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.

CHAPTER 18

Statistics

The Mediatrix 4100 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 4100:

- 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 120: 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 121: Statistics Setting Example

Statistics	5-minutes sections					
	1	2	3	4	5	6
rtpStatsCurrentTotalOctetsTransmitted	50	30	60	40	100	50
rtpStatsCumulatedTotalOctetsTransmitted	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.

CHAPTER 19

Maximum Transmission Unit (MTU)

This chapter describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 4100.

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 4100 MTU

The Mediatrix 4100 MTU is 1500 bytes, which is the Ethernet typical value.

Possible Hardware Problem

The implementation of the IEEE Standard 802.1q in the Mediatrix 4100 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 4100 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.

CHAPTER 20

Troubleshooting

You can experience some problems when connecting the Mediatrix 4100 to the network. The following section examines some of these problems and possible solutions.

A Syslog message lists the problems the Mediatrix 4100 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 4100 power socket.

DESCRIPTION: There is a long delay when starting the Mediatrix 4100.

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 4100 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 4100 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 43 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:

- Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 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 Mediatrix 4100 for the new setting to take effect. See "Ethernet Connection Speed" on page 59 for more details.

DESCRIPTION: Setting the MIB variable *voiceIfAdaptativeJitterBufferEnable* to **disable** has no effect.

POSSIBLE CAUSE: You cannot disable the adaptative jitter buffer on the Mediatrix 4100.

SOLUTION: If you set the *voiceIfTargetJitterBufferLength* and *voiceIfMaxJitterBufferLength* variables to the same value, you will have a non-adaptative jitter buffer. See "Adaptative Jitter Buffer" on page 142 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 4100 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 4100 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: 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.
- *LAN* LED lit.

POSSIBLE CAUSE: Network communication is not working.

SOLUTION: Check that:

- The LAN cable is securely connected to the Mediatrix 4100 and to the network connector.
- You did not connect a crossover network cable.

POSSIBLE CAUSE: Configurable parameters of the Mediatrix 4100 are not set properly.

SOLUTION: Refer to this manual for a complete description of the configurable Mediatrix 4100 parameters.

DESCRIPTION: Unable to establish a call from the Mediatrix 4100 to an endpoint such as an IP phone, a gateway or another access device.

POSSIBLE CAUSE: When the Mediatrix 4100 – 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 4100. See "T.38 Fax" on page 149 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 *voiceIfG711VoiceActivity DetectionEnable* MIB variable to have the same setting as the Call Agent.

b. Restart the unit.

See "Voice Activity Detection" on page 143 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 4100 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 146 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 4100 suffers from a limitation of its DSP. The Mediatrix 4100 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 4100 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 4100 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 4100 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 118 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 4100 attempts to transfer the software upgrade.

POSSIBLE CAUSE: The Ethernet cable has become disconnected from the Mediatrix 4100 or the PC running the file transfer.

SOLUTION: Reconnect the cable and start again.

POSSIBLE CAUSE: Power to the Mediatrix 4100 has been disrupted during the file transfer.

SOLUTION: Check the power connection to the Mediatrix 4100 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 4100 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 4100 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 43 for more details.

SNMP Management Software Issues

The following are issues you may encounter when trying to contact the Mediatrix 4100 with a SNMP management software.

DESCRIPTION: The SNMP network management software cannot access the Mediatrix 4100.

POSSIBLE CAUSE: The SNMP network management software does not have the proper Mediatrix 4100 information.

SOLUTION: Check that:

- The IP information for the Mediatrix 4100 is correctly configured.
- The Mediatrix 4100 was restarted after defining the IP information.
- The line through which you are trying to access the Mediatrix 4100 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 4100 IP address. If impossible, perform a recovery reset as indicated in section "Reset / Default Switch" on page 18.

DESCRIPTION: There is no response when trying to access the Mediatrix 4100.

POSSIBLE CAUSE: The Mediatrix 4100 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 4100.

DESCRIPTION: When trying to set a variable, the Mediatrix 4100 does no respond, nor sends an error message.

POSSIBLE CAUSE: In secure management mode, the Mediatrix 4100 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 4100 returns a "Wrong value" error message.

POSSIBLE CAUSE: The Mediatrix 4100 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 4100 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 4100 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 4100.

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 4100 is in secure mode management?

POSSIBLE CAUSE: In secure management mode, the Mediatrix 4100 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 4100 with read-write permission.

Appendices

Page Left Intentionally Blank

APPENDIX

A

Standards Compliance and Safety Information

This Appendix lists the various standards compliance of the Mediatrix 4100.

Standards Supported

The Mediatrix 4100 complies to the following standards:

Table 122: Standards Compliance

Category	Specification
Agency approvals	• European Union, CE mark (Declaration of Conformity) • Anatel • CSA • FCC
Safety standards	• UL60950-1 1st Edition • CAN/CSA-C22.2 No. 60950-1-03 • IEC 60950 (1st Edition 2001 With all national deviations) • Anatel Resolution 238:2000
Emissions	• FCC Part 15:1998 Class B • EN55022 (2006) Class B • EN61000-3-2 (2000) Harmonic current emissions • EN61000-3-3 (1995) Voltage fluctuations and flicker (with amendment A1) • Resolution 442: 2006
Immunity	EN55024:1998 including the following (with amendments A1): • 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
Telecom	• FCC Part 68:Subpart D • Industry Canada CS-03, issue 9, Part I, November 15, 2004

Note: The standards compliance of the Mediatrix 4100 are printed on a sticker located on the bottom of the unit.

Disclaimers

The following are the disclaimers related to the Mediatrix 4100.

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.

Federal Communications Commission (FCC) Part 68

This equipment complies with Part 68 of the FCC Rules. On the underside of this equipment is a label that contains, among other information, the FCC Registration Number, Ringer Equivalence Number (REN) and USOC jack type for this equipment. You must, upon request, provide this information to your telephone company.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN's of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your telephone company to determine the maximum REN for your calling area. If your telephone equipment causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact Media5 for information on how to obtain service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company.

Connection to party lines is subject to state tariffs.

INSTALLATION

This device is equipped with an USOC RJ-11C connector.

Industry Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Note: The Ringer Equivalence Number (REN) for this terminal equipment is 0.0. The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Number of all the devices does not exceed 5.

Note: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved 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 4100 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 overtreat 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 vare 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 (15A) Warning
- TN Power Warning
- Product Disposal Warning
- No. 26 AWG Warning
- LAN and FXS Ports Connectors Warning
- Socket Outlet Warning

Circuit Breaker (15A) 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, 15A 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.

LAN anf 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.

APPENDIX B

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 4100 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 4100 can be integrated with existing telephone, fax and data equipment such as PCs and routers.

Table 123: Industry Standard Protocols

Parameter	Description
Vocoders	• G.711 (a-law, u-law) • G.723.1a • 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 3164
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

- 1 x RJ-21X TELCO 25 pairs connector, analog phone/fax (FXS) interface (Mediatrix 4124).
- 8 x RJ-11 connectors, analog phone/fax (FXS) interface (Mediatrix 4108).
- 16 x RJ-11 connectors, analog phone/fax (FXS) interface (Mediatrix 4116).
- 1 x RJ-11 connector, PSTN bypass.
- 2 x RJ-45 connectors, 10/100 BaseT Ethernet access (autosense: up to 100 Mbits).

Power

- AC: Standard power cord receptacle (IEC 320 – C14) for universal AC input internal SMPS.
- Seamless switch over period if the client UPS detects a power loss and activates within 8 ms.

Casing / Installation

- Casing: Desktop (Plastic ABS UL94 5V).
- Installation: rack-mountable, 1U size.

Product Architecture Details

- Supports up to 24 (depending on model) concurrent communications using any vocoders.
- DSP-based DTMF detection, generation and synthesis.
- DSP-based echo cancellation (G.168).
- 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 124: Fax Technical Specifications

Parameter	Description
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)

- RJ21X connector (Mediatrix 4124)
- RJ-11 connectors (Mediatrix 4108 and Mediatrix 4116)
- Direct connection to a fax machine or telephone (Internal installation and internal cabling) (Mediatrix 4108 and Mediatrix 4116)
- DC feeding of the access line protected for over voltage
- Loop current detection and hook flash detection capable
- Generation of Selective Ring

Table 125: Analog Line Interface

Parameter	Description
Trunk Type	Loop Start: capable of Wink and Immediate signalization
Ring Source	45 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 3 ringer equivalents (3 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 126: DTMF Tone Detection

Parameter	Description
16-Digit DTMF Decoding	0 to 9, *, #, A, B, C, D
Permitted Amplitude Tilt	High frequency can be +4 dB to -8 dB relative to low frequency
Dynamic Range	-25 dBm to 0 dBm per tone
Frequency Accept	± 1.5% of nominal frequencies
Minimum Tone Duration	40 ms, can be increased with software configuration

Table 126: DTMF Tone Detection (Continued)

Parameter	Description
Interdigit Timing	Detects like digits with a 40 ms interdigit delay

DTMF Tone Generation

Table 127: DTMF Tone Generation

Parameter	Description
Per Frequency Nominal	-8 dBm to -5 dBm
Frequency Deviation	Within 1.5% of nominal values

MTBF Value

The Mean Time Before Failure (MTBF) value of the Mediatrix 4100 is 180,000 (Mediatrix 4124), 190,000 (Mediatrix 4116), and 200,000 (Mediatrix 4108) hours at 25 degrees Celsius ambient temperature. It has been defined using RelCalc v5.0, Bellcore method (LimitedStress - Method I, Case 3), Desktop unit.

Power Consumption

Measurements at the DC input

Table 128: Power Consumption at the DC Input

Parameter	Description
Idle Mode: 120Vac	0.54A 43W
Idle Mode: 240Vac	0.36A 43W
24 Extensions Off-Hook (worst case): 120Vac	0.58A 66W
24 Extensions Off-Hook (worst case): 240Vac	0.5A 66W

Operating Environment

Table 129: Operating Environment

Parameter	Description
Operating Temperature	0°C to 40°C
Humidity	Up to 85 %, non-condensing
Storage	-20°C to +70°C

Dimensions and Weight

Table 130: Dimensions and Weight

Parameter	Description
Height	4.4 cm (1.74 in.) approx.
Width	43 cm (17.19 in.) approx.
Depth	21 cm (8.4 in.) approx.
Weight	1.7 kg (3.7 lbs)

Warranty

All Media5 products carry Media5's standard three-year hardware and software warranty. An extended warranty is available.

APPENDIX C

Cabling Considerations

This Appendix describes the pin-to-pin connections for cables used with the Mediatrix 4100.

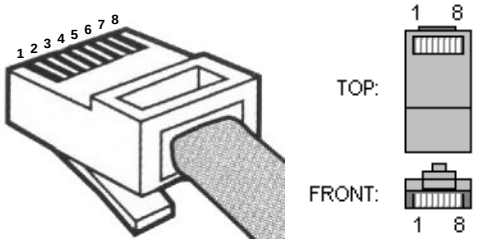
Warning: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

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 32: RJ-45 Cable



Straight Through Cable

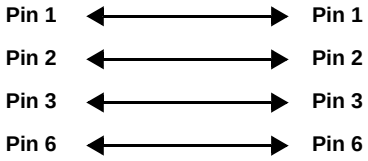
A RJ-45 straight through cable is used to connect a computer to a network device. For example straight through cables are the type of cables that connect a computer to a network hub, network switch, and network routers.

Table 131: 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 33: Straight Through Connectivity



Pin Name And Function

The following is the meaning of each pin in a RJ-45 cable.

Table 132: 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	

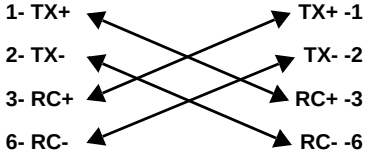
Crossover Cable

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 34: Crossover Connectivity



RJ21X Connector (Mediatrix 4124)

The Mediatrix 4100 uses the RJ21X, or “Amphenol-type”, connector as network interface with the Key Service Unit (KSU) or PBX Main Distribution Frame. The Mediatrix 4100 can thus be used in a variety of situations:

- It can be directly connected to a PBX via analog lines. These analog lines would be wired in a RJ21X cable.
- The PBX may have some analog lines connected to the SCN, while other lines could be connected to the IP network via the Mediatrix 4100.

See “Placing a Call” on page 4 for a few examples of Mediatrix 4100 use.

Creating a RJ21X Cable

The Mediatrix 4100 can use from 1 to 24 single or multiple-pair circuits bridged to the network or other connected equipment. These circuits are usually wired in a RJ21X cable and then plugged into the RJ21X connector of the Mediatrix 4100.

To meet the Class B EMI requirements, a shielded cable and connector shall be used. The shield shall be an overall aluminium foil and be connected to the connector shield.

Note: Installation of the analog lines via a RJ21X cable shall be done by a qualified technician.

The cable may be directly connected to the PBX or cross-connected via a Bix termination and cross-connect system. In fact, depending on the technician involved, the scenarios may vary.

RJ21X Pinout

Pins 1 (ring) and 26 (tip) of the ribbon connector are considered position 1. Pins 2 (ring) and 27 (tip) are position 2. This pairing continues through 24 pairs.

Table 133: RJ21X Pinout

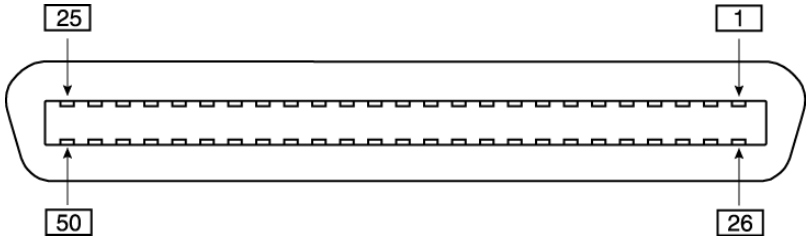
Line	Ring	Tip
1 (with Bypass)	pin1	pin26
2	pin2	pin27
3	pin3	pin28
4	pin4	pin29
5	pin5	pin30
6	pin6	pin31
7	pin7	pin32
8	pin8	pin33
9	pin9	pin34
10	pin10	pin35
11	pin11	pin36
12	pin12	pin37
13	pin13	pin38
14	pin14	pin39
15	pin15	pin40
16	pin16	pin41

Table 133: RJ21X Pinout (Continued)

Line	Ring	Tip
17	pin17	pin42
18	pin18	pin43
19	pin19	pin44
20	pin20	pin45
21	pin21	pin46
22	pin22	pin47
23	pin23	pin48
24	pin24	pin49

Note: Pins 25 and 50 are unused.

Figure 35: Front View of the RJ21X Receptacle – Pinout



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 36: RJ-11 Connector Pin Numbers

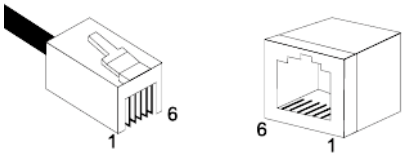


Table 134: RJ-11 Pinout Information

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.

Loop Current vs Cable Length

When installing the Mediatrix 4100, be sure that the cable length is not too long for the loop current. Considering the following operating parameters:

- Standard analog devices such as telephones or faxes with typically 300 Ohms of DC impedance.
- Cable with 85 Ohms/Km (AWG26)
- 0 dBm signal at interface

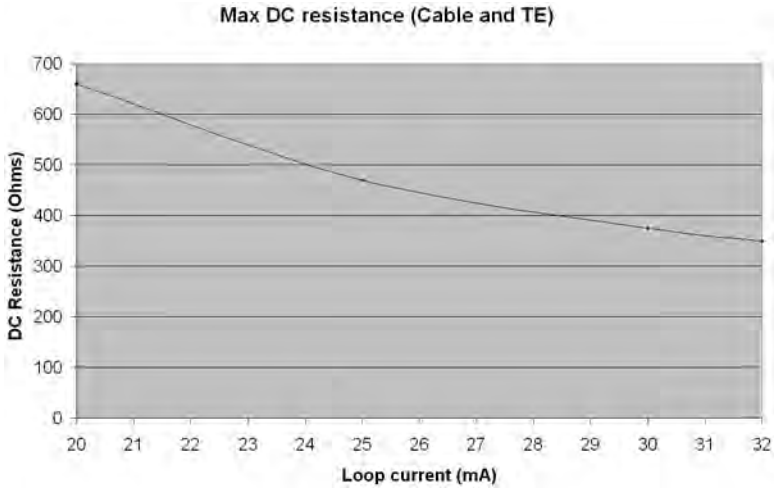
Observe the following values:

Table 135: Max DC Resistance

Loop Current in mA	Maximum Cable Length in Meters	Rdc Max in Ohms
20	2100	660
25	1000	470
30	450	375
32	300	350

Rdc max includes both equipment (standard analog telephones or faxes) and cable DC resistance. This is illustrated in Figure 37 on page 206.

Figure 37: Max DC Resistance



APPENDIX D

Country-Specific Parameters

The following parameters differ depending on the country in which you are.

Definitions

The following are some useful definitions.

Table 136: 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 dialled an unassigned code, or the digits dialled got messed up along the way.
Call Waiting Tone	Indicates someone is trying to call.
Alernative 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 4100.

Table 137: 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
Alernative 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 4100 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 138: 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
Alernative 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 139: 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
Alernative 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 140: 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
Alernative 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 141: 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
Alernative 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 142: 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
Alernative 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 143: 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
Alernative 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 144: 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
Alernative 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 145: 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
Alernative 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 146: 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
Alernative 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 147: 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
Alernative 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 148: 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
Alernative 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 149: 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
Alernative 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 150: 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
Alernative 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 151: 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
Alernative 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 152: 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
Alernative 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 153: 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
Alernative 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		
Tbrl-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 154: 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
Alernative 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		
Tbrl-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 155: 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
Alernative 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 156: 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
Alernative 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 157: 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
Alernative 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 158: 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
Alernative 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 159: 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
Alernative 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 160: 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
Alernative 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 161: 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
Alernative 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

APPENDIX E

Glossary

10 BaseT

An Ethernet local area network that works on twisted pair wiring.

100 BaseT

A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

Access Device

Device capable of sending or receiving data over a data communications channel.

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*.

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 162: 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 163: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.
Z	Geographical (regional) zone of the number (in France, there are five zones). It has two digits.
ABPQ	First four digits corresponding to a local zone defined by central offices.
12 34	Unique number to reach a specific destination.

In this context, the area code corresponds to the *Z* portion of the numbering plan. Because virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an area code for the location of your communication unit.

Call Agent (Connection Manager)

Manages the connection state of the Mediatrix 4100. 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.723.1

A codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

G.726

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.

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.

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 allocation 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 IIETF that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

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.

Ring

One of the two wires (the two are Tip and Ring) needed to set up a telephone connection. See *Tip*.

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.

Tip

The first wire in a pair of telephones wire. The second wire is called the “ring” wire. The tip is the conductor in a telephone pair cable which is usually connected to the positive side of a battery at the telephone company’s central office. It is the telephone industry’s equivalent of Ground in a normal electrical circuit. See also *Ring*.

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.

APPENDIX F

List of Acronyms

ADSI	Analog Display Services Interface
AWG	American Wire Gauge
CE	Cummunauté européenne (French)
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
DTMF	Dual Tone Multi-Frequency
FCC	Federal Communications Commission (USA)
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
GMT	Greenwich Mean Time
Hz	Hertz
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
KSU	Key Service Unit
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
PBX	Private Branch eXchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
REN	Ringer Equivalence Number
RSIP	Restart in Progress
RTCP	Real Time Control Protocol
SCN	Switched Circuit Network

SDP	Session Description Protocol
SMI	Structure of Management Information
SMPS	Switching Mode Power Supply
STUN	Simple Traversal of User Datagram Protocol (UDP) through Network Address Translation (NAT)
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
VAC	Volts Alternating Current
VAD	Voice Activity Detection
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	eXtensible Markup Language

APPENDIX G

List of MIB Parameters

C

checkTcpIpStackForSuccessfulBoot 21
configFileAutoUpdateOnRestartEnable 106
configFileAutoUpdatePeriod 107
configFileAutoUpdatePeriodicEnable 108
configFileAutoUpdateTimeRange 107
configFileAutoUpdateTimeUnit 107
configFileFetchingConfigSource 19
configFileFetchingDhcpSiteSpecificCode 48, 100
configFileFetchingFileLocation 101
configFileFetchingFileName 101
configFileFetchingHost 48, 100
configFileFetchingPort 49, 100
configFileFetchingSelectConfigSource 48, 100
configFileFetchingSpecificFileName 102
configFileFetchingStaticHost 49, 100
configFileFetchingStaticPort 49, 100
configFilePrivacyEnable 104
configFilePrivacyGenericSecret 103
configFilePrivacySpecificSecret 104
configFileTransferPassword 105, 106, 107
configFileTransferProtocol 105, 106, 107
configFileTransferUsername 105, 106, 107

D

dataIfClearChannelCodecPreferred 149
dataIfCodecMediaTypeImageEnable 148
dataIfCodecT38Enable 149, 151
dataIfCodecT38ProtectionLevel 151
dataIfT38NoSignalEnable 151
dataIfT38NoSignalTimeout 151

F

fxsByPassEnable 153
fxsEpSpecificLoopCurrentOverride 131
fxsEpSpecificLoopCurrentOverrideEnable 131
fxsFlashHookDetectionDelayMax 130
fxsFlashHookDetectionDelayMin 130
fxsLoopCurrent 131
fxsMeterPauseDuration 75
fxsMeterPulseDuration 75
fxsMeterPulseFreq 75

G

groupAdminState 105, 122, 123
groupReset 21
groupSetAdmin 21, 105, 122, 123

I

IfAdminInitialAdminState 130

ifAdminSetAdmin 129
imageAutoUpdateEnable 124, 126
imageAutoUpdateOnRestartEnable 124
imageAutoUpdatePeriod 125
imageAutoUpdateTimeRange 125
imageAutoUpdateTimeUnit 125
imageConfigSource 19
imageDhcpPrimarySiteSpecificCode 47, 116
imageDhcpSecondarySiteSpecificCode 47, 116
imageLocation 118, 119
imageLocationProvisionSource 118
imagePrimaryHost 19, 47, 116
imagePrimaryPort 19, 47, 116
imageSecondaryHost 19, 47, 116
imageSecondaryPort 19, 47, 116
imageSelectConfigSource 47, 116
imageSelectionFileLocation 118, 119
imageStaticPrimaryHost 117
imageStaticPrimaryPort 117
imageStaticSecondaryHost 117
imageStaticSecondaryPort 117
imageTransferPassword 123, 124, 125
imageTransferProtocol 122, 123, 124, 125
imageTransferUsername 123, 124, 125

L

lanStaticAddress 52
lanStaticNetworkMask 52
localHostAddress 19, 43, 44
localHostConfigSource 19
localHostDefaultRouter 19, 43
localHostDhcpServer 43
localHostDnsOverrideEnable 47
localHostFqdn 45
localHostFqdnConfigSource 45
localHostFqdnSelectConfigSource 45
localHostPrimaryDns 19, 43
localHostSecondaryDns 19, 43
localHostSelectConfigSource 43
LocalHostSnmpPort 46
localHostSnmpPort 19, 46
localHostStaticFqdn 45
localHostStaticPrimaryDns 45
localHostStaticSecondaryDns 45
localHostStaticSnmpPort 46
localHostStaticWanAddress 44
localHostSubnetMask 19, 43
LocalHostWanAddress 44
localHostWanAddressSelectConfigSource 44

M

mgcpAddPtimeIfPresentInLCO 66
mgcpCADhcpSiteSpecificCode 50, 62
mgcpCAHost 50, 62
mgcpCAPort 50, 62
mgcpCASelectConfigSource 50, 62
mgcpCAStaticHost 63
mgcpCAStaticPort 63
mgcpDefaultDigitMap 66

mgcpDefaultPackage 70
mgcpDtmfPackageLDuration 71
mgcpDtmfPackageTCriticalDuration 71
mgcpDtmfPackageTPartialDuration 71
mgcpEndpointIdListIncludeNotStarted 66
mgcpEndpointIdTerm1 67
mgcpEndpointIdTerm2 67
mgcpFwKeepAliveEnable 78
mgcpFwKeepAliveTimeout 78
mgcpGenericMediaPackageRbkDuration 71
mgcpGenericMediaPackageRtDuration 70
mgcpLinePackageBzDuration 71
mgcpLinePackageDlDuration 72
mgcpLinePackageHdPersistent 72
mgcpLinePackageHfPersistent 73
mgcpLinePackageHuPersistent 73
mgcpLinePackageMwiDuration 72
mgcpLinePackageOsiDuration 72
mgcpLinePackageOtDuration 72
mgcpLinePackageRgDuration 72
mgcpLinePackageRoDuration 72
mgcpLinePackageSlDuration 72
mgcpLinePackageWtDuration 72
mgcpncsAnswerStreamFormat 80
mgcpncsBracketsAroundIpAddressInDomainNameEnable 84
mgcpncsConnectRtpSockets 81
mgcpncsFakeRfc3407Recognition 83
mgcpncsG729AnnexBNegotiation 145
mgcpncsImmediateModemToneReporting 82
mgcpncsMakeOsiSignalBrief 82
mgcpncsMultipleFaxToneDetection 81
mgcpncsOriginLineSessionIDAndVersionMaxLength 80
mgcpncsPolarityReversalOnCallingCardServiceToneEnable 84
mgcpncsRtpUdpChecksumEnable 81
mgcpncsT38CapabilitiesUsingAudioCodec98 82
mgcpncsUseItuT38Format 83
mgcpncsValidateOfferAnswerModel 79
mgcpPiggyBackingEnable 66
mgcpPort 66
mgcpRestartLevel 66
mgcpRetransmissionAlgorithm 68
mgcpRetransmissionDisconnectInitialWaitingPeriod 69
mgcpRetransmissionDisconnectMaxWaitingPeriod 69
mgcpRetransmissionDisconnectMinWaitingPeriod 69
mgcpRetransmissionDisconnectThreshold 69
mgcpRetransmissionDisconnectThresholdDnsQuery 69
mgcpRetransmissionDisconnectTimeout 68
mgcpRetransmissionHistoryTimeout 69
mgcpRetransmissionInitialPeriod 68
mgcpRetransmissionMaxPeriod 68
mgcpRetransmissionMaxWaitingDelay 69
mgcpRetransmissionSuspicionThreshold 68
mgcpRetransmissionSuspicionThresholdDnsQuery 69
mgcpXPPackageIrDuration 74
msConfigSource 19
msDhcpSiteSpecificCode 48, 162
msEnable 161
msHost 19, 48, 161
msSelectConfigSource 48, 161
msStaticHost 48, 162

msStaticPort 48
msStaticTrapPort 48, 162
msTrapConfigInformation 111
msTrapPort 19, 48, 161
msTrapRetransmissionPeriod 161
msTrapRetransmissionRetryCount 161
mxDebugPcmCaptureEnable 179
mxDebugPcmCaptureEndpointNumber 179
mxDebugPcmCaptureIpAddress 179

N

ncsCADhcpSiteSpecificCode 50, 86
ncsCAHost 50
ncsCaHost 86
ncsCAPort 50, 86
ncsCASelectConfigSource 50, 86
ncsCAStaticHost 87
ncsCAStaticPort 87
ncsCompatibilityRtpPayloadType18EncodingName 92
ncsCompatibilityVersion 93
ncsDefaultDigitMap 87
ncsEndpointIdListIncludeNotStarted 88
ncsEndpointIdTerm1 88
ncsEndpointIdTerm2 88
ncsLinePackageBzDuration 91
ncsLinePackageDlDuration 91
ncsLinePackageLDuration 91
ncsLinePackageMwiDuration 91
ncsLinePackageOtDuration 91
ncsLinePackageRbkDuration 91
ncsLinePackageRgDuration 91
ncsLinePackageRoDuration 91
ncsLinePackageRtDuration 91
ncsLinePackageSlDuration 92
ncsLinePackageTCriticalDuration 92
ncsLinePackageTPartialDuration 92
ncsPiggyBackingEnable 88
ncsPort 87
ncsRestartLevel 87
ncsRetransmissionAlgorithm 89
ncsRetransmissionDisconnectInitialWaitingPeriod 90
ncsRetransmissionDisconnectMaxWaitingPeriod 90
ncsRetransmissionDisconnectMinWaitingPeriod 90
ncsRetransmissionDisconnectThreshold 90
ncsRetransmissionDisconnectThresholdDnsQuery 90
ncsRetransmissionDisconnectTimeout 89
ncsRetransmissionHistoryTimeout 90
ncsRetransmissionInitialPeriod 89
ncsRetransmissionMaxPeriod 89
ncsRetransmissionMaxWaitingDelay 90
ncsRetransmissionSuspicionThreshold 89
ncsRetransmissionSuspicionThresholdDnsQuery 90

Q

qosSignalingDiffServ 163
qosSignalingIeee8021qEnable 164
qosSignalingIeee8021qUserPriority 164
qosT38FaxDiffServ 163
qosT38FaxIeee8021qEnable 164

qosT38FaxIeee8021qUserPriority 164
qosVlanIeee8021qDefaultUserPriority 165
qosVlanIeee8021qTaggingEnable 165
qosVlanIeee8021qVirtualLanID 165
qosVoiceDiffServ 163
qosVoiceIeee8021qEnable 164
qosVoiceIeee8021qUserPriority 164

S

snmpAgentAccess 38
sntpConfigSource 19
sntpEnable 157
sntpHost 51, 158
sntpPort 51, 158
sntpSelectConfigSource 51, 158
sntpStaticHost 158
sntpStaticPort 158
sntpSynchronizationPeriod 157
sntpSynchronizationPeriodOnError 157
sntpTimeZoneString 107, 125, 159
stunEnable 156
stunKeepAliveInterval 156
stunQueryCacheDuration 156
stunQueryTimeout 156
stunStaticHost 156
stunStaticPort 156
sysAdminCommand 43, 122, 123
sysAdminDefaultSettingsEnable 20
sysAdminDownloadConfigFileStatus 102, 111
sysConfigCommand 105
sysConfigComputerEthernetSpeed 59
sysConfigDownloadConfigFile 106, 108, 111
sysConfigDownloadConfigMode 111
sysConfigNetworkEthernetSpeed 59
sysConfigStatsNumberPeriods 172
sysConfigStatsPeriodLength 172
syslogConfigSource 19
syslogDhcpSiteSpecificCode 49, 168
syslogHost 19, 49, 168
syslogMsgDisplayLocalHost 169
syslogMsgDisplayMacAddress 169
syslogMsgDisplayTime 169
syslogMsgDisplayTimeFormat 169
syslogMsgMaxSeverity 167
syslogPort 19, 49, 168
syslogSelectConfigSource 49, 168
syslogStaticHost 168
syslogStaticPort 168
sysMacAddress 9, 52
sysMibVersion 38

T

telephonyCountrySelection 96
telephonyIpSignalingProtocolSelection 39, 61, 85

V

voiceIfAdaptativeJitterBufferEnable 178
voiceIfCodecG723Enable 136

voiceIfCodecG723MaxPTime 137
voiceIfCodecG723MinPTime 137
voiceIfCodecG72616kbpsEnable 136
voiceIfCodecG72616kbpsMaxPTime 138
voiceIfCodecG72616kbpsMinPTime 138
voiceIfCodecG72616kbpsPayloadType 136
voiceIfCodecG72624kbpsEnable 136
voiceIfCodecG72624kbpsMaxPTime 138
voiceIfCodecG72624kbpsMinPTime 138
voiceIfCodecG72624kbpsPayloadType 136
voiceIfCodecG72632kbpsEnable 136
voiceIfCodecG72632kbpsMaxPTime 138
voiceIfCodecG72632kbpsMinPTime 138
voiceIfCodecG72632kbpsPayloadType 136
voiceIfCodecG72640kbpsEnable 136
voiceIfCodecG72640kbpsMaxPTime 138
voiceIfCodecG72640kbpsMinPTime 138
voiceIfCodecG72640kbpsPayloadType 136
voiceIfCodecG729Enable 136
voiceIfCodecG729MaxPTime 139
voiceIfCodecG729MinPTime 139
voiceIfCodecPcmaEnable 136
voiceIfCodecPcmaMaxPTime 137
voiceIfCodecPcmaMinPTime 137
voiceIfCodecPcmuEnable 136
voiceIfCodecPcmuMaxPTime 137
voiceIfCodecPcmuMinPTime 137
voiceIfCodecPreferred 135
voiceIfDtmfDetectionRiseTimeCriteria 142
voiceIfDtmfDetectionUnitBreakPowerThreshold 142
voiceIfDtmfDetectionUnitMaxPowerThreshold 141
voiceIfDtmfDetectionUnitMinPowerThreshold 141
voiceIfDtmfDetectionUnitNegativeTwist 142
voiceIfDtmfDetectionUnitPositiveTwist 142
voiceIfDtmfPayloadType 140
voiceIfDtmfTransport 136, 139, 140
voiceIfG711ComfortNoiseGenerationEnable 146
voiceIfG711VoiceActivityDetectionEnable 144
voiceIfG729VoiceActivityDetectionEnable 144
voiceIfMaxJitterBufferLength 143, 178
voiceIfTargetJitterBufferLength 143, 178
voiceIfUserInputGainOffset 146
voiceIfUserOutputGainOffset 146

Index

Numerics

10 BaseT 6, 10, 11, 59
    defined 235
    see also *cabling*
100 BaseT 6, 10, 11, 59
    defined 235
    see also *cabling*
802.1q, in QoS 164

A

acronyms 243
ADSI
    caller ID 96
    defined 235
A-Law 133
    defined 235
analog lines
    see *lines*
    see *RJ21X connector*
analog modem, feature 133
area code, defined 235
audience, intended xiii
automatic
    configuration update 106
    software update 124

B

brackets around domain name, in MGCP/NCS 84
brief OSI signal, in MGCP/NCS 82
broadcast storm, behaviour when restarting 21
Bypass connection
    connecting 10, 11
    defined 153

C

cable length vs loop current 206
cabling
    loop current vs cable length 206
    RJ-11 205
    RJ21X
        creating 203
        defined 203
        Tip and Ring positions 203
    RJ-45
        crossover 202
        pin name 202
        pinout information 201
        straight through 201
    see also *10 BaseT*
    see also *100 BaseT*
call
    emergency, bypass 153
    placing 4
call agent
    defined 236
    setting 62, 86
caller ID
    ADSI 96
    country-specific, selecting 97
caller ID (continued)
    DTMF signalling 95
        ETSI 300 659-1 January 2001 (Annex B) 95
        TDK-TS 900 301-1 January 2003 95
    FSK generation 95
        Bellcore GR-30-CORE 95
        British Telecom (BT) SIN227, SIN242 96
        ETSI 300 659-1 96
        UK CCA specification TW/P&E/312 96
    generation 95
clear channel fax
    enabling 148
    preferred codec 149
    setting 147
codec
    data
        clear channel fax 147
            enabling 148
            preferred 149
        enabling 147
        T.38 149, 151
    voice
        defined 133
        DTMF detection 140
        DTMF transport type 139, 140
        enabling 136
        packetization time 137
        preferred 135
comfort noise 145
compliance to standards. see *standards compliance*
conference mode, feature 75
configuration
    file 38
    using a GUI 35
configuration file
    automatic update 106
    download server 99
        configuration source 99
        DHCP information, using 100
        HTTP server, configuring 99
        IP address 99
        SNTP server, configuring 99
        static information, using 100
        TFTP server, configuring 99
    download, setting 101
    encryption
        decrypting generic 103
        decrypting specific 103
        defined 103
    example 114
    HTTP, downloading via 105
    management server, downloading from 111
    syslog messages 103
    TFTP, downloading via 104
configuration sources, setting all to static 43
configuring the software
    configuration file 38
    DHCP (dynamic), using 42
    MIB. see *SNMP*
    static
        setting configuration sources to 43
        using 43
connecting the unit 9

connectors
analog lines (RJ21X) 6
Bypass 7
ETH1 6
ETH2 6
FXS lines 6, 7
port numbering convention, FXS 7
reset / default 7
universal power supply unit 8
country-specific parameters 207
caller ID, selecting 97
setting 96
crossover cable. see *cabling*
customer services xviii

D

default router, setting 43
Default Settings
factory reset procedure 20
disabling 20
in recovery mode 18
DHCP information
configuration file download server 100
Image 116
management server 161
MGCP call agent 62
NCS call agent 86
SNTP 158
syslog daemon 168
see also *static information*
DHCP server
configuring 52
defined 236
FQDN, entering 56
IP address of, setting 43
IP addresses, entering 55
network configuration 53
requirement 3
site specific option 54
vendor class ID 53
vendor specific option 53
Differentiated Services (DS) Field, in QoS 163
disabling lines 129
DNS
defined 236
primary 43
static 46
requirement 3
secondary 43
static 46
documentation
Media5 download portal xvii
Mediatrix download portal xvii
domain name, brackets around 84
downgrading software, procedure 126
downloading software
automatic update 124
configuration source 116
emergency download 126
HTTP server, configuring 115
HTTP, via 123
Image path 118
LED states 121
SNTP server, configuring 115
TFTP server, configuring 115
downloading software (continued)
TFTP, via 122
troubleshooting 181
zip file 118
DTMF
defined 236
detection 140
out-of-band 139
signalling, caller ID 95
transport type 139
payload type 140

E

echo cancellation 145
emergency call, bypass 153
emergency software download 126
enabling lines 129
encryption, of configuration files
decrypt generic 103
decrypt specific 103
defined 103
end user technical support xviii
endpoint. See *lines*
Ethernet connection, setting speed of 59
examples of use, MTU/MDU IP telephony 5

F

factory reset
disabling 20
reverting to 20
see also *recovery mode*
fake RFC 3407 recognition, in MGCP/NCS 83
far end disconnect, signalling 131
fax
clear channel 147
multiple tone detection 81
T.38 149
no-signal 151
user gain vs communication quality 146
features, conference mode 75
firewall, traversal 78
flash hook, setting 130
Foreign Exchange Service/Station (FXS)
defined 237
see also *lines*
FQDN, entering 56
FSK generation, caller ID 95

G

G.711 133
comfort noise 145
defined 237
voice activity detection 143
G.723.1 134
defined 237
G.726 134
comfort noise 145
defined 237
payload type 136
voice activity detection 143
G.729 135
Annex B negotiation 144
defined 237

G.729 135 (continued)
voice activity detection 144
GUI, using a 35

H

hardware
cleaning 9
condensation 9
front indicators 6
proper location 8
rear connections 8
HTTP
configuration file download 105
server
configuring 99, 115
requirement 3
software download via 123
humidity level 9

I

IEEE 802.1q, in QoS 164
Image server
DHCP information, using 116
static information, using 117
immediate modem tone reporting, in MGCP/NCS 82
indicators of the hardware 6
installation
connecting the hardware 9
package contents 3
provisioning sequence, initial 13
rack-mounting 9
requirements 3
reserving IP address 9
RJ21X connector 203
safety recommendations 3
selecting site for 8
setting up the unit for the first time 12
verifying 21
intended audience xiii
IP address
default router 43
defining
decimal 41
hexadecimal 41
octal 41
DHCP server 43
DHCP, using 42
DNS, primary 43
static 46
DNS, secondary 43
static 46
download server 99
entering 55
ETH2 connector, static 51
Image server 116
locating 41
Management Server 161
MGCP call agent 62
NCS call agent 86
of unit 43
SNTP server 158
static
setting configuration sources to 43
using 43
IP address (continued)
subnet mask 43
syslog daemon 168

J

jitter
buffer protection 142
defined 237

L

LAN
cable 21
defined 238
LEDs
behaviour
in download mode 121
in starting mode 13
defined 238
In Use 14
LAN 14
patterns
AdminMode 14, 16
Booting 14, 16
DefaultSettings ending 15
DiagFailed 15
ImageDownloadError 15
ImageDownloadInProgress 15
InitFailed 15
NormalMode 14, 16
RebootPending 15
RecoveryMode 15, 17
RecoveryModePending 15
ResetPending 15
Power 14
Ready 14
states 14
lines
comfort noise 145
data codecs 147
clear channel fax 147
clear channel, enabling 148
clear channel, preferred 149
enabling 147
T.38 149, 151
echo cancellation 145
far end disconnect, signalling 131
jitter buffer protection 142
locking/unlocking 129
multiple connections on 130
user gain 146
voice activity detection 143
voice codecs
defined 133
DTMF detection 140
DTMF transport type 139, 140
enabling 136
packetization time 137
preferred codec 135
local
host, in customized syslog messages 169
IP address, setting 43
time, in customized syslog messages 169
location
caller ID, selecting 97

location (continued)
country, setting 96
locking lines 129
loop current vs cable length 206
loop current, setting 131

M

MAC address 9
defined 238
in customized syslog messages 169
Management Server
defined 238
DHCP information, using 161
in configuration file download 111
static information, using 162
using 161
Media5 download portal xvii
Mediatrix download portal xvii
meter pulse, setting 75
MGCP, setting
brackets around domain name 84
brief OSI signal 82
call agent 62
DHCP information, using 62
static information, using 63
configuration 61
connect RTP sockets 81
endpoints 67
fake RFC 3407 recognition 83
firewall traversal 78
immediate modem tone reporting 82
meter pulse 75
multiple fax tone detection 81
Offer/Answer model 79
offered stream format 80
packages
DTMF 71
Generic Media 70
Line 71
XL 73
X-P 74
polarity reversal on calling card service tone 84
retransmission 68
services 61
session ID/version 80
switching to 61
T.38 capabilities using audio codec 98 82
T.38 negotiation syntax 83
UDP checksum 81
MIB
defined 25
in SNMP protocol 25
see also *parameters*
MIB structure
changing a parameter value 35
conformance 34
description
mediatrixAdmin 33
mediatrixConfig 33
mediatrixExperimental 33
mediatrixIpTelephonySignaling 33
mediatrixMgmt 33
mediatrixModules 33
mediatrixProducts 33
events 34
MIB structure (continued)
introduction 25
objects 34
OID, defined 25
persistent parameters 35
SMI, defined 25
SNMP messages. see *SNMP*
tables
defined 36
generic 36
groupAdmin 37
ifAdmin 37
textual conventions 34
volatile parameters 35
mounting, on a rack 9
MTU, requirements 175
MTU/MDU IP telephony, example of use 5
Mu (μ)-Law 133
defined 238

N

NAT
in configuration file download 104
see also *STUN*
NCS, setting
brackets around domain name 84
brief OSI signal 82
call agents 86
DHCP information, using 86
static information, using 87
compatibility version 93
configuration 85
connect RTP sockets 81
endpoints 88
fake RFC 3407 recognition 83
immediate modem tone reporting 82
Line package 91
multiple fax tone detection 81
Offer/Answer model 79
offered stream format 80
polarity reversal on calling card service tone 84
retransmission 89
RTP Payload Type 18 92
services 85
session ID/version 80
switching to 85
T.38 capabilities using audio codec 98 82
T.38 negotiation syntax 83
UDP checksum 81
no-signal, in T.38 151

O

Offer/Answer model 79
OID, defined 25
operating temperature 9
out-of-band DTMF 139
overview of the product 4

P

package contents 3
packetization time, setting for voice codecs 137
parameters
changing value of 35

parameters (continued)
using a GUI 35
PCM traces, enabling 179
persistent parameters, defined 35
placing a call 4
polarity reversal on calling card service tone, in MGCP/NCS 84
port number
configuration file fetching 48
configuration file server 99
DHCP setting 55
image server 47, 116
management server 48, 161
MGCP 66
MGCP call agent 50, 62
NCS 87
NCS call agent 50, 86
SNMP agent 46
SNMP trap 46
syslog 49, 168
port numbering convention, FXS connectors 7
product overview 4
protocol, switching 39
provisioning
configuration file 38
initial sequence 13
MIB files 38

Q

QoS
802.1q 164
defined 239
Differentiated Services (DS) Field 163
VLAN 165

R

rack-mounting the unit 9
rear connections 8
recovery mode
LED patterns 17
resetting in 18
see also *factory reset*
related documentation xiv
requirements 3
restart
behaviour in case of broadcast storm 21
software-initiated 21
RFC
RFC 1350 195
RFC 1769 157
RFC 1889 195
RFC 1890 140, 195
RFC 2131 52, 195
RFC 2132 52, 53, 54, 195
RFC 2347 195
RFC 2348 195
RFC 2349 195
RFC 2475 163
RFC 2833 139, 195
RFC 3164 167, 195
RFC 3264 79
RFC 3389 145, 195
RFC 3435 61, 195
RFC 3489 155, 195
RJ-11. see *cabling*
RJ21X connector
creating 203
defined 203
Tip and Ring positions 203
RJ-45. see *cabling*
RTCP 163
RTP, Payload Type 18 92

S

safety
recommendations 3, 193
warnings
Circuit Breaker (15A) 192
LAN Connector 192
No. 26 AWG 192
Product Disposal 192
Socket Outlet 192
TN Power 192
signaling protocol, MGCP. see *MGCP, setting*
site specific information, DHCP setting 54
site, selecting for unit 8
SMI, defined 25
SNMP
access limitation 38
behaviour 27
non-secure management mode 28
secure management mode 28
configuring 46
messages 26
MIB 25
SNMP configuration file 29
versions 26
SNTP
defined 240
DHCP information, using 158
enabling 157
server, configuring 99, 115
static information, using 158
time zone, defining custom 159
software
downgrading, procedure 126
downloading
automatic update 124
configuration source 116
emergency procedure 126
HTTP server, configuring 115
HTTP, via 123
Image path 118
LED states 121
SNTP server, configuring 115
syslog messages 120
TFTP server, configuring 115
TFTP, via 122
troubleshooting 181
zip file 118
see also *downgrading*
standards compliance
agency approvals 187
CE marking 189
emissions 187
FCC Part 15 disclaimer 188
FCC Part 68 disclaimer 188
immunity 187
Industry Canada disclaimer 189
RoHS China 190

standards compliance (continued)
safety standards 187
telecom 187
standards supported xvi
caller ID
Bellcore GR-30-CORE 95
British Telecom (BT) SIN227, SIN242 96
ETSI 300 659-1 96
ETSI 300 659-1 January 2001 (Annex B) 95
TDK-TS 900 301-1 January 2003 95
UK CCA specification TW/P&E/312 96
ITU-T Q.24 139
PKT-SP-EC-MGCP-I01-990312 195
Recommendation ITU T.38 version 0 149
Recommendation ITU-T T.38, section D.2.3 83
RFC 1350 195
RFC 1769 157
RFC 1889 195
RFC 1890 140, 195
RFC 2131 52, 195
RFC 2132 52, 53, 54, 195
RFC 2347 195
RFC 2348 195
RFC 2349 195
RFC 2475 163
RFC 2833 139, 195
RFC 3164 167, 195
RFC 3264 79
RFC 3389 145, 195
RFC 3435 61, 195
RFC 3489 155, 195
static
ETH2 connector IP address 51
setting DNS address as 46
static information
configuration file download server 100
Image 117
management server 162
MGCP call agent 63
NCS call agent 87
setting all configuration sources to 43
SNTP 158
syslog daemon 168
see also *DHCP information*
statistics
MGCP 171
NCS 171
resetting 172
RTP 171
setting how to collect 172
viewing 171
straight through cable. see *cabling*
STUN
configuring 156
defined 155
subnet mask, setting 43
support services xviii
switching protocol 39
syslog
daemon
configuring the application 169
customizing messages
local host 169
local time 169
MAC address 169
defined 167
syslog (continued)
daemon
DHCP information, using 168
enabling 167
messages examples 167
requirement 3
static information, using 168
messages
configuration file 103
examples 167
software download 120

T

T.38
defined 240
enabling 151
negotiation syntax in MGCP/NCS 83
not supported by other endpoint 180
number of redundancy packets 151
protection level 151
T.38 capabilities using audio codec 98, in MGCP/NCS 82
tables
defined 36
generic 36
groupAdmin 37
ifAdmin 37
technical support for end user xviii
temperature, operating 9
textual conventions, in MIB structure 34
TFTP
configuration file download 104
server
configuring 99, 115
defined 241
requirement 3
software donwload via 122
time zone, defining custom 159
TPE. see *cabling*
translated warning definition 191
troubleshooting
call
cannot establish to endpoint 180
cannot make 180
cannot disable adaptative jitter buffer 178
DHCP unreachable 178
fax
poor line condition during transmission 180
unable to send in clear channel 181
unable to send in T.38 181
voice does not switch back to codec after clear channel fax 181
LEDs, all off 177
long delay when starting unit 177
PCM traces, enabling 179
SNMP
cannot set a variable 183, 184
MIB variable empty after downgrade 184
network manager cannot access unit 183
no response when trying to access unit 183
SNMPv3 variables contents 184
traps not received by network manager 183
when viewing table, unit does not respond 184
wrong value error message 183
software download
cannot communicate with image server 181

troubleshooting (continued)
software download
long time to perform 182
path not recognized 182
transfer problems 182
unable to reach unit after changing Ethernet speed 178
value not accepted 178

U

UDP, checksum 81
Unit Manager Network product
as management server 3, 46, 48, 161
defined xvii
using 35, 41, 43, 115
unlocking lines 129
using this manual xvi
UTP. see *cabling*

V

vendor specific information, DHCP setting 53
verifying the installation 21
viewing statistics and performances 171
VLAN, in QoS 165
voice activity detection 143
volatile parameters, defined 35