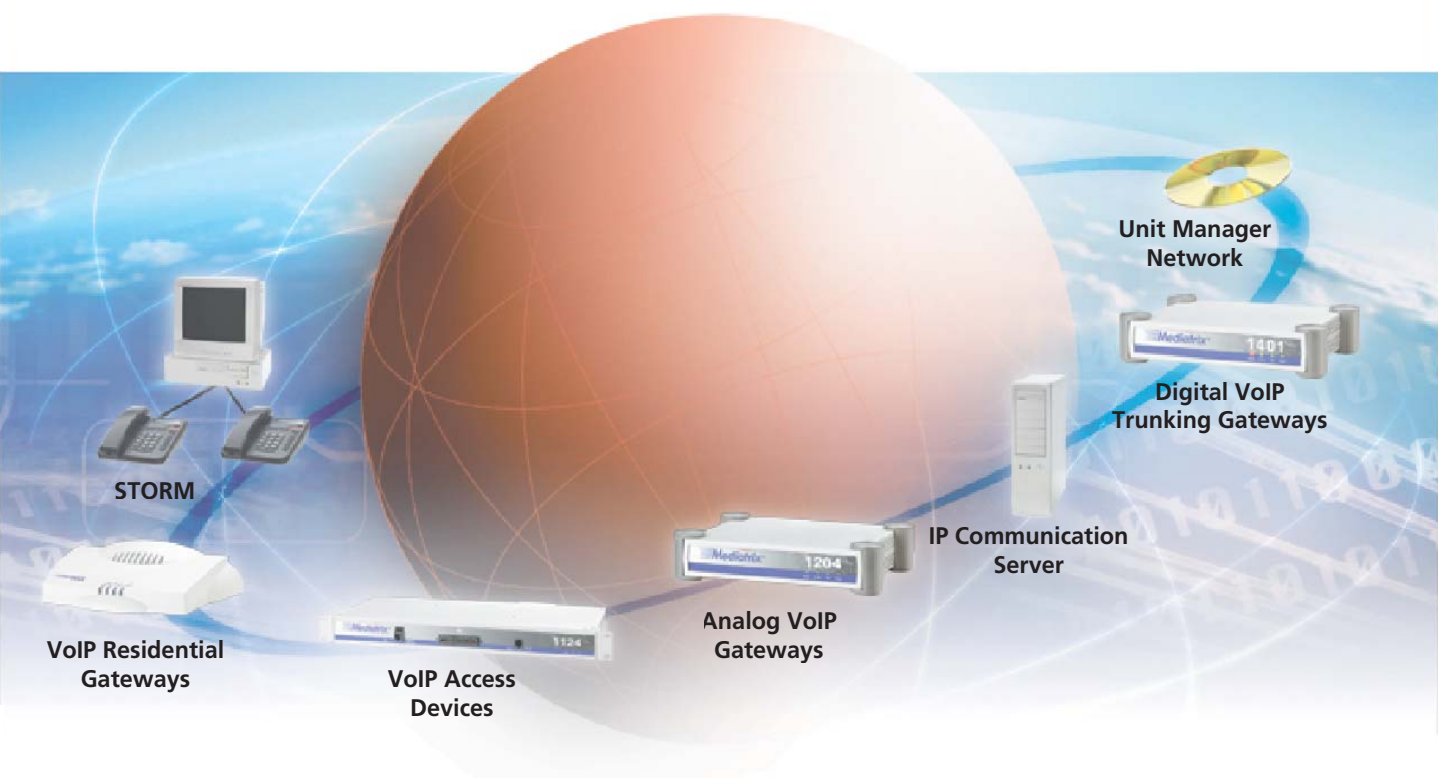




EMPOWERING THE EDGE OF THE IP NETWORK



# Mediatrix<sup>®</sup> 1102

## Mediatrix 1100 Series

# Administration Manual

## SIP Version

Product Version 4.3  
MIB Version Supported: 1.1.9.32

Document Revision L

January 14, 2003

**Mediatrix Telecom, Inc.  
4229 Garlock Street  
Sherbrooke, Québec, Canada J1L 2C8**

**Mediatrix® 1102 Administration Manual (SIP Version)**

© 2001-2003, Mediatrix Telecom, Inc.

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

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

**Trademarks**

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated.

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

## Supplementary Copyright Information

### **CMU/UCD copyright notice: (BSD like)**

---

Copyright 1989, 1991, 1992 by Carnegie Mellon University  
Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California  
All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

### **Networks Associates Technology, Inc copyright notice (BSD)**

---

Copyright (c) 2001, Networks Associates Technology, Inc  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the NAI Labs nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**Cambridge Broadband Ltd. copyright notice (BSD)**

---

Portions of this code are copyright (c) 2001, Cambridge Broadband Ltd.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**OpenSSL License**

---

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
  - "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
  - "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### **Original SSLey License**

---

Copyright (C) 1995-1998 Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com))

All rights reserved.

This package is an SSL implementation written by Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
  - "This product includes cryptographic software written by Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com))".

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
  - "This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

# Contents

## Preface

<b>Introduction .....</b>	<b>xiii</b>
Intended Audience .....	xiii
SCN vs PSTN .....	xiii
Related Documentation .....	xiv
Using this Manual .....	xiv
Safety Warnings .....	xvi
Safety Recommendations .....	xvii
End User Technical Support .....	xviii

## Chapter 1

<b>Getting Started .....</b>	<b>1</b>
Overview .....	1
About the Mediatrix 1102 .....	1
Implementing the Solution .....	2
Features .....	2
Hardware Features .....	2
Software Features .....	3
Panels .....	4
Front Indicators .....	4
Rear Connectors .....	5
SNMP .....	6
SNMP Versions .....	7
Changing a Parameter Value .....	8

## Chapter 2

<b>Installation .....</b>	<b>11</b>
Requirements .....	11
Safety Recommendations .....	12
Package Contents .....	12
Choosing a Suitable Installation Site .....	12
Wall-Mounting .....	13
Connecting the Mediatrix 1102 .....	14
First Time Set up .....	15
Reserving an IP Address .....	15
Initial Provisioning Sequence .....	16

Special Vocal Features .....	17
LED Behavior in Boot Mode .....	17
Using the Default Settings Switch .....	17
At Run-Time .....	17
At Boot-Time .....	18
Recovery Mode .....	18
Factory Settings Mode .....	20
Performing a Software Restart .....	21
Verifying the Installation .....	21

## Chapter 3

<b>IP Address and Network Configuration .....</b>	<b>23</b>
IP Addresses .....	23
IP Addresses Formats .....	23
Provisioning Source .....	24
Configuring the DHCP Server .....	25
Connection to the DHCP Behavior .....	25
Network Configuration .....	26
Services .....	26
DHCP or Static Configuration .....	26
Local Host .....	27
Image .....	29
Management Server .....	30
Syslog .....	31
SIP Servers .....	31
SNTP .....	33
Vendor and Site Specific DHCP Options .....	33
Site Specific Options .....	33
Vendor Specific Options .....	35
Entering IP Addresses .....	37
Option Codes .....	39
Settings Example .....	39
Error Handling .....	40
DHCP Server Failures .....	40
Vendor/Site Specific Option Missing .....	41
DNS Failures .....	41
Ethernet Connection Speed .....	41

## Chapter 4

<b>Basic Configuration .....</b>	<b>43</b>
Configuring the Software .....	43
Sending Configuration Data to the Mediatrix 1102 .....	44
Provisioning Sequence .....	46

Setting the Location (Country).....	46
Caller ID Information.....	47
Caller IDs Supported .....	48
FSK Generation.....	48
Placing a Call.....	49

## Chapter 5

---

### Software Download..... 51

Before Downloading .....	51
Configuring the TFTP Server.....	51
Extracting the Zip File.....	51
DHCP vs. Static Configuration .....	51
Download Procedure .....	54
LED States .....	56
Emergency Software Procedure.....	56
Using the Emergency Software .....	56

## Chapter 6

---

### Port Configuration ..... 59

Tables.....	59
Locking/Unlocking Ports.....	59
Setting Voice Information .....	59
Jitter Buffer .....	59
Voice Activity Detection .....	60
Echo Cancellation.....	61
Comfort Noise.....	61
User Gain Variables .....	62
Selecting Codecs.....	63
Voice Codecs .....	63
Data Codecs.....	66
Detecting a Current Drop.....	67
Loop Current.....	67

## Chapter 7

---

### Setting SIP Protocol Features ..... 69

Setting up SIP Servers .....	69
Registrar Server .....	69
Proxy Server.....	70
Outbound Proxy Server .....	72
Defining SIP User Agents.....	74

Session Timers .....	76
Authentication Information .....	77
Setting up the Urgent Gateway Information .....	78
Using a NAT Firewall .....	79
Method 1: NAT/Firewall Public IP Address .....	80
Method 2: NAT Traversal Scheme .....	80
Setting Interop Parameters .....	81
Replaces Configuration Setting .....	81
SIP Transfer Version .....	82
Session Timers Version .....	83
Transmission Timeout .....	83

## Chapter 8

<b>Telephony Configuration .....</b>	<b>85</b>
Using Digit Maps .....	85
Special Characters .....	86
How to Use a Digit Map .....	86
Validating a Digit Map .....	88
Setting up Digit Maps .....	88
Using Refused Digit Maps .....	90
Digit Map Examples .....	91
Example 1 – Standard Calls .....	91
Example 2 – PBX Emulation .....	93
Supplementary Telephony Services .....	96
Call Hold .....	96
Call Forward .....	96
Call Waiting .....	101
Second Call .....	103
Call Transfer – Blind Transfer .....	103
Call Transfer – Attended Transfer .....	104
Conference Call .....	104
Automatic Speed Dialing .....	105
IP Address Call Service .....	106
SNTP Settings .....	106
DHCP vs. Static Configuration .....	107
Defining a Custom Time Zone .....	108

## Chapter 9

<b>Management Server Configuration .....</b>	<b>113</b>
Using the Management Server .....	113
DHCP vs. Static Configuration .....	113

## Chapter 10

---

<b>Miscellaneous Configuration .....</b>	<b>117</b>
Using QoS .....	117
Differentiated Services (DS) Field .....	117
IEEE 802.1q .....	118
VLAN .....	120
Syslog Daemon Configuration .....	121
DHCP vs. Static Configuration .....	121
Configuring the Syslog Daemon .....	123
Setting up Flash Hook Detection .....	123

## Chapter 11

---

<b>Using Statistics .....</b>	<b>125</b>
RTP Statistics .....	125
Statistics Buffers .....	125
How are Statistics Collected? .....	125
Example .....	126

## Chapter 12

---

<b>Maintenance .....</b>	<b>129</b>
Caution Regarding Handling .....	129
Location .....	129
Condensation .....	129
Cleaning .....	129
Troubleshooting .....	129
General Operation Problems .....	130
Software Upgrade Problems .....	132
SNMP Management Software Problems .....	133

## Appendix A

---

<b>LED Patterns .....</b>	<b>135</b>
LED Indicators .....	135
LED States .....	135
LED Patterns .....	136
NormalMode LED Pattern Description .....	138
Recovery Mode LED Patterns .....	140

## Appendix B

<b>Country Specific Parameters .....</b>	<b>143</b>
Australia.....	143
Austria .....	144
China .....	144
France .....	145
Germany.....	145
Hong Kong.....	146
Indonesia .....	147
Israel.....	147
Italy .....	148
Japan.....	148
Malaysia .....	149
North America.....	149
Spain .....	150
Sweden.....	151
Switzerland.....	151
Thailand.....	152
UK.....	152

## Appendix C

<b>Standards Compliance .....</b>	<b>153</b>
Standards Supported.....	153
Disclaimers .....	154
Federal Communications Commission (FCC) Part 15.....	154
CE Marking.....	154

## Appendix D

<b>Glossary.....</b>	<b>155</b>
----------------------	------------

## Appendix E

<b>List of Acronyms.....</b>	<b>163</b>
------------------------------	------------



The Mediatrix 1102 offers two Ethernet port switches enabling to establish two connections between conventional analog telephones or Group 3 fax machines and either a WAN, a LAN or a personal computer. It can be used to provide connectivity to broadband access equipment for a Service Provider's IP Telephony offering to residential or SME markets.

To ensure maximum flexibility, the Mediatrix 1102 can:

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

---

## Intended Audience

This manual provides all the information needed to install and manage the Mediatrix 1102. It is intended for network administrators who install and set up network equipment; consequently, it assumes a basic working knowledge of LANs.

From the perspective of the LAN administrator, a Mediatrix 1102 presents itself just like another device that is to be added to the LAN. It requires the same kind of TCP/IP addressing. The Mediatrix 1102 can also use a DHCP server on the LAN to automatically receive its IP configuration assignment.

## SCN vs PSTN

In Mediatrix Telecom, Inc.'s 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.

## What's New in this Version

- Updated the country-specific information. See [“Appendix B - Country Specific Parameters” on page 143](#) for more details.
- Updated [“Chapter 3 - IP Address and Network Configuration” on page 23](#).
- Added safety warnings. See [“Safety Warnings” on page xvi](#) for more details.

---

## Related Documentation

In addition to this manual, the Mediatrix 1102 document set includes the following:

- ▶ *Mediatrix 1102 User's Manual*  
Provides information to the end-user on how to use the Mediatrix 1102. The manual is not printed – it is located on the documentation CD provided with the Mediatrix 1102.
- ▶ *MIB Reference Manual*  
Lists and explains all parameters in the MIB structure.
- ▶ *Mediatrix 1102 Quick Start booklet*  
This printed booklet allows you to quickly setup and work with the Mediatrix 1102.

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

---

## Using this Manual

The following information provides an explanation of the symbols which appear on the Mediatrix 1102 and in the documentation for the product.



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

---

**Waarschuwing:** Dit waarschuwingssymbool betekent gevaar. U overtreedt in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

**Varoitus:** Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

**Attention:** Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

**Warnung:** Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst.

**Avvertenza:** Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

**Advarsel:** Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

**Aviso:** Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

**¡Advertencia!:** Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

**Warning!:** 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.



**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.

---

---

## Safety Warnings

This section lists the following safety warnings:

- ▶ Circuit Breaker (15A) Warning
- ▶ TN Power Warning
- ▶ Product Disposal Warning
- ▶ No. 26 AWG Warning
- ▶ LAN Port 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 Port Warning



**Warning:** Do not connect the LAN port 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.
-

**End User Technical Support**

In order to maximize technical support resources, Mediatrix Telecom, Inc. works through its partner channels to resolve technical support issues. All end users requiring technical support are encouraged to contact their vendor directly.

This chapter provides an overview of the Mediatrix 1102 and introduces the Simple Network Management Protocol (SNMP) as remote management tool.

---

## Overview

The Mediatrix 1102 is a standalone Internet telephony terminal that connects to virtually any business telephone system supporting standard analog lines.

This version of the Mediatrix 1102 uses the Session Initiation Protocol (SIP), which is a protocol for transporting call setup, routing, authentication, and other feature messages to endpoints within the IP domain.

## About the Mediatrix 1102

The Mediatrix 1102:

- ▶ 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.
  - SIP protocol for call management
  - T.38 for fax relay
- ▶ Supports the following Codecs:
  - G.711 ( $\mu$ -law, A-law)
  - G.723.1A
  - 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

**Implementing the Solution**

When an Internet telephony call is placed from one location to another, the voice signals pass through the Mediatrix 1102. The voice signals are compressed into data packets, which are then diverted by the unit onto an IP/data network such as a LAN, a WAN, or the public Internet. Upon reaching its destination, the data is converted back into voice signals, then fed into the corresponding endpoint.

The Mediatrix 1102 utilizes technology that optimizes available bandwidth, so users do not hear echoes, stops and starts, or annoying clicks and pops. When traffic congestion is properly managed, Mediatrix 1102 customers cannot tell that their conversation is being carried over a packet network rather than the traditional Switched Circuit Network (SCN).

See the *Mediatrix 1102 User's Manual* for call processes examples.

---

**Features**

The following are some of the features the Mediatrix 1102 offers.

**Hardware Features****2 FXS Ports**

Central Office quality SLICs supporting all the BORSCHT functions and thus meet most worldwide telephony standards.

**2 Ethernet Ports**

Two Ethernet port switches that enable to establish two connections to either a WAN, a LAN or a personal computer. One of the Ethernet ports can be used as a remote power feeding, IEEE 802.3af compliant and Power DSine certified, when the LAN offers the capability.

**Fax Interface**

Handles G3 and Super G3 fax transmissions at speeds up to 14.4 kbps. Automatic fax mode detection is standard on all ports. Real-Time Fax Over UDP with the T.38 protocol stack is also available.

**Analog Modem**

Supports 9.6 kbps to 33.6 kbps analog modems (V.34 support over clear channel). If configured adequately, modems with higher rate capabilities (for instance, V.90) will automatically fall back in the transmission range supported, which is usually near 33.6 kbps.

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.

## Software Features

### 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, who will then play the DTMF sequence back by re-generating the true tones. Such a mechanism is known as out-of-band DTMF.

The Mediatrix 1102 receives and sends out-of-band DTMFs as per RFC 2833 using RTP (<http://www.ietf.org/rfc/rfc2833.txt?number=2833>). DTMFs supported are 0-9, A-D, \*, #.

### RTCP

Supports the Real Time Control Protocol, which is used to send packets to convey feedback on quality of data delivery.

### Fully Configurable “SCN-Like” Experience

The Mediatrix 1102 provides the tones heard on the standard telephone network. For instance, a dial tone is heard as soon as the handset is lifted. Call progress tones such as ringback and busy are also provided. The Mediatrix 1102 can be configured to take almost any kind of telephone number.

### Remote Site Configuration/Management

Integrates seamlessly into your existing administration environment. Implementation of a SNMP agent allows device-related adjustment parameters to be modified and polled remotely. The software upgrade is downloaded via a TFTP server.

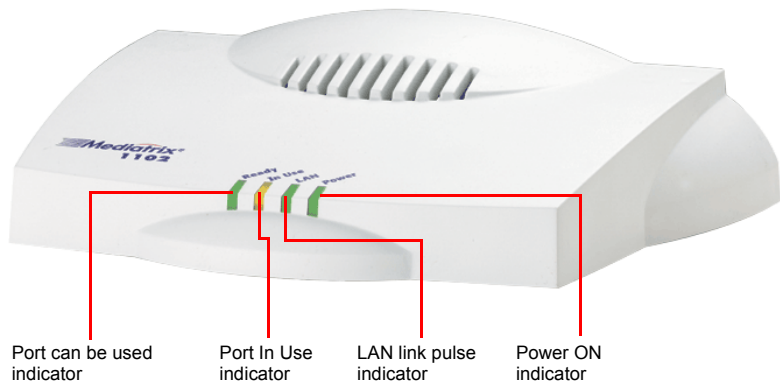
## Panels

This section provides an overview of the front and rear panels of the Mediatrix 1102.

### Front Indicators

[Figure 1](#) shows the four (4) visual indicators located on the front of the Mediatrix 1102.

**Figure 1:** Front Panel Indicators



[Table 1](#) describes the LEDs on the front panel of the Mediatrix 1102.

**Table 1:** Front Panel Indicators

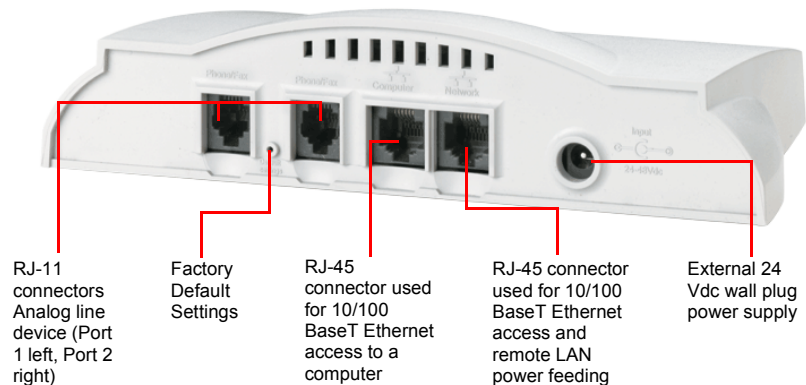
Indicator	Description
– <b>Ready</b> – Port can be used indicator	When lit, the unit is ready to initiate or receive a call. The unit does not have to be registered to a server.
– <b>In Use</b> – Port In Use indicator	When lit, at least one of the FXS ports is in use.
– <b>LAN</b> – Network link pulse indicator	Provides the state of the network connected to the <i>Network</i> port.
– <b>Power</b> – Power ON indicator	When lit, power is applied to the Mediatrix 1102.

See [“Appendix A - LED Patterns” on page 135](#) for a detailed description of the LED patterns the Mediatrix 1102 may have and the states they represent.

## Rear Connectors

The Mediatrix 1102 has several connections that must be properly set. [Figure 2](#) shows the back panel.

**Figure 2: Back Panel Connectors**



[Table 2](#) describes the back panel connections.

**Table 2: Back Connections of the Mediatrix 1102**

Connection	Description
Network	A 10/100 BaseT Ethernet RJ-45 connector for access to a LAN, WAN or computer. It can also be used as remote power feeding and is IEEE 802.3af compliant and Power DSine certified. It is possible to use either a cross-over or straight Ethernet cable to connect in the <i>Network</i> port. The <i>Network</i> port performs automatic MDI / MDIX detection, meaning that it will adapt to the type of cable connected to it.
Computer	A 10/100 BaseT Ethernet RJ-45 connector that can be connected into the network card of a computer. In this case, the Mediatrix 1102 acts as a small Ethernet switch. It is possible to use either a cross-over or straight Ethernet cable to connect in the <i>Computer</i> port. The <i>Computer</i> port performs automatic MDI / MDIX detection, meaning that it will adapt to the type of cable connected to it.

**Table 2:** Back Connections of the Mediatrix 1102 (Continued)

Connection	Description
Phone/Fax	Two RJ-11 connectors to attach a conventional telephone or G3 fax machine. Note that Port 1 is the leftmost connector. These analog devices feed the signal, either voice or data, to be converted and transmitted to the network.
Power connector	External 24 Vdc wall plug power supply. Note that if the remote power feeding through the <i>Network</i> port is used, this connector is not required.
Default Settings switch	Resets configuration parameters of the Mediatrix 1102 to default (known) values. It can be used to reconfigure the unit.  <b>Warning:</b> Read Section <a href="#">“Using the Default Settings Switch”</a> on page 17 before attempting to reset the unit.

## SNMP

The Mediatrix 1102 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 system) 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:

1. The protocol between the manager and the element, called the *Simple Network Management Protocol (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.
2. 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)*.

3. A *Management Information Base* (MIB) that specifies what variables the network elements maintain (the information that can be queried and set by the manager).

See the *MIB Reference Manual* for more details on the MIB structure and SNMP.

**SNMP Versions** The Mediatrix 1102 supports two (2) versions of SNMP: SNMPv1 and SNMPv2c. SNMP defines a few types of messages that are exchanged between the manager and agent.

### SNMPv1

The following messages are specific to SNMPv1.

**Table 3:** SNMPv1 Message Types

Operator	Description
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.
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 <b>get-request</b> , <b>get-next-request</b> , and <b>set-request</b> operators.
trap	Notify the manager when something happens on the agent.

The first three messages are sent from the manager to the agent, and the last two are from the agent to the manager.

## SNMPv2c

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

**Table 4:** SNMPv2 Message Type

Operator	Description
get-bulk	Contrary to the get-next operation, 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.

### Changing a Parameter Value

Modifying a parameter value involves contacting the Mediatrix 1102 with any SNMP MIB browser. Be sure to use the MIB modules that match the version of those located inside the current software build of the unit.

You can use the built-in MIB browser of the Unit Manager Network. See the *Unit Manager Network Administration Manual* for more details. You can also use the Unit Manager Express, a free MIB browser located on the documentation CD provided with the Mediatrix 1102 unit.

You must locate the proper parameter to modify and change (SET) its value. Most of the parameters require that you reboot the Mediatrix 1102 unit. A reboot may be software-initiated or manually initiated with the *Default Settings* switch or power connector.



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

#### ► To change software variables:

1. Contact the Mediatrix 1102 with a MIB browser.
2. Load the proper MIB.

3. Select the specific variable you want to modify.  
All variables in the MIBs have a description and a list of possible values. Read the comments very carefully before changing a variable's value.
4. Modify the variable according to the proper values listed.
5. Redo steps 3 and 4 for each variable you want to modify.  
Some variables require to reboot the Mediatrix 1102.



This chapter explains the requirements for installing the Mediatrix 1102. It also describes the installation and the initial provisioning of the unit.

## Requirements

The Mediatrix 1102 requires the following items:

**Table 5:** Mediatrix 1102 Required Items

Item	Description
Phone or Fax	A standard telephone or fax attached to an FXS port. You can attach one or two phones or faxes to the Mediatrix 1102.
Remote Termination / Endpoints	Other endpoints on the IP network where the Mediatrix 1102 terminates a call. For instance, it could be: <ul style="list-style-type: none"> <li>• a standard telephone/fax attached to the same Mediatrix 1102, another Mediatrix 1102, or an access device such as a Mediatrix 1104 or Mediatrix 1124</li> <li>• a Soft Phone</li> <li>• an IP phone directly connected to the IP network</li> <li>• etc.</li> </ul>
DHCP Server (optional)	Supplies all network parameters to the Mediatrix 1102 such as the IP address and subnet mask. It is used for automatic configuration.
DNS Server (optional)	Translates domain names into IP addresses.
SIP Server	Manages the active calls of the Mediatrix 1102.
Management Server	Module or software that is used to remotely manage and configure the Mediatrix 1102. Such software could be the Unit Manager Network.
TFTP Server	Necessary for software updates.
Syslog Daemon (optional)	Receives all status messages coming from the Mediatrix 1102. See <a href="#">“Syslog Daemon Configuration” on page 121</a> for more details.

---

## Safety Recommendations

To ensure general safety, follow these guidelines:

- ▶ Do not open or disassemble the Mediatrix 1102.
- ▶ Do not get the Mediatrix 1102 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 1102 package contains the following items:

- ▶ the Mediatrix 1102 unit
- ▶ a power cord for the country in which you will be using the Mediatrix 1102
- ▶ a documentation CD
- ▶ a Quick Start booklet

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

---

## Choosing a Suitable Installation Site

The Mediatrix 1102 is suited for use in an office environment where it can be wall-mounted or free standing.



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

---

When deciding where to position the Mediatrix 1102, ensure that:

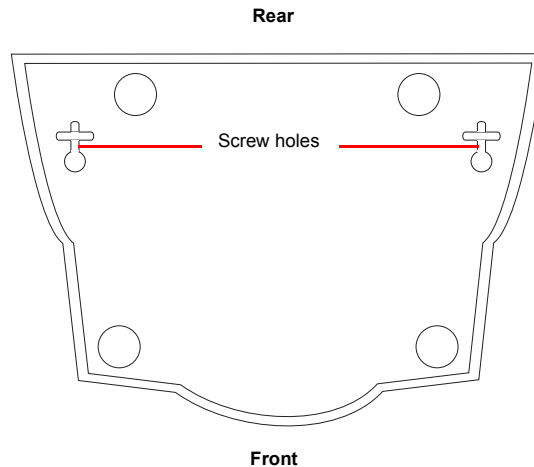
- ▶ The Mediatrix 1102 is accessible and cables can be easily connected.
- ▶ The cabling is away from the following:
  - Sources of electrical noise such as radios, transmitters, and broadband amplifiers
  - Power lines and fluorescent lighting fixtures
  - Water or moisture that could enter the casing of the Mediatrix 1102.
- ▶ The airflow is not restricted around the Mediatrix 1102 or through the vents in the front and back of the unit. The unit requires a minimum of 25 mm (1 in.) clearance.
- ▶ The operating temperature is between 0°C and 40°C.
- ▶ The humidity is not over 85% and is non-condensing.

**Wall-Mounting** The Mediatrix 1102 has two screw holes on its bottom surface, allowing a single unit to be wall-mounted.

► **To wall-mount the Mediatrix 1102:**

1. Disconnect all of the cables from the Mediatrix 1102 before mounting.
2. Ensure that the wall you are using is smooth, flat, dry and sturdy. Attach a piece of plywood, approximately 250 mm x 200 mm x 12 mm (10 inches x 8 inches x 0.5 inches) securely to the wall, if necessary.
3. Position the Mediatrix 1102 against the wall (or plywood) as illustrated in [Figure 3](#).

**Figure 3:** Bottom View - Wall Mounting Screw Holes



You can position the Mediatrix 1102 any way you want. However, Mediatrix Telecom, Inc. recommends that you do not position the unit with its front up, because it may fall down.

4. Mark the position of the screw holes on the wall. Drill the two holes and install two screws.
5. Place the screw holes of the Mediatrix 1102 over the screws installed in the previous step.
6. Connect the network cabling as per ["Connecting the Mediatrix 1102"](#) on page 14.

---

## Connecting the Mediatix 1102

This section describes how to set the connectors of the Mediatix 1102. [Figure 4 on page 15](#) illustrates the connectors that correspond to the steps.



**Warning:** Do not connect the Mediatix 1102 directly to Analog Telephone Systems.

---

### ► To connect the Mediatix 1102 hardware:

1. Connect analog telephones or fax machines into the *Phone/Fax* connectors.

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



**Note:** The Mediatix 1102 telephone line interface has been designed to interface with a conventional telephone line. Connections to certain PBX / Key systems supply a higher line voltage that could damage the Mediatix 1102.

2. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Network* connector of the Mediatix 1102 and 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.

This port can be used as a remote power feeding, IEEE 802.3af compliant and Power DSine certified, if the LAN offers the capability. It is possible to use either a cross-over or straight Ethernet cable to connect in the *Network* port. The *Network* port performs automatic MDI / MDIX detection, meaning that it will adapt to the type of cable connected to it.

3. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Computer* connector of the Mediatix 1102 and connect the other end to the network card of a computer.

In this case, the Mediatix 1102 acts as a small Ethernet switch. Use a standard telecommunication cord with a minimum of 26 AWG wire size. It is possible to use either a cross-over or straight Ethernet cable to connect in the *Computer* port. The *Computer* port performs automatic MDI / MDIX detection, meaning that it will adapt to the type of cable connected to it.

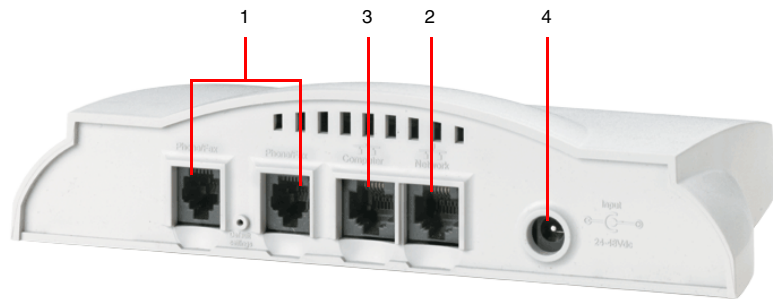
4. Connect the power cord to the Mediatrix 1102 and then connect the other end to an electrical outlet.



**Warning:** The electrical outlet shall be installed near the Mediatrix 1102 so that it is easily accessible.

This step is not required if you are using the LAN-powered option.

**Figure 4:** Steps for Connecting the Mediatrix 1102 Hardware



## First Time Set up

The Mediatrix 1102 default MIB parameters are set so that the unit can be directly plugged into a network and provisioned with a DHCP server. It is strongly recommended to set your DHCP server before installing the unit on the network. See [“Chapter 3 - IP Address and Network Configuration” on page 23](#) for more details.

If you are experiencing problems, or if you do not want to use a DHCP server, you must perform a Recovery Mode procedure, as explained in [“Recovery Mode” on page 18](#).

## Reserving an IP Address

Before connecting the Mediatrix 1102 to the network, Mediatrix Telecom, Inc. strongly suggests that you reserve an IP address in your DHCP server for the unit you are about to connect. This way, you will know the IP address associated to 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 1102 unique identifier is its media access control (MAC) address. The MAC address appears on the label located on the bottom side of the unit. It can also be found in the *sysMgmtMIB* under the *sysMacAddress* variable. You can also dial the following digits on a telephone connected to the Mediatrix 1102:

\*#\*1

The Mediatrix 1102 will then answer back with its MAC address. See [“Special Vocal Features” on page 17](#) for more details.

### Initial Provisioning Sequence

When starting the Mediatrix 1102 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 1102 hardware and connected it to a compatible Ethernet interface that supplies TCP/IP network access (e.g. router, switch, hub or computer). See [“Connecting the Mediatrix 1102” on page 14](#) for more details.



**Note:** The Mediatrix 1102 requests its configuration only on the first boot.

#### ► Initial provisioning sequence:

1. When the Mediatrix 1102 boots, 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 1102 IP address.

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

- Mediatrix 1102 IP address
  - Subnet Mask
  - Default Router IP address
  - Primary DNS IP address
  - Secondary DNS IP address
  - Management Server IP address and port number
  - SIP Servers IP address and port number
3. The Mediatrix 1102 uses the IP address of the Management Server to request its configuration.
  4. The Management Server configures the Mediatrix 1102.

**Special Vocal Features**

When entering special characters on the telephone pad, the Mediatrix 1102 talks back to you with relevant information.

**Table 6:** Special Vocal Features

Digits to Dial	Information Vocally Sent by the Mediatrix 1102
*##*0	Current IP address of the Mediatrix 1102 (static or DHCP).
*##*1	MAC address of the Mediatrix 1102.

**LED Behavior in Boot Mode**

When the Mediatrix 1102 boots and it is not configured to use a DHCP server, it uses static IP addresses. If the static information is not valid, the *Power* and *Ready* LEDs blink at 1 Hz with 75% duty cycle. This lets you know that you must perform a Factory reset or Recovery mode operation. See [“Using the Default Settings Switch” on page 17](#) for more details.

**Using the Default Settings Switch**

The *Default Settings* switch allows you to:

- ▶ cancel an action that was started
- ▶ revert to known factory settings in case the Mediatrix 1102 refuses to work properly for any reason or the connection to the network is lost
- ▶ reconfigure a unit

**At Run-Time**

The *Default Settings* switch can be used at run-time, meaning that you can press the switch while the Mediatrix 1102 is running without powering the unit off. [Table 7](#) describes the actions you can perform in this case.

**Table 7:** Default Settings Button Interaction

Default Settings Button Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	LAN	Power
2 to 5 seconds	Reboots the Mediatrix 1102	No changes are made to the Mediatrix 1102 settings.	Off	Off	Off	Off
5 to 10 seconds	Reboots the Mediatrix 1102 in Recovery Mode	Sets the Mediatrix 1102 IP address to its default value in the MIB and restarts the unit.	Blink	Off	HW	Blink <sup>a</sup>

**Table 7:** Default Settings Button Interaction (Continued)

Default Settings Button Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	LAN	Power
10 to 15 seconds	Reboots the Mediatrix 1102 in Factory Reset Mode	Deletes the persistent MIB values, creates a new configuration file with the default factory values, then restarts the unit.	On	On	On	On

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

**At Boot-Time** The *Default Settings* switch can be used at boot-time, meaning that you power the unit off, then depress the *Default Settings* button and power the unit back on. In this case, the following explains the reset behaviour:

- ▶ Pressing the *Default Settings* switch at startup until the four LEDs start blinking restarts the Mediatrix 1102 in “Recovery Mode”.
- ▶ Pressing the *Default Settings* switch at startup until the four LEDs stop blinking and remain ON applies the “Factory Settings” procedure. This feature reverts the Mediatrix 1102 back to its default factory settings.

See [“Appendix A - LED Patterns” on page 135](#) for a detailed description of the LED patterns related to the *Default Settings* switch.

**Recovery Mode** Using the *Default Settings* switch to trigger the Recovery mode assigns a static default IP address. This assumes you are performing the procedure at run-time.

▶ **To use the *Default Settings* switch to trigger the Recovery Mode:**

1. With a 10/100 Hub and two (2) 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the Hub; one of them is connected into the Network connector of the Mediatrix 1102 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 *Network* connector of the Mediatrix 1102 and connect the other end to your computer.

You must perform the recovery mode in a closed network and perform it on only one Mediatrix 1102 at a time, since the default IP address is the same on every unit.

2. Reconfigure the IP address of your computer to *192.168.0.10* and enter the Subnet Mask of *255.255.255.0*. Reboot the computer.
3. Insert a small paper clip into the *Default Settings* switch hole of the Mediatrix 1102.



**Note:** Hold the *Default Settings* switch between 5 and 10 seconds – until the LEDs start blinking.

---

When releasing the *Default Settings* switch, 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 following parameters is set to **default**, meaning that the default factory settings will be used:

- `localHostConfigSource`
- `imageConfigSource`
- `msConfigSource`
- `syslogConfigSource`

The following variables use their default values in the MIBs:

- `localHostAddress`
- `localHostPrimaryDns`
- `localHostSecondaryDns`
- `localHostDefaultRouter`
- `localHostSnmpPort`
- `localHostSubnetMask`
- `imagePrimaryHost`
- `imagePrimaryPort`
- `imageSecondaryHost`
- `imageSecondaryPort`
- `msHost`
- `msTrapPort`
- `syslogHost`
- `syslogPort`

Please refer to the *MIB Reference Manual* for more details.

All the persistent MIB values are kept.

In this mode, SIP 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.

4. When the Mediatrix 1102 has finished its provisioning sequence, perform the changes you must do, then turn it off, plug it on the network, and turn it on again.

When rebooting, the Mediatrix 1102 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 8](#) for more details.



**Note:** The recovery mode does not alter any persistent configuration data of the Mediatrix 1102.

---

### Factory Settings Mode

Using the *Default Settings* switch to trigger the Factory settings mode reverts the Mediatrix 1102 back to its default factory settings. It deletes the persistent MIB values of the unit and creates a new configuration file with the default factory values. It should be performed with the Mediatrix 1102 connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, the Mediatrix 1102 sends requests indefinitely.

► **To use the *Default Settings* switch to trigger the Factory Settings mode:**

1. Power the Mediatrix 1102 off.
2. Insert a small paper clip into the *Default Settings* switch hole of the Mediatrix 1102. While pressing the *Default Settings* switch, power the unit on.

The electrical outlet shall be installed near the Mediatrix 1102 so that it is easily accessible. Do not depress before the four LEDs stop blinking and are steadily ON.

3. Release the paper clip.

The Mediatrix 1102 restarts.

This procedure resets all variables in the MIB modules to their default value; defaults include the *localHostSelect ConfigSource* variable set to **dhcp**.

When the Mediatrix 1102 has finished its provisioning sequence, it is ready to be used with a DHCP-provided IP address and MIB parameters.



**Note:** The factory default settings mode alters any persistent configuration data of the Mediatrix 1102.

---

## Performing a Software Restart

You can initiate a software restart of the Mediatrix 1102 by using MIB parameters.

### ► To perform a software restart:

1. In the *groupAdminMIB*, locate the *groupAdminMIBObjects* group.  
This group allows you to set the type of restart you want to perform.
2. Set the *groupSetAdmin* variable to the type of restart you want to do:
  - *Locked*: waits for the state of all ports to be locked, then starts the reset. This is called a graceful restart.
  - *ForceLock*: starts the reset immediately. This is called an abrupt restart.
  - *Unlock*: the command is discarded.
3. Set the *groupReset* variable to **SoftReset**.  
The Mediatrix 1102 restarts.

---

## Verifying the Installation

There are two ways to verify that the Mediatrix 1102 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 1102 you want to verify. If the Mediatrix 1102 does not respond, do the following:

- Verify that the LAN cable is securely connected to the

Mediatrix 1102 and to the network connector.

- ▶ Make 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).

# IP Address and Network Configuration

The Mediatrix 1102 must be provisioned with various IP addresses and network parameters to be fully functional. This usually occurs when the Mediatrix 1102 is started for the first time or any time it is restarted. The Mediatrix 1102 can use static addresses as well as addresses 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 the *MIB Reference Manual* 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 Unit Manager Network, the IP addresses are grouped in two distinct folders for easy management.

**Table 8:** 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 will be reflected in the <i>ipAddressStatus</i> folder.

## IP Addresses Formats

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

**Table 9:** IP Addresses Formats

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.	0..9

**Table 9:** IP Addresses Formats (Continued)

Format	Description	Allowed Char.
Hexadecimal	You can enter IP addresses in (base 16) hexadecimal format. Prepending “0x” to the value will instruct the unit to interpret the value 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 your value will instruct the unit to interpret the value 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 will yield the decimal IP address 192.168.0.9. Also, note that IP addresses cannot contain decimal numbers higher than 255.

There may be some confusion between the three available IP address formats. In particular, it is important to understand that prefixing “0” to your values will make 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 1102 IP address information may come from a variety of sources.

**Table 10:** Variable Provisioning Sources

Source	Description
Static	The value is entered by the operator and remains the same every time the Mediatrix 1102 restarts. If the operator does not specify a value, a default static value applies.
DHCP	The value is obtained at boot-time by querying a DHCP server and using standard DHCP fields or options. See <i>RFC 2131</i> section 2 and <i>RFC 2132</i> .

**Table 10:** Variable Provisioning Sources (Continued)

Source	Description
DHCP – Site specific options	The value is obtained at boot-time by querying a DHCP server and using a non-standard option specific to the site where the Mediatrix 1102 is used. See <a href="#">“Site Specific Options” on page 33</a> for more details.
DHCP – Vendor specific options	The value is obtained at boot-time by querying a DHCP server and using a standard option that is reserved for storing vendor specific information. See <a href="#">“Vendor Specific Options” on page 35</a> for more details.
DNS	The value is obtained at boot-time by querying a DNS server.

## Configuring the DHCP Server

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 1102 unique identifier is its media access control (MAC) address. The MAC address appears on the label located on the bottom side of the unit. It can also be found in the *sysMgmtMIB* under the *sysMacAddress* variable. Mediatrix Telecom, Inc. recommends to reserve an IP address with an infinite lease for each Mediatrix 1102 on the network.



**Note:** Mediatrix Telecom, Inc. 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, you must use the Site Specific instead of Vendor Specific information.

### Connection to the DHCP Behavior

When the Mediatrix 1102 boots, it requests a DHCP offer to get its IP addresses and network information. The Mediatrix 1102 waits four (4) seconds before sending another request. The delay between each request is increased exponentially after each request up to a maximum delay of 64 seconds, 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.

As soon as it receives at least one reply, the Mediatrix 1102 stops broadcasting. If the offer is valid, the Mediatrix 1102 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 1102 makes its DHCP request that will be released immediately.

### Network Configuration

**Table 11** lists some of the network options you must configure in the DHCP server:

**Table 11:** 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

## Services

This section describes the services the Mediatrix 1102 uses and their various settings. It also describes the DHCP or Static information you can set.

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

### DHCP or Static Configuration

The configuration your Mediatrix 1102 uses can either be:

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

## DHCP Configuration

Using DHCP-assigned IP addresses ensures that the Mediatrix 1102 receives the addresses that are stored in the DHCP server.

The Mediatrix 1102 can receive numerous information from the DHCP server, including the vendor or site specific information. Note that the Mediatrix 1102 will not make a DHCP request in the following cases:

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

Refer to [“Services” on page 26](#).

## Verifying the DHCP-Assigned IP Addresses

You can query the MIB structure to see the IP addresses that have been assigned to the Mediatrix 1102. Those IP addresses are located under the *ipAddressStatus* folder in read-only variables.

This assumes that you know the local host IP address. There are two ways to get the local host IP address of a Mediatrix unit:

- ▶ Use the autodetect feature of the Unit Manager Network product. Refer to the *Unit Manager Network Administration Manual* for more details.
- ▶ Connect a telephone in the Mediatrix unit, dial “\*#\*0” and listen the IP address that will be given.

## Static Configuration

Using static IP addresses allows you to bypass the DHCP or still be able to use the Mediatrix 1102 if you are not running a DHCP server.

### Local Host

The *ipAddressConfigLocalHost* group is vital to the proper operation of the Mediatrix 1102. If a variable of this group is not properly set, the Mediatrix 1102 may not be able to boot or be contacted after it has booted.

- ▶ **To select the local host configuration source:**
  1. In the *ipAddressConfig* folder, locate the *localHostSelectConfigSource* variable (under the *ipAddressConfigLocalHost* group).

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

**Table 12:** Local Host Variables

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

### FQDN Configuration Source

You can select where to get the Fully Qualified Domain Name (FQDN). The Mediatrix 1102 uses the FQDN to set up information such as the SIP servers.

#### ► To select the FQDN configuration source:

1. In the *ipAddressConfig* folder, locate the *localHostFqdnSelectConfigSource* variable (under the *ipAddressConfigLocalHost* group).

This variable indicates the source to be used for the provisioning of the Mediatrix 1102 FQDN information.

**Table 13:** FQDN Configuration Source

Source	Comment
static	Set the <i>localHostStaticFqdn</i> variable in the <i>ipAddressConfigLocalHostStatic</i> group.
dhcp	The DHCP-provided "host name" (option number 12) is used. No site specific code is provided. The Mediatrix 1102 takes the FQDN in the DHCP offer.
dns	The FQDN is set with the name associated to the host IP address. This DNS may be provided by the DHCP server or taken from the <i>localHostStaticPrimaryDns</i> or <i>localHostStaticSecondaryDns</i> variables.
none	The Mediatrix 1102 uses the host IP address inserted within angle brackets (e.g. [192.168.0.1]).

The default value is **none**.

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

You can see the FQDN value assigned to the Mediatix 1102 in the read-only variable *localHostFqdn* (*ipAddressStatusLocalHost* group).

### SNMP Configuration

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

**Table 14:** SNMP Source

Variable	Default Static Value	DHCP Source
LocalHost SnmpPort	161	N/A

### Image

The *ipAddressConfigImage* group provides the configuration necessary for downloading applications into the Mediatix 1102. This includes emergency downloads in case of repetitive failure to start the main application.

#### ► 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 15:** Image Information Source

Variable	Default Static Value	DHCP Source
imagePrimary Host	"192.168.0.10"	Use option specified in variable <i>imageDhcpPrimarySiteSpecificCode</i> , bytes 0-3.  If not specified (0), use option 43, sub-option 117, bytes 0-3.

**Table 15:** Image Information Source (Continued)

Variable	Default Static Value	DHCP Source
imagePrimary Port	69	Use option specified in variable <i>imageDhcpPrimarySiteSpecific Code</i> , bytes 4-5.  If not specified (0), use option 43, sub-option 117, bytes 4-5. If bytes 4-5 are not present, use the default static value.
imageSecondary Host	"192.168.0.10"	Use option specified in variable <i>imageDhcpSecondarySiteSpecific Code</i> , bytes 0-3.  If not specified (0), use option 43, sub-option 118, bytes 0-3.
imageSecondary Port	69	Use option specified in variable <i>imageDhcpSecondarySiteSpecific Code</i> , bytes 4-5.  If not specified (0), use option 43, sub-option 118, bytes 4-5. If bytes 4-5 are not present, use the default static value.

**Management Server**

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

► **To select the Management Server configuration source:**

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

**Table 16:** Management Server Source

Variable	Default Static Value	DHCP Source
msHost	"192.168.0.10"	Use option specified in variable <i>msDhcpSiteSpecificCode</i> , bytes 0-3.  If not specified (0), use option 43, sub-option 200, bytes 0-3.

**Table 16:** Management Server Source (Continued)

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

**Syslog**

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

► **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 17:** Syslog Source

Variable	Default Static Value	DHCP Source
syslogHost	"192.168.0.10"	Option 7 (first of the list).
syslogPort	514	Not provided by the DHCP, use the default static value.

**SIP Servers**

The *ipAddressConfigSipServer* group provides the configuration necessary for contacting different SIP servers.



**Note:** Although the DHCP option #120 is reserved for SIP servers, no standard currently defines the content and layout of this option.



**Note:** If, for a given server, the host address is a FQDN and the port is 0, then the host and port for this server are obtained through a DNS SRV request.

► **To select the SIP Servers configuration source:**

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

2. Set this variable to either **static** or **dhcp** (vendor/site specific option).

**Table 18:** SIP Servers Source

Variable	Default Static Value	DHCP Source
sipHomeDomainProxyHost	"192.168.0.10"	Use option specified in variable <i>sipHomeDomainProxyDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 204, bytes 0-3
sipHomeDomainProxyPort	0	Use option specified in variable <i>sipHomeDomainProxyDhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 204, bytes 4-5. If bytes 4-5 are not present, use the default static value.
sipOutboundProxyHost	"0.0.0.0"	Use option specified in variable <i>sipOutboundProxyDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 205, bytes 0-3.
sipOutboundProxyPort	0	Use option specified in variable <i>sipOutboundProxyDhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 205, bytes 4-5. If bytes 4-5 are not present, use the default static value.
sipRegistrarHost	"192.168.0.10"	Use option specified in variable <i>sipRegistrarDhcpSiteSpecificCode</i> , bytes 0-3. If not specified (0), use option 43, sub-option 203, bytes 0-3.
sipRegistrarPort	0	Use option specified in variable <i>sipRegistrarDhcpSiteSpecificCode</i> , bytes 4-5. If not specified (0), use option 43, sub-option 203, bytes 4-5. If bytes 4-5 are not present, use the default static value.

**SNTP**

The *ipAddressConfigSntp* group provides the configuration necessary for contacting a NTP/SNTP server.

If you are using a NTP or SNTP server (see [“SNTP Settings” on page 106](#) for more details), a 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 1102 uses *Option 42* to specify the IP address corresponding to server that provides NTP/SNTP (RFC 1769).

► **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 19: 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.

## 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 26](#) 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, you must change the value of the *xxSiteSpecificCode* MIB variables from the default value (0) to the value you will select in the DHCP server. See [“Settings Example” on page 39](#) for an example of vendor specific and site specific settings.

### Site Specific Options

Site specific options are non-standard DHCP options specific to the network where the Mediatrix 1102 is used. You are responsible for allocating an option number (between 128 and 254) for each information element to be stored. See *RFC 2132* section 2 for more details.

Mediatrix units support only one type of information to be stored in site specific options: IP addresses with optional port number. The layout for storing IP addresses is explained in section [“Entering IP Addresses” on page 37](#).

**Figure 5** is an example of site specific option #146, containing address 192.168.0.1.

**Figure 5: 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 your DHCP server. These options must be between 128 and 254. You must then enter the values in the proper MIB variables.

The following describes how to set site specific information in a Windows 2000-based DHCP server. The procedure differs from one DHCP server program to another.

► **To create site specific information:**

1. Open the DHCP.
2. In the console tree, click the applicable DHCP server.
3. Select *Server Options* under the applicable DHCP server.
4. In the *Action* menu, select the *Configure Options* task.
5. Scroll down the list and select the option of your choice.  
You must use only the options in the 128-254 range.
6. Enter the site specific information you want to add.  
You can enter only one information per option. For instance, site specific option 128 may be the Image server information.  
See [“Entering IP Addresses” on page 37](#) for more details on the syntax to use.
7. Repeat steps 4-5 for each information to add, each time selecting a different site specific option number.
8. Click OK when you are done.



**Note:** Be sure to update the MIB variables with the site specific code you have selected.

## 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. Since there are different information elements that can be stored in this option, each element has been allocated a “sub-option” number. See [Table 21 on page 39](#) for the complete list.

Mediatrix Telecom, Inc. vendor specific DHCP options are laid-out in conformance to “Encapsulated vendor-specific options”, as described in *RFC 2131*, section 8.4.

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, len, data). The codes can be anything between 1 and 254, and the vendor, Mediatrix Telecom, Inc., chooses these codes. See [Table 21 on page 39](#) for actual codes.

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

**Figure 6:** General Layout of a Vendor Specific Information Option

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

**Figure 7:** Layout for Encapsulated Vendor Specific Options

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

[Figure 8](#) is an example of a vendor specific option containing an *msHost* IP address (192.168.1.2).

**Figure 8:** Example of Encapsulated Vendor Specific Option

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

Mediatrix units support only one type of information to be stored in vendor specific options: IP addresses with optional port number. The layout for storing IP addresses is explained in section [“Entering IP Addresses” on page 37](#).

The following describes how to set vendor specific information in a Windows 2000-based DHCP server. The procedure differs from one DHCP server program to another.

## Vendor Class ID

When using the vendor specific option, you must first define a Vendor Class ID for the Mediatrix 1102 (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, such as 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 using option code 43 ("[To create vendor specific information:](#)" on page 36), 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.

► **To create a new vendor class:**

1. Open the DHCP.
2. In the console tree, click the applicable DHCP server.
3. On the *Action* menu, click *Define Vendor Classes*.
4. Click *Add*.
5. In *New Class*, type the required information.

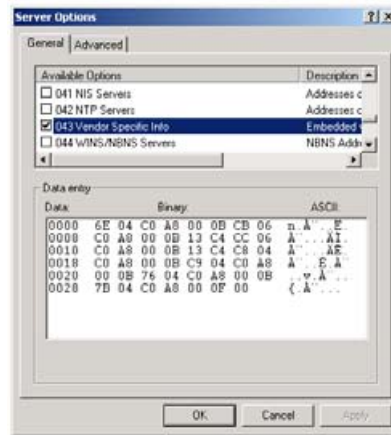
The class to add is *Mediatrix 1102*. You can add it as a binary or ASCII string.

### **Creating Vendor Specific Information**

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

► **To create vendor specific information:**

1. Open the DHCP.
2. In the console tree, click the applicable DHCP server.
3. Select *Server Options* under the applicable DHCP server.
4. In the *Action* menu, select the *Configure Options* task.
5. Scroll down the list and select the *043 Vendor Specific Info* option.

**Figure 9:** Vendor Specific Information

The *Server Options* window lists the current vendor specific information set in the DHCP server.

- Click in the last line entered, then type in the vendor specific information you want to add.

A new line is automatically created. Use one line for each vendor specific information you want to add. You can enter a maximum of 255 characters per line.

See [“Entering IP Addresses” on page 37](#) for more details on the syntax to use.

- When you are done, click *OK*.

The following table lists the vendor specific information you can set in the DHCP server. These codes cannot be modified or the Mediatrix 1102 will not recognize the information.

If the option is not in the DHCP server, the Mediatrix 1102 will use an invalid value (0.0.0.0).

### Entering IP Addresses

In the DHCP server, IP addresses can be entered in decimal, hexadecimal or octal format. See [“IP Addresses” on page 23](#) 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 20:** 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:

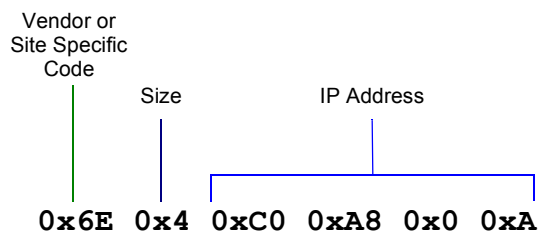
```
[4-6 bytes address]
```

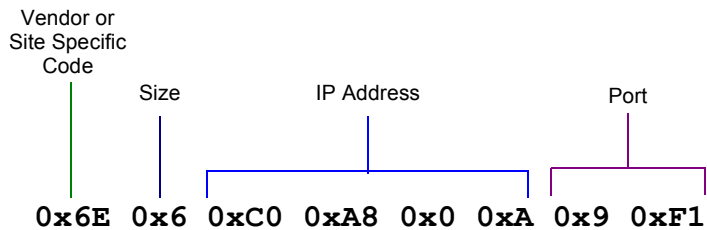
The DHCP server will add the proper code and length in the packet it sends out.

### Example

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

**Figure 10:** Example – Short Address String



**Figure 11:** Example – Long Address String

**Option Codes** This table summarises all vendor specific sub-option codes.

**Table 21:** Sub-Option Codes

Code		Description	Format
Decimal	Hexadec.		
117	0x75	Image Primary Server host (TFTP) address and port.	IP address
118	0x76	Image Secondary Server host (TFTP) address and port.	IP address
200	0xC8	Management Server SNMP Trap host address and port.	IP address
203	0xCB	SIP Registrar host address and port.	IP address
204	0xCC	SIP Home Domain Proxy address and port.	IP address
205	0xCD	SIP Outbound Proxy address and port.	IP address

### 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 22:** 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 23:** 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 24:** 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 DHCP server cannot be contacted, the Mediatrix 1102 performs one of the following actions:

1. Retries contacting the DHCP server until it answers. The Mediatrix 1102 will not reboot.

2. Uses the replacement value from [Table 24 on page 40](#) for all variables that depend on the DHCP.

This assumes that the Mediatrix 1102 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 1102 uses the replacement value from [Table 24 on page 40](#) for each variable that depends on missing vendor/site specific options.

### **DNS Failures**

If the DNS cannot be contacted, the Mediatrix 1102 performs one of the following actions:

1. Retries contacting the DNS until it answers. The retry algorithm is application-specific.
2. Uses the replacement value from [Table 24 on page 40](#) for all variables that depend on the DNS.

---

## **Ethernet Connection Speed**

You can set the speed of the Ethernet connection of the Mediatrix 1102.

### **► To set the Ethernet connection speed:**

1. Contact the Mediatrix 1102 with a MIB browser.  
Be sure to use the MIB files that match the version of the MIB located inside the current software build of the Mediatrix 1102.
2. Locate the *sysConfigInterfaceEthernetSpeed* variable in the *sysConfigMIB*.

The following values are available:

- Auto detect
- 10Mbs-HalfDuplex(1)
- 100Mbs-HalfDuplex(2)
- 10Mbs-FullDuplex(3)
- 100Mbs-FullDuplex(4)

A half-duplex connection refers to a transmission in both directions, but not at the same time, while a full-duplex connection refers to a transmission in both directions simultaneously.

If unknown, set the variable to **Auto detect** so that the Mediatrix 1102 can automatically detect the network speed.

3. Reboot the Mediatrix 1102.



**Note:** Restart the Mediatrix 1102 for the new setting to take effect.

---

This chapter describes how to configure the Mediatrix 1102 for basic operation.

## Configuring the Software

The Mediatrix 1102 software parameters are fully programmable 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 1102.

You can use any third-party SNMP browser or network management application running the SNMP protocol to monitor and configure the Mediatrix 1102. However, the information may not be presented in the same manner depending on the SNMP browser used.



**Note:** It is assumed that you have basic knowledge of TCP/IP network administration.

You can also use the Unit Manager Express, a free MIB browser located on the documentation CD provided with the Mediatrix 1102 unit.

## Network Management

When managing a Mediatrix 1102 over the network, it must be correctly configured with an IP address and a subnet mask.

### IP Addresses

To operate correctly, each unit on a network must have a unique IP address. IP addresses have the format *n.n.n.n* where *n* is a decimal number between 0 and 255, for example, *192.168.0.1*. If your network has a connection to the external IP network, you need to apply for a registered IP address. This system ensures that each IP address is unique; if you do not have a registered IP address, you may be using an address identical to someone else's and your network may not operate correctly.

### Subnets and Using a Subnet Mask

You can divide your IP network into sub-networks or subnets. Support for subnets is important because the number of bits assigned to the device part of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices. Note that if you have a small network (less than 254 devices), you may decide not to have subnets. If you are unsure about what mask to use, Mediatrix Telecom, Inc. suggests to use a general mask, *255.255.255.0*.

- ▶ By using the graphical user interface of the Management Server.

The Management Server could be a product such as the Unit Manager Network. See the *Unit Manager Network Administration Manual* for more details on how to use it to configure any Mediatrix 1102 unit on the network.

Please refer to the *MIB Reference* manual for a complete list of variables that can be set.

### **Sending Configuration Data to the Mediatrix 1102**

The configuration data that must be provisioned into the Mediatrix 1102 can be supplied in two ways:

- ▶ as a configuration file sent from the Management Server to the Mediatrix 1102 via TFTP
- ▶ as a MIB sent from the Management Server to the Mediatrix 1102 via SNMP

### **Configuration File**

The configuration file is the fastest way to deliver the necessary information. This may be important when you must initialize 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 16](#) for more details).

It is also possible to request a configuration file by setting the following two MIB variables in the *sysConfigDownloadConfig* group of the *sysConfigMIB*:

- ▶ *sysConfigDownloadConfigFile* = fileDownload
- ▶ *sysConfigDownloadConfigMode* = request

The Management Server, if properly set up, can send a new configuration file at any time you want. This could be used to update the MIB variables all at the same time. This requires to reboot the Mediatrix 1102.

The configuration file format selected is closely related to the *SNMPMib* package and uses XML (eXtensible Markup Language). The persistence file format uses two different element tags with some attributes.

The first one, *MX\_Config\_File*, provides information about the file being parsed. Its attributes are:

- ▶ **FileId**: a unique user-defined identifier
- ▶ **VersionNumber**: the version of the configuration file format

- ▶ **MIBVersionNumber**: the version of the MIB file (optional)

The second element tag is Object and contains the information that identifies a MIB variable and its value. It uses the attributes *Name*, *Prefix*, *Suffix* and *Value*. The *Name* attribute is a concatenation of the module name and the label of a variable. The *Prefix* and an optional *Suffix* are used to uniquely identify the variable (the suffix is required only for columnar variables). This variable is assigned the value with the *Value* tag.

#### Example of a Configuration File

```
<MX_Config_File VersionNumber="1.0" FileId="ConfigFile">
<Object Name="MX-SYSLOG-MIB_syslogMsgMaxSeverity"
Prefix="1.3.6.1.4.1.4935.15.17.1.5" Suffix="0" Value="5"/>
<Object Name="MX-SYSLOG-MIB_syslogSelectConfigSource"
Prefix="1.3.6.1.4.1.4935.15.1.20.1" Suffix="0" Value="0"/>
<Object Name="MX-SYSLOG-MIB_syslogStaticHost"
Prefix="1.3.6.1.4.1.4935.15.1.20.10.1" Suffix="0"
Value="192.168.1.213"/>
<Object Name="MX-SYSLOG-MIB_syslogStaticPort"
Prefix="1.3.6.1.4.1.4935.15.1.20.10.2" Suffix="0"
Value="514"/>
<Object Name="MX-SYSLOG-MIB_syslogDhcpSiteSpecificCode"
Prefix="1.3.6.1.4.1.4935.15.1.20.30.1" Suffix="0"
Value="0"/>
<Object Name="MX-SYSTEM-CONFIG-
MIB_sysConfigInterfaceEthernetSpeed"
Prefix="1.3.6.1.4.1.4935.15.3.1.10" Suffix="0" Value="0"/>
<Object Name="MX-SYSTEM-CONFIG-
MIB_localHostSelectConfigSource"
Prefix="1.3.6.1.4.1.4935.15.1.1.1" Suffix="0" Value="0"/>
<Object Name="MX-SYSTEM-CONFIG-MIB_localHostStaticAddress"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.1" Suffix="0"
Value="192.168.0.1"/>
<Object Name="MX-SYSTEM-CONFIG-
MIB_localHostStaticPrimaryDns"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.2" Suffix="0"
Value="192.168.0.10"/>
<Object Name="MX-SYSTEM-CONFIG-
MIB_localHostStaticSecondaryDns"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.3" Suffix="0"
Value="192.168.0.10"/>
<Object Name="MX-SYSTEM-CONFIG-
MIB_localHostStaticDefaultRouter"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.4" Suffix="0"
Value="192.168.0.10"/>
<Object Name="MX-SYSTEM-CONFIG-MIB_localHostStaticSnmpPort"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.5" Suffix="0"
Value="161"/>
<Object Name="MX-SYSTEM-CONFIG-
```

```

MIB_localHostStaticSubnetMask"
Prefix="1.3.6.1.4.1.4935.15.1.1.10.6" Suffix="0"
Value="255.255.255.0"/>
<Object Name="MX-TELEPHONY-
MIB_telephonyIpSignalingProtocolSelection"
Prefix="1.3.6.1.4.1.4935.15.25.1.3" Suffix="0" Value="1"/>
<Object Name="MX-TELEPHONY-MIB_telephonyCountrySelection"
Prefix="1.3.6.1.4.1.4935.15.25.1.6" Suffix="0" Value="1"/>
</MX_Config_File>

```

## 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 1102 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.

### Provisioning Sequence

You can change the configuration at will after the initial provisioning and the provisioning system can refresh the Mediatrix 1102 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.

### Restart Handler

The Provisioning Server provides a restart handler, which synchronizes the provisioned data in the Mediatrix 1102 in the event it goes off line and is rebooted again.

## Setting the Location (Country)

It is very important to set variables according to the country in which the Mediatrix 1102 is used because a number of parameter values are set according to this choice. These parameters are:

- ▶ Tones
- ▶ Rings
- ▶ Impedances
- ▶ Line Attenuations

See [“Appendix B - Country Specific Parameters”](#) on page 143 for more information on these country-specific settings.

► **To set a country location:**

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

This variable indicates the current country used by the Mediatrix 1102.

2. Set the variable as follows:
  - North America 1
  - North America 2
  - Austria
  - France
  - Germany 1
  - Germany 2
  - UK
  - Italy
  - Spain
  - Switzerland
  - Sweden
  - Australia 1
  - Australia 2
  - Japan
  - Israel
  - Thailand
  - Indonesia
  - China
  - Hong Kong
  - Malaysia

---

## 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
- ▶ Called Line Identity
- ▶ Reason for Absence of Calling Line Identity
- ▶ Calling Party Name
- ▶ Reason for Absence of Calling Party Name
- ▶ Visual Indicator (MWI)

### **Caller IDs Supported**

A generator to send calling line identification is integrated into the Mediatrix 1102. 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)

DTMF generation units and FSK generation units can be used on different ports at the same time.

### **FSK Generation**

Different countries use different standards to send Caller ID information. The Mediatrix 1102 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

Continuous phase binary FSK modulation is used for coding which is compatible with:

- ▶ BELL 202
- ▶ ITU-T V.23, the most common standard

## Placing a Call

A call can be placed from a phone or fax connected to a Mediatrix 1102 unit. The unit automatically detects if the call originates from a voice or fax transmission and acts accordingly.

When placing a call, the Mediatrix 1102 collects the DTMF digits dialed and sends a message to the Registrar Server. The Registrar Server 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 1102 as you normally do. Please refer to the *Mediatrix 1102 User's Manual* for more information.



This chapter describes how to download the latest software version available on the designated software server into the Mediatrix 1102.

---

## Before Downloading

To download a new software, you must setup the following applications on your computer:

- ▶ TFTP server
- ▶ MIB browser (with the current Mediatrix 1102 MIB tree)  
You can use the Unit Manager Express MIB browser, which is located on the Documentation CD provided with the Mediatrix 1102. See the *Unit Manager Express User's Manual* for more details.
- ▶ Software upgrade zip file
- ▶ Syslog daemon (optional)

## Configuring the TFTP Server

Downloading a new software version into the Mediatrix 1102 requires a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

## Extracting the Zip File

Extract the contents of the zip file that contains the new software information. Be sure to use the defined folder name. It creates a directory that includes the files required for the Mediatrix 1102 to properly update its software.



**Note:** Do not change the name or content of the directory extracted. Mediatrix Telecom, Inc. 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.

---

## DHCP vs. Static Configuration

The Mediatrix 1102 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 1102 through a DHCP server or manually enter them yourself in the static variables.

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

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable (under the *ipAddressConfigImage* group).  
This variable defines whether the Mediatrix 1102 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 25:** Primary Image Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>imageDhcpPrimarySiteSpecificCode</i> variable to <b>0</b> . You must set the DHCP server with the vendor specific code 117 (hexadecimal 0x75).
site specific code	Set the <i>imageDhcpPrimarySiteSpecificCode</i> variable to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

See [“Vendor and Site Specific DHCP Options” on page 33](#) for more details.

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

**Table 26:** Secondary Image Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>imageDhcpSecondarySiteSpecificCode</i> variable to <b>0</b> . You must set the DHCP server with the vendor specific code 118 (hexadecimal 0x76).

**Table 26:** Secondary Image Server DHCP Information (Continued)

To use a...	You must...
site specific code	Set the <i>imageDhcpSecondarySiteSpecificCode</i> variable to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

See [“Vendor and Site Specific DHCP Options”](#) on page 33 for more details.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable.

This variable defines whether the Mediatrix 1102 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 27:** Image Static Information

Variable	Description
<i>imagePrimaryStaticHost</i>	Static primary image server IP address or domain name. <b>Default Value:</b> 192.168.0.10
<i>imagePrimaryStaticPort</i>	Static primary image server IP Port number. <b>Default Value:</b> 69
<i>imageStaticSecondaryHost</i>	Static secondary image server IP address or domain name. <b>Default Value:</b> 192.168.0.10
<i>imageStaticSecondaryPort</i>	Static secondary image server IP Port number. <b>Default Value:</b> 69

## Download Procedure

The download procedure is simple to implement.

### ► To download the latest software:

1. Make sure you are trying to install the latest version of the software.
2. Setup the Image server used to download the software (see [“Before Downloading” on page 51](#)).
3. Contact the Mediatrix 1102 with any SNMP MIB browser.  
Be sure to use the MIB modules that match the version of the MIBs located inside the current software build of the Mediatrix 1102.
4. If the DHCP server did not provide the information to the Mediatrix 1102, configure the *imageStaticPrimaryHost* variable in the *ipAddressConfigImage* group with the current address of the PC that runs the TFTP server.  
For instance, set the variable with a valid IP address such as 192.168.0.2.
5. Locate the *imageMIBObjects* group in the *imageMIB*.  
Configure the *imageLocation* variable with the path, on the remote image server, of the directory that contains the files required for the download (extracted from the zip file).  
You should use the “/” character when defining the path to indicate sub-directories. For instance, *c:/temp/download*.  
However, some TFTP servers on Windows will not recognize the “/” character and produce an error. In this case, you should rather use the “\” character.



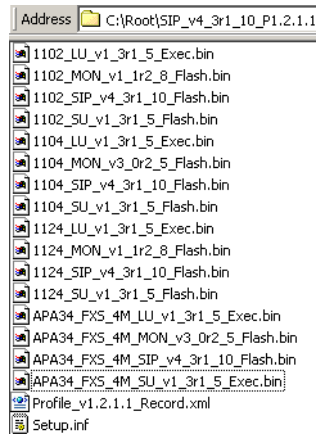
**Note:** This directory must be located under the root path as defined in the TFTP server or the software download will not proceed. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server’s documentation.

Let’s consider the following example:

- The directory that contains the files required for download is called: **SIP\_v4\_3r1\_10\_P1.2.1.1**.
- The download path in the TFTP server is: **C:/Root/**.

The extracted files should then look something like in [Figure 12 on page 55](#):

**Figure 12:** Software Download Files Example



Note that you can define the **C:/Root/** part as you want. The file names may also differ from the example shown above.

6. Set the *groupSetAdmin* variable (in the *groupAdminMIB*) to **ForceLock**.

All activities in progress on the Mediatrix 1102 are terminated immediately and the software upgrade may take place.

7. Initiate the image download by setting the *sysAdmin Command* (in the *sysAdminMIB*) variable to **Download Software**.

This will start the download process.



**Caution:** Never shutdown the Mediatrix 1102 manually while in the download process, because the image may be partially written to the Flash EPROM and the Mediatrix 1102 will be unable to restart.

If you are using a Syslog daemon, you will receive messages that inform you when the update is completed. The LEDs also indicate the completion of the download process. See [“LED States” on page 56](#) for more details.

The Mediatrix 1102 stops responding for a few seconds while the image is written to the Flash EPROM memory, then it reboots automatically.

8. Update the MIB browser with the latest MIB version coming with the download.

**LED States**

When the Mediatix 1102 initiates a software download, the four LEDs located on the front panel are used to report the status of the process:

**Table 28:** LED States in Software Download

Event	LED State
Image downloading	Each LED blinks alternately at 1 Hz with 1/4 ON duty cycle.
Image writing (writing to EEPROM phase)	<i>Ready</i> LED ON, <i>In Use</i> LED ON, <i>LAN</i> LED ON, <i>Power</i> LED OFF. <b>Warning:</b> Do not turn the Mediatix 1102 off while in this state.
Image download failed	All LEDs blink at the same time at 2 Hz with 50% ON duty cycle for 4 seconds.
Image download completed successfully	All LEDs ON.

See ["Appendix A - LED Patterns" on page 135](#) for a detailed description of the LED patterns related to the software download process.

**Emergency Software Procedure**

If the software download is suddenly interrupted, it may not be complete. Without any protection against this situation, the Mediatix 1102 is not functional.

A transfer may be interrupted for the following reasons:

- ▶ An electrical shortage.
- ▶ The user of the Mediatix 1102 can accidentally power off the unit.

In this situation, the emergency software procedure (also called rescue application) automatically starts a new software download.

**Using the Emergency Software**

When the emergency software procedure starts, the following steps apply:

1. The Mediatix 1102 tries to initiate the software download with the primary software server.
2. If the software download fails with the primary software server, the Mediatix 1102 tries to initiate the software download with the secondary software server.

3. If the software download also fails with the secondary software server, the Mediatrix 1102 idles for one (1) minute.
4. After this one (1) minute, the Mediatrix 1102 tries to initiate the software download again.
5. If the software download fails again with the primary and secondary software servers, the Mediatrix 1102 idles for two (2) minutes before trying to initiate the software download.
6. If the emergency software download still fails, the Mediatrix 1102 tries to initiate the software download again by doubling the delay between each try up to a maximum of 16 minutes:
  - first try: 1 minute delay
  - second try: 2 minutes delay
  - third try: 4 minutes delay
  - fourth try: 8 minutes delay
  - fifth try: 16 minutes delay
  - sixth try: 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.



The two ports of the Mediatrix 1102 must be properly unlocked and set in order to work as they should be.

---

## Tables

Most of the variables related to the analog lines (ports) are located in tables. These tables display the information for all ports. Before changing a parameter value, you must build its corresponding table with your MIB browser's table functionality.

---

## Locking/Unlocking Ports

You can independently lock/unlock each port of the Mediatrix 1102.

► **To set basic port properties:**

1. In the *ifAdminMIB*, locate the *ifAdminSetAdmin* variable. This variable locks/unlocks the selected port of the Mediatrix 1102.
2. Set the *ifAdminSetAdmin* variable to **Lock**. The Mediatrix 1102 cancels the port registration to the SIP server when the port is locked and registers the port when it is unlocked.

---

## Setting Voice Information

The variables located in the *voicelfTable* define how to transmit the audio signal.

### Jitter Buffer

The jitter buffer allows better protection against packet loss, but increases the voice delay. If the network to which the Mediatrix 1102 is connected suffers from a high level of congestion, the level of jitter buffer protection should be higher. If the network to which the Mediatrix 1102 is connected suffers from a low level of congestion, the level of jitter buffer protection should be lower.

► **To set Jitter Buffer variables:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Enable the Jitter Buffer protection by setting the *voicelfAdaptiveJitterBufferEnable* variable to **enable**.

3. Define the Jitter Buffer length in the *voicelfTargetJitterBufferLength* variable.

The adaptive jitter buffer attempts to hold packets to the target holding time. This is the minimum delay the jitter buffer adds to the system. The target jitter buffer length is in ms and must be equal to or smaller than the maximum jitter buffer.

Values range from 0 ms to 125 ms. The default value is 30 ms. Values can be changed by increments of 1 ms, but Mediatrix Telecom, Inc. recommends to use multiple of 5 ms.

4. Define the maximum Jitter Buffer length in the *voicelfMaxJitterBufferLength* variable.

This is the maximum jitter the adaptive jitter buffer can handle. The jitter buffer length is in ms and must be equal to or greater than the target jitter buffer.

Values range from 0 ms to 125 ms. The default value is 125 ms. Values can be changed by increments of 1 ms, but Mediatrix Telecom, Inc. recommends to use multiple of 5 ms.

### Voice Activity Detection

The Voice Activity Detection (VAD) enables the Mediatrix 1102 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 lightly affect the voice quality.

If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity).

During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent (c.f. *draft-ietf-avt-rtp-cn-05.txt*).



---

**Note:** G.723 and G.729 VAD is not configurable because it is built-in in the codec, while it is generic in G.711.

---

#### ► To enable Voice Activity Detection:

1. In the *voicelfMIB*, locate the *voicelfTable* group.

2. Define the *voicelfG711VoiceActivityDetectionEnable* variable.

This variable specifies the sensitivity of the VAD algorithm to silence periods. The following settings are available:

**Table 29:** Voice Activity Detection Settings

Variable	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**.

### Echo Cancellation

The Echo cancel control allows to cancel the echo effect caused by signal reflections. An echo is a signal that has been reflected or otherwise returned with sufficient 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.

#### ► To enable the echo cancellation:

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Set the *voicelfEchoCancellationEnable* variable to **enable**.

### Comfort Noise

During silence periods, Comfort Noise (CN) packets containing information about background noise may be received (c.f. *draft-ietf-avt-rtp-cn-05.txt*).

If Comfort Noise Generation (CNG) is enabled, then those packets are used to generate local comfort noise.



**Note:** G.723 and G.729 CNG is not configurable because it is built-in in the codec, while it is generic in G.711.

► **To enable Comfort Noise:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the *voicelfG711ComfortNoiseGenerationEnable* variable.

This variable specifies the type of comfort noise. Changing this variable requires a reboot of the unit in order to take effect.

The following settings are available:

**Table 30:** Comfort Noise Settings

Variable	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.

**User Gain Variables**

The user gain allows you to modify the input and output sound level.



**Caution:** Use these settings with great care, because there are no limits to the sound level range you can use. Mediatrix Telecom, Inc. recommends not to modify the user gain variables unless absolutely necessary, otherwise default calibrations are not valid anymore and some fax or modem tones may not be recognizable anymore.

Using a high user gain may cause sound saturation (the sound is distorted). These parameters also directly affect the fax communication quality and may even prevent a fax to be sent.

The user gain may be used to compensate if there is no available configuration for the country in which the Mediatrix 1102 is located. Since the user gain is in dB, it is easy for you to adjust the loss plan (e.g.: if you need an additional 1 dB for analog to digital, just put 1 for user gain input).

► **To set user gain variables:**

1. In the *voicelfMIB*, locate the *voicelfTable* group.
2. Define the following variables:

**Table 31:** User Gain Variables

Variable	Description
voicelfUserInputGainOffset	User input gain offset in dB (from analog to digital). Values range from -36 dB to +24 dB. However, going above +6 dB may introduce clipping/distorsion depending on the country selected. Under -24 dB, you will not have much signal either. <b>Default Value:</b> 0
voicelfUserOutputGainOffset	User output gain offset in dB (from digital to analog). Values range from -36 dB to +24 dB. However, going above +6 dB may introduce clipping/distorsion depending on the country selected. Under -24 dB, you will not have much signal either. <b>Default Value:</b> 0

## Selecting Codecs

The Mediatrix 1102 supports various codecs for transmitting audio or data signals. These codecs are located in the *voicelfCodecTable* of the *voicelfMIB*. The 2 ports of the Mediatrix 1102 can simultaneously use the same codec (for instance, G.729), or a mix of any of the supported codecs. You must set and enable these codecs for **each** port.

### Voice Codecs

All ports of the Mediatrix 1102 can use one of the available voice codecs.

- G.711 PCMA and PCMU  
Specified in ITU-T Recommendation G.711. Audio data is encoded as 8 bits per sample, after logarithmic scaling. PCMU denotes  $\mu$ -law scaling, PCMA A-law scaling.
- G723.1  
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 for compressing 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.

▶ **G729**

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 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 comfort noise frame occupies 2 octets.

### Setting a Preferred Codec

You can set a preferred codec, which is the codec you want to favour during negotiation.

▶ **To set a preferred codec:**

1. In the *voicelfCodecTable*, locate the *voicelfCodecPreferred* variable.

This variable sets the preferred codec for this port.

2. Choose the codec you want to use from one of the available configurations:
  - pcmu
  - pcma
  - g723
  - g729

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 not enabled, they are not considered.

► **To set voice codecs:**

1. Choose the codec you want to use.

You have the choice between the following codecs:

- PCMU (G.711 u-Law)
- PCMA (G.711 a-Law)
- G.723.1
- G.729.AB

Codecs are enabled by setting the related variable to **enable**. The following codec variables are available:

- voicelfCodecPcmuEnable
- voicelfCodecPcmaEnable
- voicelfCodecG723Enable
- voicelfCodecG729Enable



**Note:** When enabling the G.723 codec, you have the choice between 5.3 kbps or 6.3 kbps.

2. Set other codec options.

[Table 32](#) lists other codec options that can be set.

**Table 32:** Other Codec Options

Variable	Definition	Values (ms)
voicelfCodecPcmuMinPTime	Lower boundary for the packetization period of the given codec. <b>Default Value:</b> 20	10-80, with increments of 1
voicelfCodecPcmuMaxPTime	Upper boundary for the packetization period of the given codec. <b>Default Value:</b> 80	10-80, with increments of 1
voicelfCodecPcmaMinPTime	Lower boundary for the packetization period of the given codec. <b>Default Value:</b> 20	10-80, with increments of 1
voicelfCodecPcmaMaxPTime	Upper boundary for the packetization period of the given codec. <b>Default Value:</b> 80	10-80, with increments of 1
voicelfCodecG723MinPTime	Lower boundary for the packetization period of the given codec. <b>Default Value:</b> 30	30, 60, 90, 120

**Table 32:** Other Codec Options (Continued)

Variable	Definition	Values (ms)
voicelfCodecG723MaxPTime	Upper boundary for the packetization period of the given codec. <b>Default Value:</b> 30	30, 60, 90, 120
voicelfCodecG729MinPTime	Lower boundary for the packetization period of the given codec. <b>Default Value:</b> 10	10-80, with increments of 10
voicelfCodecG729MaxPTime	Upper boundary for the packetization period of the given codec. <b>Default Value:</b> 40	10-80, with increments of 10



**Note:** The packetization time is not negotiated between endpoints, so a minimum and a maximum don't make much sense. The selected value will be the default RTP value (20 ms for G.711 and G.729, 30 ms for G.723) if it's included in the range delimited by the minimum and maximum. Otherwise, it will be the minimum.

- Set the DTMF transport type in the *voicelfDtmfTransport* variable (*voicelfDtmfTransportTable* group).

The following choices are available:

- inBand
- outOfBandUsingRtp
- outOfBandUsingSignalingProtocol

### Data Codecs

All ports of the Mediatrrix 1102 can use one of the available data codecs. You have the choice between the following codecs:

- ▶ Clear Channel Fax
- ▶ T.38

#### ▶ To set data codecs:

- Choose the codec you want to use.

The following codec variables are available:

- dataIfCodecMediaTypeImageEnable*: you have the choice to enable it via PCMA, PCMU, or PCMA/PCMU.

The clear channel codec used is the first one of PCMU or PCMA that is supported in the SDP's

audio media type codec list of both endpoints, or PCMU if none is supported.

- *dataIcfCodecT38Enable*: enabled by setting the variable to **enable**.
2. Set the number of redundancy packets sent with the current packet in the *dataIcfCodecT38ProtectionLevel* variable. Available values range from 1 to 5, 3 being the default value.

---

## Detecting a Current Drop

When a telephone connected to one of the FXS ports is put on-hook, the Mediatrix 1102 signals this by performing a current loop drop. The current loop drop, also referred to as Power Denial mode, is typically used for disconnect supervision. It signals that the remote telephone has been taken on-hook. The Mediatrix 1102 will detect a Current Drop if this signal is maintained for at least 600 ms with an open circuit or has a current drop lower than 0.4 mA.

### Loop Current

You can also set the loop current of the Mediatrix 1102 flowing through the current detector that permits the detection of the on-hook and off-hook states.

► **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.



# Setting SIP Protocol Features

The Mediatrix 1102 uses SIP signalling programs and information defined in a SIP stack to work properly. This includes server addresses, etc.

---

## Setting up SIP Servers

The SIP stack uses three types of servers that have their specific tasks:

- ▶ Registrar server
- ▶ Proxy server
- ▶ Outbound Proxy server

### Registrar Server

The Registrar server accepts REGISTER requests, and places the information it receives in those requests into the location service for the domain it handles.

### DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the Registrar server. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

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

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatrix 1102 must get its SIP Registrar Server configuration through a DHCP Server or not.

2. Set the *sipServerSelectConfigSource* variable to **dhcp**.

You can query the Registrar Server's IP address and port number assigned by the DHCP server in the following read-only variables (under the *ipAddressStatusSipServer* group of the *ipAddressStatus* folder):

- sipRegistrarHost
- sipRegistrarPort

- Set how you want to define the SIP Registrar server information in the DHCP server:

**Table 33:** SIP Registrar Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>sipRegistrarDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to <b>0</b> , which is the default value. You must set the DHCP server with the vendor specific code 203 (hexadecimal 0xCB).
site specific code	Set the <i>sipHomeDomainProxyDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

► **To use static information:**

- In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatrix 1102 must get its SIP Registrar Server configuration through a DHCP Server or not.

- Set the *sipServerSelectConfigSource* variable to **static**.
- Set the following variables:

**Table 34:** SIP Registrar Server Static Address

Variable	Description
<i>sipRegistrarStaticHost</i>	SIP Registrar server static IP address or domain name. <b>Default Value:</b> 192.168.0.10
<i>sipRegistrarStaticPort</i>	SIP Registrar server static IP port number. <b>Default Value:</b> 0

**Proxy Server**

The Proxy server is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is passed on to another entity that can

further process the request. Proxies are also useful for enforcing policy and for firewall traversal. A proxy interprets, and, if necessary, rewrites parts of a request message before forwarding it.

### DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the Proxy server. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

#### ► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatrix 1102 must get its SIP Proxy Server configuration through a DHCP Server or not.

2. Set the *sipServerSelectConfigSource* variable to **dhcp**.

You can query the Proxy Server's IP address and port number assigned by the DHCP server in the following read-only variables (under the *ipAddressStatusSipServer* group of the *ipAddressStatus* folder):

- *sipHomeDomainProxyHost*
- *sipHomeDomainProxyPort*

3. Set how you want to define the SIP Proxy server information in the DHCP server:

**Table 35:** SIP Proxy Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>sipHomeDomainProxyDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to <b>0</b> , which is the default value. You must set the DHCP server with the vendor specific code 204 (hexadecimal 0xCC).
site specific code	Set the <i>sipHomeDomainProxyDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatix 1102 must get its SIP Proxy Server configuration through a DHCP Server or not.

2. Set the *sipServerSelectConfigSource* variable to **static**.
3. Set the following variables:

**Table 36:** SIP Proxy Server Static Address

Variable	Description
sipHomeDomainProxyStatic Host	SIP Proxy server static IP address or domain name. <b>Default Value:</b> 192.168.0.10
sipHomeDomainProxyStatic Port	SIP Proxy server static IP port number. <b>Default Value:</b> 0

### Outbound Proxy Server

A SIP outbound proxy is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. The outbound proxy receives all outbound traffic and forwards it. Incoming traffic may or may not go through the outbound proxy. The outbound proxy's address is never used in the SIP packets, it is only used as a physical network destination for the packets.



**Note:** When the SIP outbound proxy is enabled, the SIP proxy will still be used to create the *To* and the *From* headers, but the packets will physically be sent to the outbound proxy.

The SIP outbound proxy is enabled if the IP address is valid (i.e. not 0.0.0.0). The default static value in the MIB is 0.0.0.0.

► **To disable the SIP outbound proxy:**

1. In the *ipAddressConfig* folder, locate the *sipOutboundProxyStaticHost* variable (under the *ipAddressConfigSipServerStatic* group).

This is the SIP outbound proxy server IP address or domain name.

2. Set this variable to **0.0.0.0**.

To re-enable the SIP outbound proxy, simply enter a valid IP address in the *sipOutboundProxyStaticHost* variable.

### DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the SIP Outbound Proxy. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

#### ► To use DHCP-assigned information:

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatrix 1102 must ask for its SIP outbound proxy settings through a DHCP server or not.

2. Set the *sipServerSelectConfigSource* variable to **dhcp**.

You can query the SIP outbound proxy's IP address and Port number assigned by the DHCP server in the following read-only variables (under the *ipAddressStatusSipServer* group of the *ipAddressStatus* folder):

- *sipOutboundProxyHost*
- *sipOutboundProxyPort*

3. Set how you want to define the SIP Outbound Proxy server information in the DHCP server:

**Table 37:** SIP Outbound Proxy Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>sipOutboundProxyDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to <b>0</b> , which is the default value. You must set the DHCP server with the vendor specific code 205 (hexadecimal 0xCD).
site specific code	Set the <i>sipOutboundProxyDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSipServer</i> group) to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *sipServerSelectConfigSource* variable (under the *ipAddressConfigSipServer* group).

This variable defines whether the Mediatrix 1102 must ask for its SIP outbound proxy settings through a DHCP server or not.

2. Set the *sipServerSelectConfigSource* variable to **static**.
3. Set the following variables:

**Table 38:** SIP Outbound Proxy Static Address

Variable	Description
sipOutboundProxyStaticHost	Static SIP outbound proxy server IP address or domain name. <b>Default Value:</b> 192.168.0.10
sipOutboundProxyStaticPort	Static SIP outbound proxy server IP port number. <b>Default Value:</b> 0

## Defining SIP User Agents

A user agent is a logical entity that can act as both client and server for the duration of a dialog. Each FXS line (also known as endpoint) of the Mediatrix 1102 is defined as a SIP User Agent. You can set information for each SIP User Agent such as its telephone number and friendly name. The user agent information will be used to dynamically create the *To*, *From* and *Contact* headers used in the request sent by the UAC. These headers will make up the Caller ID information that is displayed on telephones/faxes equipped with a proper LCD display. See [“Caller ID Information” on page 47](#) for more details.

Most of the variables related to the SIP user agents are located in tables. Not only can you display and define the information for all ports, but you can also use these tables to create/edit five (5) user names and passwords per port. Before changing a parameter value, you must build its corresponding table with your MIB browser's table functionality. Depending on the MIB browser you are using, the tables may not appear the same way.

► **To set User Agent information:**

1. In the *sipMIB*, set the SIP User Agent port number in the *sipPort* variable.  
The default value is 5060.
2. In the *sipUAIfTable* group, set the following information:

**Table 39:** SIP User Agent Information

Variable	Description
sipUAMainUsername	<p>A string that uniquely identifies this endpoint in the domain, such as a telephone number. This string is used in the creation of the <i>Contact</i> and <i>From</i> headers. The SIP <i>From</i> header carries the permanent location (IP address, home domain) where the endpoint is. The SIP <i>Contact</i> header carries the CURRENT location (IP address) where the endpoint can be reached. Contact headers are used in two ways:</p> <ul style="list-style-type: none"> <li>• First, contacts are registered to the SIP registrar. This enables callers to be redirected to the endpoint's current location.</li> <li>• Second, a contact header is sent along with any requests the UA sends (e.g. : INVITE), and will be used by the target UA as a return address for later requests sent by the target to this endpoint.</li> </ul>
sipUADisplayName	<p>Friendly name for the SIP User Agent. A friendly name or display name contains a descriptive version of the URI, and is intended to be displayed to a user interface.</p>
sipUAOtherAccepted Usernames	<p>A comma-separated list of user names that the endpoint will recognise as its own, but will NOT register in contacts sent to the registrar. Only the username in <i>sipUAMainUsername</i> is registered.</p> <p>This variable can be used to add variations on the main user name. For instance, let's say that the main user name is a telephone number, 555-1111. Variations could be to prefix the local area or country code, such as 819-555-1111.</p> <p>This value can contain multiple user names. These must be separated by a "," character, such as: user1, user2, 5552222, 18195552222.</p>

**Session Timers** The session timer extension allows to detect the premature end of a call caused by a network problem or a peer's failure by resending an INVITE every  $n$  seconds.

A successful response (200 OK) to this INVITE indicates that the peer is still alive and reachable. A time out to this INVITE may mean that there are problems in the signalling path or that the peer is simply not available anymore. In that case, the call will be shut down using normal SIP means.

► **To set Session Timer information:**

1. In the *sipUAIfTable* group, set the session timer maximum expiration delay in the *sipUAMaximumSessionExpirationDelay* variable.

This is the suggested maximum time, in seconds, for the periodical session refreshes. This value is reflected in the Session-Expires header.

2. In the *sipUAIfTable* group, set the session timer minimum expiration delay in the *sipUAMinimumSessionExpirationDelay* variable.

This is the minimum value for the periodical session refreshes. This value is reflected in the Min-SE header.

The Min-SE value is a threshold that no proxy or user agent on the signalling path is allowed to cross.

### **SDP in Session Timer reINVITES**

The reINVITE is sent with the last SDP that was negotiated. Reception of a session timer reinvite should not modify the connection characteristics.

### **Relation Between Minimum and Maximum Values**

A user agent that receives a Session-Expires header whose value is smaller than the minimum it is willing to accept will reply a 422 Timer too low to the INVITE and terminate the call. The phone will not ring.

It is up to the caller to decide what to do when it receives a 422 to its INVITE. Mediatrix units will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the user agent server was ready to accept (located in the Min-SE header). This means that the maximum value as set in the Mediatrix unit might not be followed. This has the advantageous effect of establishing the call even

if the two endpoints have conflicting values. Mediatrix units will also keep retrying as long as they get 422 answers with different Min-SE values.

### Who Refreshes?

Re-sending a session timer INVITE is referred to as refreshing the session. Normally, the user agent server that receives the INVITE has the last word on who refreshes. Mediatrix units will always let the user agent client (caller) do the refreshes if the caller supports session timers. In the case the caller does not support session timers, the Mediatrix unit will assume the role of the refresher.

### Disabling the Service

To disable the session timer service, set the maximum session timer expiration value to 0.

Increasing the maximum will help to reduce network traffic, but will also make “dead” calls longer to detect.

## Authentication Information

Authentication information allows you to add some level of security to the Mediatrix 1102 lines by setting user names and passwords.

You can add two types of authentication information:

- ▶ port-specific authentication
- ▶ unit authentication

When authentication is requested from a realm, the port-specific authentication is tried first, then the unit authentication if required.

### Port-Specific Authentication

You can define five (5) user names and five (5) passwords for each port of the Mediatrix 1102. A port can thus register with five different realms.

**Table 40:** Port-Specific Authentication

Variable	Description
sipUAAuthRealm	When authentication informations are required from users, the realm identifies who requested the information.
sipUAAuthUsername	A string that uniquely identifies this endpoint in the realm, used for authentication purposes. The user name always maps to a password.
sipUAAuthPassword	User password.

## Unit Authentication

You can define five (5) user names and five (5) passwords for the Mediatrix 1102. These user names and passwords thus apply to all ports of the unit.

**Table 41:** Unit-Specific Authentication

Variable	Description
sipUnitAuthRealm	When authentication informations are required from users, the realm identifies who requested the information.
sipUnitAuthUsername	A string that uniquely identifies this endpoint in the realm, used for authentication purposes. The user name always maps to a password.
sipUnitAuthPassword	User password.

## Setting up the Urgent Gateway Information

The Urgent Gateway service allows a “911”-style service. A string to dial in case of emergency can be configured. As soon as this string is dialed, an INVITE will be sent, addressed to the “urgent gateway”. This will also bypass the outbound proxy.

### ► To enable the urgent gateway:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesUrgentGatewayEnable* variable (under the *telephonyServicesUrgentGatewayCustomization* group).

This variable sets the usage state of the urgent gateway. Urgent messages bypass the outbound proxy and go directly to the urgent gateway.

2. Define the digits that users will have to dial to start the urgent gateway call feature in the *telephonyServicesUrgentGatewayDigitMap* variable.

For instance, you could decide to put “\*60” as the sequence a user must dial to start the urgent gateway service. This sequence must respect the syntax for digit maps (see [“Using Digit Maps” on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service’s status is “enabled”.

The activating sequence is set for all the ports of the Mediatrix 1102. You cannot have different sequences for each port.

3. Set the number to reach in case of an urgent call in the *telephonyServicesUrgentGatewayTargetAddress* variable.

Accepted formats are:

- phone numbers (5551111)
- strings of type “scheme:user@host” (such as SipUrls). For instance, “sip:user@foo.com”.

Note that this string will be used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

---

## Using a NAT Fire-wall

The Mediatrix 1102 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 the NAT (Name Address Translation) technology.



**Note:** This feature is currently located under the *mediatrix Experimental* branch of the MIB structure. Mediatrix Telecom, Inc. configuration tools (such as the Unit Manager Network or Unit Manager Express) do not support MIBs located under the *mediatrixExperimental* branch. Even though experimental MIBs can be viewed with these configuration tools, SNMP operations may not work properly on them.

---

The Mediatrix 1102 uses two methods to work with NAT technology:

- ▶ Configure the Mediatrix 1102 with the public IP address of the NAT system.
- ▶ Instruct the NAT/Firewall traversal scheme to send periodic messages to the server indicating that the

## Network Address Translation

Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address.

NAT automatically provides firewall-style protection without any special set-up. That is because it only allows connections that are originated on the inside network. This means, for example, that an internal client can connect to an outside FTP server, but an outside client will not be able to connect to an internal FTP server because it would have to originate the connection, and NAT will not allow that.

Mediatrrix 1102 is located behind a NAT/Firewall system.



**Note:** These are two separate methods to work with NAT technology. Mediatrrix Telecom, Inc. recommends to use one or the other, but not both.

### Method 1: NAT/ Firewall Public IP Address

In this case, you can configure the Mediatrrix 1102 with the public IP address of the NAT system, which allows to reach the Mediatrrix 1102. SIP packets sent by the Mediatrrix 1102 will contain the NAT address configured as SIP contact. If the NAT firewall service is not activated, the real IP address of the Mediatrrix 1102 is rather used.

#### ► To activate the NAT Firewall service:

1. In the *natSipMIB*, locate the *natSipCustomEnable* variable (under the *natSipCustom* group).
2. Set the *natSipCustomEnable* variable to **Enable**.
3. Locate the *natSipCustomPublicAddress* variable.  
This is the public IP address used as Contact address by outgoing SIP packets crossing a NAT system.
4. Enter the public IP address of the NAT firewall.

### Method 2: NAT Traversal Scheme

In this case, the NAT traversal scheme inserts a “Proxy-Require” line in the header to indicate to the server that the Mediatrrix 1102 is located behind a NAT/Firewall (as defined in *draft-sen-midcom-fw-nat-00.txt*). The NAT traversal scheme sends requests to the server at regular intervals to keep the connection to the server open during the call. Otherwise it could be possible that no signalling packets are exchanged between the parties and that the firewall decides to close the connection. Voice packets cannot be used to keep the connection open because they are transmitted on another channel.



**Note:** This feature is used under licence from Nortel Networks Inc.

#### ► To enable the NAT Scheme:

1. In the *natSipMIB*, locate the *natSipNortelPingTimeout* variable (under the *natSipNortelPing* group).  
This variable defines the PING request refresh timeout in seconds. This interval must be smaller than the timeout of the Firewall used.

2. Set the *natSipNortelPingTimeout* variable.  
Set the variable to 0 if you want to disable this service.

---

## Setting Interop Parameters

You can set three parameters to control how the Mediatrix 1102 interoperates with other vendor's products and older Mediatrix units:

- ▶ Call transfer (Replaces) capability
- ▶ SIP Transfer version supported
- ▶ Session timers version supported
- ▶ Transmission timeout



**Note:** These features are currently located under the *mediatrix Experimental* branch of the MIB structure. Mediatrix Telecom, Inc. configuration tools (such as the Unit Manager Network or Unit Manager Express) do not support MIBs located under the *mediatrixExperimental* branch. Even though experimental MIBs can be viewed with these configuration tools, SNMP operations may not work properly on them.

---

## Replaces Configuration Setting

The Mediatrix 1102 allows you to configure the use of the *Replaces* header mechanism used in a transfer. When supported by the target of the transfer, the *Replaces* header mechanism ensures a more seamless transfer by permitting the initiating party to effectively replace a current call by another instead of disconnecting the call to be replaced and creating a second call.

▶ **To set Replaces configuration:**

1. In the *sipInteropMIB*, set the Replaces configuration in the *sipReplacesConfig* variable.

You have the following choices:

- *doNotUseReplaces*: The *Replaces* header is not used.
- *useReplacesWithRequire*: The *Replaces* header is used. It can be seen in the *Refer-To* header found in the REFER request sent by the transferor. It can also be seen in the INVITE sent by the transferee. The target that supports *Replaces* will use its information to merge the new INVITE with an existing call specified in the *Replaces* header.

The transferee will require the use of the replaces extension for proper completion of the transfer. If the replaces extension is not supported by the target of the transfer, the unit will go into a fallback algorithm to retry the transfer using replaces, by reversing the roles of the target and the transferee (by resending the REFER to the initial target instead of the initial transferee). As a last resort (if none of the participants supports replaces), the transfer will be carried out without using the replaces extension.

- *useReplacesNoRequire*: The *Replaces* header is used. It can be seen in the *Refer-To* header found in the REFER request sent by the transferor. It also can be seen in the INVITE sent by the transferee. The target that supports Replaces will use its information to merge the new INVITE with an existing call specified in the *Replaces* header.

This will disable the transfer fallback. The replaces information will still be present, but no check will be made that it is effectively used to complete the transfer.

### SIP Transfer Version

You can select the version of the transfer draft that the Mediatrix 1102 will use. The provisioned version is used for initiating transfers and receiving them. Transfer versions other than those provisioned will not work.

▶ transfer02

The Mediatrix 1102 will execute transfers using the methods described in the now expired *draft-ietf-sip-cc-transfer-02.txt*. This draft was obsoleted. Its use is deprecated and this setting should be used for backward compatibility issues only.

▶ transfer05UsingRefer02

The Mediatrix 1102 will execute transfers using the methods described in the more recent *draft-ietf-sip-cc-transfer-05.txt*. This draft version contains several enhancements over the previous ones. Among others, it is possible to use the replaces header to provide a more seamless attended transfer to the user. This method also uses *draft-ietf-sip-refer-02.txt*. This setting should be used if you do not need to interop with transfer02-enabled parties.

► **To set the version of transfer supported:**

1. In the *sipInteropMIB*, locate the *sipInteropTransferVersion* variable.
2. Set the version to support.
  - transfer02
  - transfer05UsingRefer02

**Session Timers Version**

You can select the version of the session timer draft that the Mediatix 1102 will use. Session timer versions other than those provisioned may not work because of backward compatibility issues between the versions.

► sessionTimer04:

The Mediatix 1102 will use the session timer extension as described in the now expired *draft-ietf-sip-session-timer-04.txt*. This draft was obsoleted. Its use is deprecated and this setting should be used for backward compatibility issues only.

► sessionTimer08:

The Mediatix 1102 will use the session timer extension as described in the more recent *draft-ietf-sip-session-timer-08.txt*. This draft version contains several enhancements over the previous ones, including the use of the Min-SE header. This setting should be used if you do not need to interoperate with session timer v4-enabled parties.

See [“Session Timers” on page 76](#) for more details.

► **To set the version of session timers supported:**

1. In the *sipInteropMIB*, locate the *sipInteropSessionTimersVersion* variable.
2. Set the version to support.
  - sessionTimer04
  - sessionTimer08

**Transmission Timeout**

If a DNS SRV answer contains more than one entry, the Mediatix 1102 will try these entries if the entry initially selected does not work. You can configure the maximum time, in seconds, to spend waiting for answers to messages, from a single source. Retransmissions still follow the algorithm proposed in *RFC2543bis*, but the total wait time can be overridden by using this feature.

For example, if you are using DNS SRV and more than one entries are present, this timeout will be the time it takes before trying the second entry.

► **To set the transmission timeout:**

1. In the *sipInteropMIB*, locate the *sipInteropTransmissionTimeout* variable.
2. Set the timeout value.  
Available values are from 1 to 32 seconds.

# Telephony Configuration

This chapter explains how to set the telephony variables of the Mediatrix 1102, i.e. the way the unit handles calls.

## Using Digit Maps

A Digit Map allows you to compare the number users just dialed to a string of arguments. If they match, users will be able to make the call. If not, users will not be able to make the call and will get a busy signal. It is thus essential to define very precisely a Digit Map before actually implementing it, or your users may encounter calling problems.

Because the Mediatrix 1102 cannot predict how many digits it needs to accumulate before transmission, you could use the Digit Map, for instance, to determine exactly when there are sufficient digits entered from the user to place a call.

The permitted digit map syntax is taken from the core MGCP specification, RFC2705: <ftp://ftp.isi.edu/in-notes/rfc2705.txt>, section 3.4.

For instance, using the phone on your desk, you can dial the following numbers:

**Table 42:** Number Examples

Number	Description
0	Local operator
00	Long distance operator
xxxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
91xxxxxxxxxx	Long distance numbers
9011 + up to 15 digits	International number

The solution to this problem is to load the Mediatrix 1102 with a Digit Map that corresponds to the dial plan. This Digit Map is expressed using a specific syntax.

A Mediatrix 1102 that detects digits or timers applies the current dial string to the Digit Map, attempting a match to each regular expression in the Digit Map in lexical order.

- ▶ If the result is under-qualified (partially matches at least

one entry in the Digit Map), waits for more digits.

- ▶ If the result matches, dials the number.
- ▶ If the result is over-qualified (i.e. no further digits could possibly produce a match), sends a fast busy signal.

### Special Characters

Digit Maps use specific characters and digits in a particular syntax. Those characters are:

**Table 43:** Digit Map Characters

Character	Use
Digits (0, 1, 2... 9)	Indicates specific digits in a telephone number expression.
T	The Timer indicates that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the SIP Server can make the call.
x	Matches any digit, excluding “#” and “*”.
	Indicates a choice of matching expressions (OR).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
[	Indicates the start of a range of characters.
]	Indicates the end of a range of characters.

### How to Use a Digit Map

Let’s say you are in an office and you want to call a co-worker’s 3-digits extension. You could build a Digit Map that says “after the user has entered 3 digits, make the call”. The Digit Map could look as follows:

xxx

This Digit Map specifies that after the user has entered any three digits, the call is placed. You could refine this Digit Map by including a range of digits. For instance, you know that all extensions in your company either begin with 2, 3, or 4. The corresponding Digit Map could look as follows:

[2-4]xx

You have just entered a range of digit. Thus, if the number you dial begins by anything other than 2, 3, or 4, the call will not be placed and you will get a busy signal. Another way to achieve the same result would be:

[234]xx

## Combining Several Expressions in a Digit Map

It is possible to combine two or more expressions in the same Digit Map by using the “|” operator, which is equivalent to OR.

Let’s say you want to specify a choice: the Digit Map is to check if the number is internal (extension), or external (a local call). Assuming that you must first dial “9” to make an external call, you could define a Digit Map as follows:

```
( [2-4] xx | 9 [2-9] xxxxxxxx )
```

The Digit Map checks if:

- ▶ the number begins with 2, 3, or 4 **and**
- ▶ the number has 3 digits

If not, it checks if:

- ▶ the number begins with 9 **and**
- ▶ the second digit is any digit between 2 and 9 **and**
- ▶ the number has 7 digits



**Note:** The Digit map must be enclosed in parenthesis when using the “|” option.

## Using the # and \* Characters

It may sometimes be required that users dial the “#” or “\*” to make calls. This can be easily incorporated in a Digit Map:

```
xxxxxxx#  
xxxxxxx*
```

The “#” or “\*” character could indicate users must dial the “#” or “\*” character at the end of their number to indicate it is complete.



**Note:** You can specify to remove the “#” or “\*” found at the end of a dialed number. See [“Setting up Digit Maps” on page 88](#).

## Using the Timer

The Timer is set at 4 seconds. It indicates that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the Mediatrix 1102 can make the call. A Digit Map for this could be:

---

[2-9]xxxxxxT

---



**Note:** When making the actual call and dialing the number, the Mediatrix 1102 automatically removes the “T” found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only.

---

### Using a Digit Map for Calls Outside the Country

If your users are making calls outside your country, it may sometimes be hard to determine exactly the number of digits they will have to enter. You could devise a Digit Map that takes this problem into account:

001x.T

Where the Digit Map looks for a number that begins with 001, then any number of digits after that (x.).

### Example

[Table 42 on page 85](#) outlined various call types one could make. All these possibilities could be covered in one Digit Map:

(0T|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|91xxxxxxxxxx|9011x.T)

### Validating a Digit Map

If you enter a Digit Map expression, the Mediatrix 1102 will validate the Digit Map and indicate if it is correct or not.

---

## Setting up Digit Maps

The variables related to the digit maps are located in tables. You can create/edit ten (10) digit maps for each Mediatrix 1102. Before changing a parameter value, you must build its corresponding table with your MIB browser’s table functionality. Depending on the MIB browser you are using, the tables may not appear the same way.

Digit Map rules are checked sequentially. If a phone number potentially matches two of the rules, the first rule encountered will be applied.

Each of these Digit Map rules has six (6) specific variables that you must define for the Digit Map to work properly.

**Table 44:** Digit Map Rules Variables

Variable	Description
digitMapAllowed Enable	<p>If enabled, this digit map will be recognised and accepted only if it is also valid. If disabled, this digit map will not be recognised. Possible values are:</p> <ul style="list-style-type: none"> <li>• disable (0)</li> <li>• enable (1)</li> </ul> <p><b>Default Value:</b> enable</p>
digitMapAllowed DigitMap	<p>The actual digit map string that will be considered valid when dialed. The string must be declared with the syntax described in <a href="#">“Using Digit Maps” on page 85</a>.</p> <p><b>Default Value:</b> x.T</p>
digitMapAllowedIs Valid	<p>The Mediatix 1102 validates the digit map after a SNMP set. The result (valid, invalid) is displayed.</p>
digitMapPrefixed DigitRemovalCount	<p>The amount of digits to remove from the beginning of the dialed number, after dialing, but before initiating the call. For instance, when dialing “1-819-xxx-xxxx”, specifying a value of “4” would mean that the call is started using the number “xxx-xxxx”.</p> <p><b>Note:</b> This rule is applied BEFORE applying both <i>digitMapSuffixStringToRemove</i> and <i>digitMapPrependedString</i>.</p> <p><b>Default Value:</b> 0</p>
digitMapPrepended String	<p>A string to insert at the beginning of the dialed number before initiating the call. This string is added after executing the operation required by the <i>digitMapPrefixedDigitRemovalCount</i> variable.</p> <p>For instance, let’s say that you need to dial a special digit, “9”, for all local calls. Dialing “xxx-xxxx” with a value of “9” would yield “9-xxx-xxxx” as the number with which to initiate the call.</p> <p><b>Note:</b> This rule is applied AFTER applying both <i>digitMapPrefixedDigitRemovalCount</i> and <i>digitMapSuffixStringToRemove</i>.</p>

**Table 44:** Digit Map Rules Variables (Continued)

Variable	Description
digitMapSuffix StringToRemove	<p>A string to look for and remove, from the end of the dialed number. This can be especially helpful if one of the digit maps contains a terminating character that must not be dialed.</p> <p>For instance, let's take a digit map such as "25#" in which the "#" signals that the user has finished entering digits. If you want to remove the "#", simply specify "#" in this variable and the resulting number will be "25".</p> <p><b>Note:</b> This rule is applied AFTER applying <i>digitMapPrefixedDigitRemovalCount</i> but BEFORE applying <i>digitMapPrependedString</i>.</p>

### Using Refused Digit Maps

A refused digit map may be defined to restrict your users to call specific numbers; for instance you want to accept all 1-8xx numbers except 1-801. You can create/edit ten (10) refused digit maps per port.

The refused digit map variables are located in the *digitMapRefusedTable* of the *digitMapMIB*.

**Table 45:** Refused Digit Map Variables

Variable	Description
digitMapRefusedEnable	<p>If enabled, this digit map will be recognised and refused only if it is also valid. If disabled, this digit map will not be recognised. Possible values are:</p> <ul style="list-style-type: none"> <li>• disable (0)</li> <li>• enable (1)</li> </ul> <p><b>Default Value:</b> disable</p>
digitMapRefusedDigitMap	<p>A string making up a digit map that will be considered invalid when dialed. The string must be declared with the syntax described in <a href="#">"Using Digit Maps" on page 85</a>.</p>
digitMapRefusedIsValid	<p>Diagnosis of the string entered in <i>digitMapRefusedDigitMap</i>. Possible values are:</p> <ul style="list-style-type: none"> <li>• invalid (0)</li> <li>• valid (1)</li> </ul>

## Digit Map Examples

The following examples will help you set up various scenarios that could apply to your situation. You can use up to ten (10) Digit Map rules for each Mediatrix 1102. Each time a user dials a digit, the number is compared to the rules and, if there is a match, the number is dialed.

### Example 1 – Standard Calls

Let's say you are located in Seattle, Washington and you want to define Digit Map rules for your users. You must consider at least four possibilities:

- ▶ You are making a long distance call outside the country.
- ▶ You are making a long distance call outside your area code.
- ▶ You are making a local call outside your area code (in the 425 area code).
- ▶ You are making a local call in the same area code.

### Digit Map Rule #1

This Digit Map rule checks for calls outside the country.

**Table 46:** Digit Map Rules #1 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	011x.# 001x.T
digitMapPrefixedDigitRemoval Count	3 A valid telephone number must contain a country code, an area code, and a number – the "011" part is thus not required.

### Digit Map Rule #2

This Digit Map rule checks for long distance calls outside your area code.

**Table 47:** Digit Map Rules #2 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	1xxxxxxxxx

**Table 47:** Digit Map Rules #2 Settings (Continued)

Variable	Setting
digitMapPrefixedDigitRemovalCount	1 The first digit "1" in the digit map indicates a user wants to call outside his/her own area code. It has to be removed because it does not need to be expressed to the SIP Server. The SIP Server needs only to know the complete number of the called party (CC+AC+directory number).
digitMapPrependedString	1 (country code) A valid telephone number must contain a country code, an area code, and a number. The country code is missing in this number and must be added. Note that in this scenario, the country code is the same code as the code used when the user wants to indicate a communication outside of his/her own area code. It is still good practice to have this number removed and to add the country code, event if these two numbers are the same.

**Digit Map Rule #3**

This Digit Map rule checks for local calls outside your area code (in the 425 Area Code).

**Table 48:** Digit Map Rules #3 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	425xxxxxx
digitMapPrependedString	1 (country code) A valid telephone number must contain a country code, an area code, and a number. The country code is missing in this number and must be added.

### Digit Map Rule #4

This Digit Map rule checks for local calls in the same area code.

**Table 49:** Digit Map Rules #4 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	([235-9]xxxxxx 45[1-9]xxxx 4[0-469]xxxx)
digitMapPrependedString	1206 (country code and area code) A valid telephone number must contain a country code, an area code, and a number. The country code and area code are missing in this number and must be added.

You could further refine these Digit Maps according to your needs. Experiment with Digit Maps.

#### Example 2 – PBX Emulation

Let's say you are located in the 819 area code. You are in an office where you must dial:

- ▶ 3 numbers to call one of your co-workers.
- ▶ 9 to get an external line.

The following four possibilities are considered:

- ▶ You are making an internal call to one of your co-workers.
- ▶ You are making a long distance call outside the country.
- ▶ You are making a long distance call outside your area code.
- ▶ You are making a local call in the same area code.

### Digit Map Rule #1

This Digit Map rule checks for internal calls.

**Table 50:** Digit Map Rules #1 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	[1-8]xx

### Digit Map Rule #2

This Digit Map rule checks for calls outside the country.

**Table 51:** Digit Map Rules #2 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	(9011x.# 9011x.T)
digitMapPrefixedDigitRemovalCount	4 A valid telephone number must contain a country code, an area code, and a number and the "9011" part is thus not required.

### Digit Map Rule #3

This Digit Map rule checks for long distance calls outside your area code.

**Table 52:** Digit Map Rules #3 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	91xxxxxxxxxx
digitMapPrefixedDigitRemovalCount	2 The first digit "9" in the digit map indicates a user wants to make an external call, while the second digit "1" indicates a user wants to call outside his/her own area code (in North America). The two digits must be removed because they do not need to be expressed to the SIP Server. The SIP Server needs only to know the complete number of the called party (CC+AC+directory number).

**Table 52:** Digit Map Rules #3 Settings (Continued)

Variable	Setting
digitMapPrependedString	<p>1 (country code)</p> <p>A valid telephone number must contain a country code, an area code, and a number. The country code is missing in this number and must be added.</p> <p>Note that in this scenario, the country code is the same code as the code used when the user wants to indicate a communication outside of his/her own area code. It is still good practice to have this number removed and to add the country code, event if these two numbers are the same.</p>

**Digit Map Rule #4**

This Digit Map rule checks for local calls in the same area code.

**Table 53:** Digit Map Rules #4 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	9[2-8]xxxxxx
digitMapPrefixedDigitRemovalCount	<p>1</p> <p>The first digit “9” in the digit map indicates a user wants to make an external call. It has to be removed because it does not need to be expressed to the SIP Server. The SIP Server needs only to know the complete number of the called party (CC+AC+directory number).</p>
digitMapPrependedString	<p>1819 (country code and area code)</p> <p>A valid telephone number must contain a country code, an area code, and a number. The country code and area code are missing in this number and must be added.</p>

You could further refine these Digit Maps according to your needs. Experiment with Digit Maps.

## Supplementary Telephony Services

The Mediatrix 1102 offers telephony services one can use directly on his/her phone. However, you must set these services before they can be used.

Most of the variables related to the telephony services are located in tables. These tables display the information for all ports. Before changing a parameter value, you must build its corresponding table with your MIB browser's table functionality.

### Call Hold

The Call Hold service allows the user to temporarily put an existing call on hold, usually by using the "flash" button of the telephone. The user can resume the call in the same way.

This service has no dependencies on other services being enabled, but it must be enabled for the following services to work properly:

- ▶ Call Waiting
- ▶ Second Call
- ▶ Blind Transfer
- ▶ Attended Transfer
- ▶ Conference

Please refer to the *Mediatrix 1102 User's Manual* for more details on how to use this feature.

#### ▶ To enable the call hold service:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.
2. Enable the Call Hold by setting the *telephonyServicesHoldEnable* variable to **enable**.

Since the Call Hold variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesHoldStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

### Call Forward

The Call Forward feature offers various ways to forward calls:

- ▶ Unconditional
- ▶ On Busy
- ▶ On No Answer

## Unconditional

The Call Forward – Unconditional feature allows users to forward their calls to another extension or line.

Please refer to the *Mediatrix 1102 User's Manual* for more details on how to use this feature.

### ► To set the Call Forward Unconditional feature:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesCallForwardUnconditionnal* group.

This group contains all of the variables required to set the Call Forward Unconditional feature.

2. Enable the Call Forward Unconditional by setting the *telephonyServicesCallForwardUnconditionnalEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

3. Define the address to which incoming calls will be forwarded in the *telephonyServicesCallForwardUnconditionnalForwardingAddress* variable.

This string represents the address or telephone number that the user wants to forward calls to. Accepted formats are:

- phone numbers (5551111)
- "scheme:user@host" type strings (such as SipUrls). For instance, "sip:user@foo.com".

Note that this string will be used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

Since this variable is located in a table, you can have a different string for each port.

4. Define the digits that users will have to dial to start the Call Forward Unconditional feature in the *telephonyServicesCallForwardUnconditionnalEnableDigitMap* variable.

For instance, you could decide to put "\*70" as the sequence a user must dial to activate the Call Forward Unconditional service. This sequence must be unique and follow the syntax for digit maps (see ["Using Digit Maps" on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service' status is "enabled". This value must also be different from the value set in Step 5.

The activating sequence is set for all the ports of the Mediatrix 1102. You cannot have a different sequence for each port.



**Note:** The status of the service as set by the users is kept in the *telephonyServicesCallForwardUnconditionnalStatus* variable (in the *telephonyServicesIfCallForwardUnconditionnalStatusTable*). For instance, if a user has started the service on his/her phone and the Mediatrix 1102 reboots for any reason, the unit will use the status kept in this variable and restore the service to “active”. This way, the user does not have to remember to restart the service.

5. Define the digits that users will have to dial to stop the Call Forward Unconditional feature in the *telephonyServicesCallForwardUnconditionnalDisableDigitMap* variable.

For instance, you could decide to put “\*71” as the sequence a user must dial to deactivate the Call Forward Unconditional service. This sequence must be unique and follow the syntax for digit maps (see “Using Digit Maps” on page 85 for details). Note that dialing this digit map will not have any effect unless the service’ status is “enabled”. This value must also be different from the value set in Step 4.

The deactivating sequence is set for all the ports of the Mediatrix 1102. You cannot have a different sequence for each port.

### On Busy

You can automatically forward the incoming calls of your users to a pre-determined extension within your system if they are already on the line.

Please refer to the *Mediatrix 1102 User’s Manual* for more details on how to use this feature.

#### ► To set the Call Forward On Busy feature:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesCallForwardBusy* group.

This group contains all of the variables required to set the Call Forward On Busy feature.

2. Enable the Call Forward On Busy by setting the *telephonyServicesCallForwardBusyEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

3. Define the address to which incoming calls will be automatically forwarded in the *telephonyServicesCallForwardBusyForwardingAddress* variable.

This string represents the address or telephone number that the user wants to forward calls to. Accepted formats are:

- phone numbers (5551111)
- "scheme:user@host" type strings (such as SipUrls). For instance, "sip:user@foo.com".

Note that this string will be used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

Since this variable is located in a table, you can have a different string for each port.

4. Define the digits that users will have to dial to start the Call Forward On Busy feature in the *telephonyServicesCallForwardUnconditionnalEnableDigitMap* variable.

For instance, you could decide to put "\*72" as the sequence a user must dial to activate the Call Forward On Busy service. This sequence must be unique and follow the syntax for digit maps (see ["Using Digit Maps" on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service' status is "enabled". This value must also be different from the value set in Step 5.

The activating sequence is set for all the ports of the Mediatrix 1102. You cannot have a different sequence for each port.



**Note:** The status of the service as set by the users is kept in the *telephonyServicesCallForwardBusyStatus* variable (in the *telephonyServicesIfCallForwardBusyStatusTable*). For instance, if a user has started the service on his/her phone and the Mediatrix 1102 reboots for any reason, the unit will use the status kept in this variable and restore the service to "active". This way, the user does not have to remember to restart the service.

5. Define the digits that users will have to dial to stop the Call Forward On Busy feature in the *telephonyServicesCallForwardUnconditionnalDisableDigitMap* variable.

For instance, you could decide to put "\*73" as the sequence a user must dial to deactivate the Call Forward On Busy service. This sequence must be unique and respect the syntax for digit maps (see ["Using Digit Maps" on page 85](#) for

details). Note that dialing this digit map will not have any effect unless the service' status is "enabled". This value must also be different from the value set in Step 4.

The deactivating sequence is set for all the ports of the Mediatrix 1102. You cannot have a different sequence for each port.

### On No Answer (Don't Answer)

You can forward the incoming calls of your users to a pre-determined extension within your system if they do not answer their phone.

Please refer to the *Mediatrix 1102 User's Manual* for more details on how to use this feature.

#### ► To set the Call Forward On No Answer feature:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesCallForwardDontAnswer* group.

This group contains all of the variables required to set the Call Forward On No Answer feature.

2. Enable the Call Forward On No Answer by setting the *telephonyServicesCallForwardDontAnswerEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

3. Define the address to which incoming calls will be forwarded in the *telephonyServicesCallForwardDontAnswerForwarding Address* variable.

This string represents the address or telephone number that the user wants to forward calls to. Accepted formats are:

- phone numbers (5551111)
- "scheme:user@host" type strings (such as SipUrls). For instance, "sip:user@foo.com".

Note that this string will be used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

Since this variable is located in a table, you can have a different string for each port.

4. Define the digits that users will have to dial to start the Call Forward On No Answer feature in the *telephonyServicesCallForwardDontAnswerEnableDigitMap* variable.

For instance, you could decide to put “\*74” as the sequence a user must dial to activate the Call Forward On No Answer service. This sequence must be unique and follow the syntax for digit maps (see [“Using Digit Maps” on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service’ status is “enabled”. This value must also be different from the value set in Step 5.

The activating sequence is set for all the ports of the Mediatrix 1102. You cannot have a different sequence for each port.



**Note:** The status of the service as set by the users is kept in the *telephonyServicesCallForwardDontAnswerStatus* variable (in the *telephonyServicesIfCallForwardDontAnswerStatusTable*). For instance, if a user has started the service on his/her phone and the Mediatrix 1102 reboots for any reason, the unit will use the status kept in this variable and restore the service to “active”. This way, the user does not have to remember to restart the service.

5. Define the digits that users will have to dial to stop the Call Forward On No Answer feature in the *telephonyServicesCallForwardDontAnswerDisableDigitMap* variable.

For instance, you could decide to put “\*75” as the sequence a user must dial to deactivate the Call Forward On No Answer service. This sequence must be unique and follow the syntax for digit maps (see [“Using Digit Maps” on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service’ status is “enabled”. This value must also be different from the value set in Step 4.

The deactivating sequence is set for all the ports of the Mediatrix 1102. You cannot have different sequences for each port.

6. Define the time, in milliseconds, the telephone keeps ringing before the call forwarding activates in the *telephonyServicesCallForwardDontAnswerTimeout* variable.

The default value is 5000.

## Call Waiting

Your users can activate/deactivate the call waiting tone for their current call. This is especially useful when transmitting faxes. The user that is about to send a fax can thus deactivate the call waiting tone to ensure

that the fax transmission will not be disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone will be automatically reactivated.

Please refer to the *Mediatrix 1102 User's Manual* for more details on how to use this feature.

► **To set the Call Waiting feature:**

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.

2. Enable the Call Waiting feature by setting the *telephonyServicesCallWaitingEnable* variable to **enable**.

This permanently activates the call waiting tone. New calls received during an already active call will result in a special tone indicating that a call is waiting on the second line. The user can then answer that call by using the “flash” button. The user will then be able to switch between the two active calls by using the “flash” button.

The call hold service must be enabled for this service to work. See [“Call Hold” on page 96](#).

If you are exclusively using faxes, you can put the variable to **disable** to permanently disable the call waiting tone.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesCallWaitingStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

3. If you want to disable the Call Waiting tone on a per-call basis, set the *telephonyServicesCallWaitingCancelEnable* variable to **enable**.

This allows a user who has call waiting enabled to disable that service on a per-call basis. Dialing the “enable” digit map for this service will disable the call waiting on the next call only. If, for any reason, the user wishes to undo the cancel, simply unhook and re-hook the telephone to reset the service.

If enabled, it becomes possible for the user to dial the digit maps for disabling this service. The call hold service must be enabled for this service to work. See [“Call Hold” on page 96](#).

Since this variable is located in a table, you can disable the service on a per-port basis.

4. Define the digits that users will have to dial to disable the Call Waiting tone in the *telephonyServicesCallWaitingCancelDigitMap* variable.

For instance, you could decide to put “\*76” as the sequence a user must dial to disable the call waiting tone on his/her telephone. This sequence must be unique and follow the syntax for digit maps (see [“Using Digit Maps” on page 85](#) for details). Note that dialing this digit map will not have any effect unless the service’ status is “enabled”.

The deactivating sequence is set for all the ports of the Mediatix 1102. You cannot have a different sequence for each port.

### Second Call

The Second Call allows a user with an active call to put the call on hold, then initiate a new call on the second line. This service is most useful with the transfer and conference services.

The call hold service must be enabled for this service to work. See [“Call Hold” on page 96](#).

Please refer to the *Mediatix 1102 User’s Manual* for more details on how to use this feature.

#### ► To enable the second call service:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.
2. Enable the Call Hold by setting the *telephonyServicesSecondCallEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesSecondCallStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

### Call Transfer – Blind Transfer

The blind call transfer service is sometimes called Transfer without Consultation or Unattended Transfer. With this service enabled, a user can transfer a call on hold to a still ringing (unanswered) call.

The call hold and second call services must be enabled for this service to work. See [“Call Hold” on page 96](#) and [“Second Call” on page 103](#).

Please refer to the *Mediatix 1102 User’s Manual* for more details on how to use this feature.

► **To enable the blind transfer service:**

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.
2. Enable the blind transfer service by setting the *telephonyServicesBlindTransferEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesBlindTransferStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

**Call Transfer –  
Attended  
Transfer**

The attended call transfer service is sometimes called Transfer with Consultation. With this service enabled, a user can transfer a call on hold to an active call.

The call hold and second call services must be enabled for this service to work. See [“Call Hold” on page 96](#) and [“Second Call” on page 103](#).

Please refer to the *Mediatrix 1102 User’s Manual* for more details on how to use this feature.

► **To enable the attended transfer service:**

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.
2. Enable the attended transfer service by setting the *telephonyServicesAttendedTransferEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesAttendedTransferStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

**Conference  
Call**

The Conference Call service allows a user to link two or more calls together to form a single conversation, called a conference. Note that:

- Only 3-way conferences are currently supported.
- It is possible for a participant of the conference to put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. It is not possible for the participant that has initiated the conference to put the conference on

hold.

The call hold and second call services must be enabled for this service to work. See [“Call Hold” on page 96](#) and [“Second Call” on page 103](#).

Please refer to the *Mediatix 1102 User’s Manual* for more details on how to use this feature.

► **To enable the conference call service:**

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIfActivationTable* group.
2. Enable the conference call service by setting the *telephonyServicesConferenceEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

The current status of the service can be found in the *telephonyServicesConferenceStatus* read-only variable (under the *telephonyServicesIfStatusTable*).

### **Automatic Speed Dialing**

The automatic speed dialing feature allows you to define a phone number that will be automatically dialed when the handset is taken off hook.

When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

Please refer to the *Mediatix 1102 User’s Manual* for more details on how to use this feature.

► **To set the automatic speed dialing feature:**

1. In the *telephonyServicesMIB*, locate the *telephonyServicesAutoSpeedDial* group.  
This group contains all of the variables required to set the automatic speed dialing feature.
2. Enable the automatic speed dialing feature by setting the *telephonyServicesAutoSpeedDialEnable* variable to **enable**.

Since this variable is located in a table, you can enable/disable the service on a per-port basis.

3. Define the number to dial when the handset is taken off hook in the *telephonyServicesAutoSpeedDialTargetAddress* variable.

This string represents the address or telephone number that the user wants to automatically call. Accepted formats are:

- phone numbers (5551111)
- "scheme:user@host" type strings (such as SipUrls). For instance, "sip:user@foo.com".

Note that this string will be used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

Since this variable is located in a table, you can define a different number for each port of the Mediatix 1102.

### IP Address Call Service

The IP address call service allows a user to dial an IP address without the help of a SIP server.

Please refer to the *Mediatix 1102 User's Manual* for more details on how to use this feature.

#### ► To enable the IP address call service:

1. In the *telephonyServicesMIB*, locate the *telephonyServicesIpAddressCallCustomization* group.
2. Enable the IP address call feature by setting the *telephonyServicesIpAddressCallEnable* variable to **enable**.

---

## SNTP Settings

The Simple Network Time Protocol (SNTP)<sup>1</sup> enables the notion of time (date, month, time) into the Mediatix 1102. It updates the internal clock of the unit, which is the client of a SNTP server. It is especially 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 (see RFC 1769 for more details).

#### ► To enable the SNTP feature:

1. In the *sntpMIB*, locate the *sntpEnable* variable.  
This variable enables the SNTP feature.
2. Set the *sntpEnable* variable to **Enable**.

---

1. Only available in units that run the SIP signalling protocol.

- Set the following synchronization information:

**Table 54:** SNTP Synchronization Information

Variable	Description
sntpSynchronizationPeriod	Time interval (in minutes) between request made to the SNTP server. The result will be used to synchronize the unit with the time server. The maximum value is set to 1440 minutes which corresponds to 24 hours. <b>Default Value:</b> 1440
sntpSynchronizationPeriodOnError	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1440 minutes which corresponds to 24 hours. <b>Default Value:</b> 60

### DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the SNTP server. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

#### ► To use DHCP-assigned information:

- In the *ipAddressConfig* folder, locate the *sntpSelectConfigSource* variable (under the *ipAddressConfigSntp* group).  
This variable defines whether the Mediatrix 1102 must ask for its SNTP server settings through a DHCP server or not.
- 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 of the *ipAddressStatus* folder.
- Set the DHCP Vendor Specific code of the SNTP feature in your DHCP server.  
See [“SNTP Settings” on page 106](#) for more details.

#### ► To use static information:

- In the *ipAddressConfig* folder, locate the *sntpSelectConfigSource* variable (under the *ipAddressConfigSntp* group).  
This variable defines whether the Mediatrix 1102 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 55:** SNTP Static Address

Variable	Description
sntpStaticHost	Static SNTP server IP address or domain name. <b>Default Value:</b> 192.168.0.10
sntpStaticPort	Static SNTP server IP port number. <b>Default Value:</b> 123

### Defining a Custom Time Zone

At boot time, the Mediatrix 1102 unit queries a NTP or SNTP server to receive time information. The unit 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 1102 offers time zone configuration with daylight saving settings.

To define a custom time zone IEEE 1003.1, you must 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 will be validated and the result returned in the *sntpTimeZoneStringIsValid* variable. 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 (-), 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.

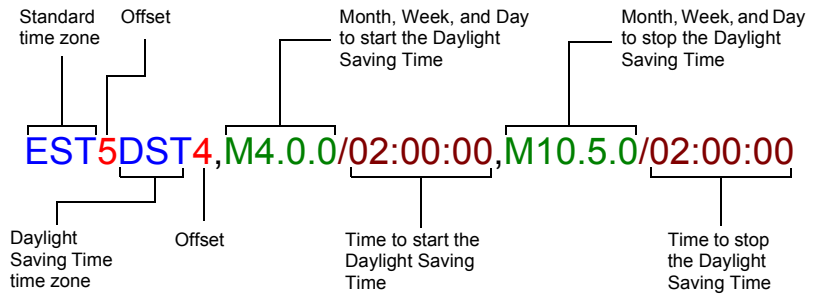
M10.1.6

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 56:** Valid POSIX Strings

Time Zone	POSIX String
Pacific Time (Canada & US)	PST8DST7,M4.1.0/02:00:00,M10.5.0/02:00:00
Mountain Time (Canada & US)	MST7DST6,M4.1.0/02:00:00,M10.5.0/02:00:00
Central Time (Canada & US)	CST6DST5,M4.1.0/02:00:00,M10.5.0/02:00:00
Eastern Time (Canada & US)	EST5DST4,M4.1.0/02:00:00,M10.5.0/02:00:00
Atlantic Time (Canada)	AST4DST3,M4.1.0/02:00:00,M10.5.0/02:00:00
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

**Table 56:** Valid POSIX Strings (Continued)

Time Zone	POSIX String
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	AUEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
UTC (Coordinated Universal Time)	UTC0



# Management Server Configuration

The Management Server is a generic name for a module or software that is used to remotely set up Mediatrix 1102 units. For instance, the Management Server could be the Mediatrix Unit Manager Network product.

---

## Using the Management Server

You have the choice of setting up Mediatrix 1102 units directly with a SNMP browser or with the Management Server. If you want to use the Management Server to setup the units, you must 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 1102.
2. Set the *msEnable* variable to **enable**.
3. Set the Trap retransmission period (*msTrapRetransmissionPeriod* variable) to the desired value.  
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 1102 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.

## DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the Management Server. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

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

1. In the *ipAddressConfig* folder, locate the *msSelectConfigSource* variable.  
This variable defines whether the Mediatrix 1102 must 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 57:** Management Server DHCP Information

To use a...	You must...
vendor specific code	Set the <i>msDhcpSiteSpecificCode</i> variable to <b>0</b> , which is the default value. You must set the DHCP server with the vendor specific code 200 (hexadecimal 0xC8).
site specific code	Set the <i>msDhcpSiteSpecificCode</i> variable to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

See [“Vendor and Site Specific DHCP Options”](#) on page 33 for more details.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *msSelectConfigSource* variable.  
This variable defines whether the Mediatrix 1102 must get its Management Server configuration through a DHCP server or not.
2. Set the *msSelectConfigSource* variable to **static**.

3. Set the following variables:

**Table 58:** Management Server Static Address

Variable	Description
msStaticHost	Static management server IP address or domain name. <b>Default Value:</b> 192.168.0.10
msStaticTrapPort	Static management server IP port number. <b>Default Value:</b> 162



This chapter describes other configuration settings not covered in the previous chapters.

## Using QoS

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. The Mediatrix 1102 supports the Differentiated Services (DS) field and 802.1q taggings. There are four variables – one variable for signalling (SIP) and one variable for each of voice, T.38 and VBD (Voice Band Data) media.



**Note:** The Mediatrix 1102 does not support RSVP (Resource Reservation Protocol).

### Differentiated Services (DS) Field

You can set various Differentiated Services parameters that will allow you to control the network traffic.



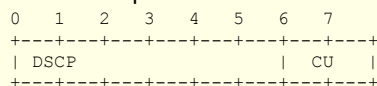
**Note:** It is the network administrator's responsibility to provision the Mediatrix 1102 with standard and correct values.

## What are 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.

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. For future extensibility, the entire DS field (TOS byte) will be configurable.

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

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

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 (184d).

This default value would result in a value of “101” precedence bits, low delay, high throughput, and normal reliability in the legacy IP networks (RFC 791, RFC 1812). Network managers of legacy IP networks could use the above-mentioned values to define filters on their routers to take advantage of priority queuing. The default value is based on the Expedited Forwarding PHB (RFC 2598) recommendation.

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 and the *MIB Reference* manual:

- 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)

**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 must be provisioned.



**Note:** It is the network administrator’s responsibility to provision the Mediatrix 1102 with standard and correct values.

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

1. In the *qosleee8021q* group of the *qosMIB*, locate the following variables:
  - *qosSignalingleee8021qEnable*
  - *qosVoicelLee8021qEnable*
  - *qosT38Faxleee8021qEnable*
  - *qosVbdleee8021qEnable*
2. Set the value of these variables to **enable**.  
The corresponding user priority configuration is enabled.
3. In the *qosleee8021q* group of the *qosMIB*, locate the following variables:
  - *qosSignalingleee8021qUserPriority*
  - *qosVoicelLee8021qUserPriority*
  - *qosT38Faxleee8021qUserPriority*
  - *qosVbdleee8021qUserPriority*

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.

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*
4. Set the value of these variables.
5. Reboot the Mediatix 1102.

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:

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 (byte)
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Dest Addr | Src Addr | VLAN | Type/Length | ...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

The VLAN field is separated as follows:

```

0 (bit)                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                               0x8100                               | Pri |T|                               VID                               |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

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

## Syslog Daemon Configuration

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from the Mediatrix 1102 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 1102, 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.

### ► To enable the Syslog daemon:

1. In the *syslogMIB*, locate the *syslogMsgMaxSeverity* variable.

This variable indicates which syslog message will be 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**.

### DHCP vs. Static Configuration

The Mediatrix 1102 must know the IP address and port number of the Syslog server. You can assign these information to the Mediatrix 1102 through a DHCP server or manually enter them yourself with the static variables.

### ► To use DHCP-assigned information:

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

This variable defines whether the Mediatrix 1102 must 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 59:** Syslog DHCP Information

To use a...	You must...
vendor specific code	Set the <i>syslogDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSyslogDhcp</i> group) to <b>0</b> , which is the default value. You must set the DHCP server with the vendor specific code 110 (hexadecimal 0x6E).
site specific code	Set the <i>syslogDhcpSiteSpecificCode</i> variable (under the <i>ipAddressConfigSyslogDhcp</i> group) to any value between 128 and 254. You must set the DHCP server with the site specific code you have chosen.

See [“Vendor and Site Specific DHCP Options” on page 33](#) for more details.

► **To use static information:**

1. In the *ipAddressConfig* folder, locate the *syslogSelectConfigSource* variable.  
This variable defines whether the Mediatix 1102 must 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 60:** Syslog Daemon Static Address

Variable	Description
<i>syslogStaticHost</i>	Syslog server static IP address or domain name. <b>Default Value:</b> 192.168.0.10
<i>syslogStaticPort</i>	Syslog server static IP port number. <b>Default Value:</b> 514

**Configuring the Syslog Daemon** You must 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.

## Setting up Flash Hook Detection

A flash hook can be described as quickly depressing and releasing the plunger in or the actual handset-cradle to create a signal indicating that special instructions will follow such as transferring the call to another extension.

The Mediatrix 1102 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 61:** Flash Hook Parameters

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



The Mediatrix 1102 collects meaningful statistics that can be read via the RTP MIB.

### 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

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 62:** 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. You must 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.

**Example**

The following is an example with *sysConfigStatsNumberPeriods* = 3 and *sysConfigStatsPeriodLength* = 1 (5 minutes).

**Table 63:** 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 sysConfigStatsPeriod Length*) accurate to 5 minutes (*sysConfigStatsPeriod Length*). 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.



This chapter explains how to maintain the Mediatrix 1102. It also contains a troubleshooting section that helps you find and correct the most common problems you may encounter with the unit.



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

---

---

### Caution Regarding Handling

The Mediatrix 1102 must be handled with some caution. This section illustrates the basic facts regarding handling, storage and cleaning.

#### Location

Install the Mediatrix 1102 in a well ventilated location where it will not be exposed to high temperature or humidity. Do not install the Mediatrix 1102 in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components. See [“Choosing a Suitable Installation Site” on page 12](#) for more details.

#### Condensation

When the unit is brought into a warm environment from the cold, condensation may result which 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 1102, wipe with a soft dry cloth. Do not use volatile liquids such as benzine and thinner which are harmful to the unit casing.

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

---

### Troubleshooting

You can experience some minor problems when connecting the Mediatrix 1102 to the network. The following section examines some of these problems and possible solutions.



**Note:** A Syslog message lists the problems the Mediatrix 1102 encounters. You can see this message with the Syslog daemon.

---

**General  
Operation  
Problems**

**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 10/100 BaseT Ethernet RJ-45 cable is connected to the network if you are using the LAN-powered version.
- The power cord is fully inserted into the Mediatrix 1102 power socket.

**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 1102 and to the network connector.
- You did not connect a crossover network cable.

**POSSIBLE CAUSE:** Configurable parameters of the Mediatrix 1102 are not set properly.

**SOLUTION:** Refer to this manual for a complete description of the configurable Mediatrix 1102 parameters.

**DESCRIPTION:** Unable to establish a call from the Mediatrix 1102 to an user agent such as an IP phone, a gateway or another terminal.

**POSSIBLE CAUSE:** When the Mediatrix 1102 – with its T.38 capability enabled – tries to establish a call with an user agent that does not support T.38, this user agent 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 1102. See [“Data Codecs” on page 66](#) for more details.

**DESCRIPTION:** “Poor line condition” error during a fax transmission

**POSSIBLE CAUSE:** The analog transmission between the fax machine and the Mediatix 1102 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 Variables” on page 62](#) for more details.

**DESCRIPTION:** The Mediatix 1102 becomes unreachable when changing the Ethernet speed at run-time.

**POSSIBLE CAUSE:** Some Hubs cannot adapt completely their port speed at run-time.

**SOLUTION:** The Mediatix 1102 must always be restarted for the new setting to take effect. See [“Ethernet Connection Speed” on page 41](#) 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 what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, let’s consider the IP address 192.168.0.1. Assuming this is part of a Class B network, the first two numbers (192.168) represent the Class B network address, and the second two numbers (0.1) identify a particular host on this network.

Let’s say you have the following information:

- Mediatix 1102 IP address: 192.168.0.1
- Subnet Mask: 255.255.0.0 (Class B)
- DHCP Server IP address: 192.168.0.20

If you happen to change the Mediatix 1102 IP address to 192.169.0.1, for instance, the subnet mask is still valid, but you will not be able to reach your DHCP server anymore. Refer to subnet mask documentation for more details.

**Software  
Upgrade  
Problems**

**DESCRIPTION:** An error occurs when the Mediatrix 1102 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.
- Make sure that the directory contains files. If not, you must extract them from the zip file again. See [“Download Procedure” on page 54](#) for more details.
- Make sure that the software server (TFTP) 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 1102 attempts to transfer the software upgrade

**POSSIBLE CAUSE:** The Ethernet cable has become disconnected from the Mediatrix 1102 or the PC running the file transfer.

**SOLUTION:** Reconnect the cable and start again.

**POSSIBLE CAUSE:** Power to the Mediatrix 1102 has been disrupted during the file transfer.

**SOLUTION:** Check the power connection to the Mediatrix 1102 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 Windows will not recognize the “/” character and produce an error.

**SOLUTION:** Use the “\” character in the path definition.

**SNMP  
Management  
Software  
Problems**

**DESCRIPTION:** The SNMP network management software cannot access the Mediatrix 1102

**POSSIBLE CAUSE:** The SNMP network management software does not have the proper Mediatrix 1102 information.

**SOLUTION:** Check that:

- The IP information for the Mediatrix 1102 is correctly configured.
- The Mediatrix 1102 was reset after defining the IP information.
- The port through which you are trying to access the Mediatrix 1102 has been unlocked or is not the correct port. If it is locked, check the connections and network cabling for the port.

Try to locate the Mediatrix 1102 IP address. If impossible, perform a recovery reset as indicated in section [“Using the Default Settings Switch” on page 17](#).

**DESCRIPTION:** There is no response when trying to access the Mediatrix 1102

The Mediatrix 1102 speaks two of the three most common SNMP protocols: SNMPv1 and SNMPv2c. If you try to access it using any other protocol, it stays silent.

**DESCRIPTION:** Traps are not received by the SNMP network manager

**PROBLEM:** 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 1102.

**DESCRIPTION:** When trying to set a variable, the Mediatrix 1102 does not respond, nor sends an error message

In secure management mode, the Mediatrix 1102 does not accept SNMPv1 and SNMPv2c SET requests. However, the MIB variables are viewable in any management mode (secure and not secure).

**DESCRIPTION:** When I try to set a variable with a MIB browser such as the 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.

Mediatrix Telecom, Inc. configuration tools (such as the Unit Manager Network or Unit Manager Express) do not support MIBs that are located under the *mediatrixExperimental* branch of the MIB structure. The configuration tools do 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 experimental MIBs can be viewed with Mediatrix Telecom, Inc. configuration tools, SNMP operations may not work properly on them.

**DESCRIPTION:** When viewing a table, the unit does not respond

It may take time to fill completely a table: from 1 to 5 seconds. This is normal, since the unit is an embedded device with limited processing power.

This Appendix presents the possible states of Mediatrix units, as seen from an operator perspective. For each state, a LED pattern is associated so that the operator knows the progression of operations.

This document applies to the following Mediatrix products:

- ▶ Mediatrix 1102
- ▶ Mediatrix 1104
- ▶ Mediatrix 1124



**Note:** This appendix refers to the *Default Settings* button as the “button”. See [“Using the Default Settings Switch” on page 17](#) more details.

## LED Indicators

The number and type of LED indicators vary depending on the Mediatrix unit you have. [Table 64](#) shows the available LED indicators according to the hardware platforms.

**Table 64:** Description of LED Indicators

Mediatrix Product	LEDs			
	Ready (Green)	In Use (Yellow/Orange)	LAN (Green)	Power (Green)
Mediatrix 1102	•	•	•	•
Mediatrix 1104	•	•	•	•
Mediatrix 1124	•	–	•	•

## LED States

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 (2) seconds and stays on for one (1) 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.

## LED Patterns

The LED patterns represent logical states. [Table 65](#) describes the different states a Mediatrix unit can have and their associated LED patterns.

**Table 65:** States and LED Patterns

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
Booting	<p>This state follows a hardware start or a reset. If a software download has to take place, the Mediatrix unit enters the <i>ImageDownloadInProgress</i> state, otherwise the application is started. In both cases, the Power LED blinks while waiting for a DHCP offer, otherwise it is steady ON.</p> <p>If a recovery is in progress, then the Mediatrix unit enters the <i>RecoveryMode</i> state or the <i>RecoveryModePending</i> state if the button is pressed, otherwise the <i>NormalMode</i> state is selected.</p>	Off	Off	HW	On or Blink at 1 Hz 75%
Normal Mode	<p>This is the “normal” state of the Mediatrix unit where calls can be initiated. In this state, each LED has a separate behaviour.</p> <p>If the <i>groupAdminState</i> MIB variable is set to “locked”, the Mediatrix unit enters the <i>AdminMode</i> state.</p>	See “ <a href="#">NormalMode LED Pattern Description</a> ” on page 138			
AdminMode	<p>This is the “administration” mode of the Mediatrix unit where calls are not permitted and maintenance actions can be performed.</p> <p>When the <i>groupAdminState</i> MIB variable returns to “unlocked”, the Mediatrix unit goes back to the <i>NormalMode</i> state</p> <p><b>NOTE:</b> The <i>Ready</i> and <i>Power</i> LEDs blink off phase in turns.</p>	Blink 0.5 Hz 50%	Off	HW	Blink 0.5 Hz 50%
Recovery Mode	<p>In this state, the IP addresses for local host, image server, syslog server, etc., are set to known values, allowing configuration of the Mediatrix unit. Calls are not allowed.</p> <p>The “known” addresses are temporary (non persistent). Resetting the Mediatrix unit will return it to the <i>NormalMode</i> state.</p> <p><b>NOTE:</b> The <i>Ready</i> and <i>Power</i> LEDs are in phase.</p>	Blink 0.5 Hz 75%	Off	HW	Blink 0.5 Hz 75%

**Table 65:** States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
Reset Pending	This is when the button is pressed and held for at least 2 seconds while in any substate of Operation Modes.  If the button is released within 5 seconds, data is stored and the Mediatrix unit is reset, otherwise the Mediatrix unit triggers the <i>RecoveryModePending</i> state.	Off	Off	Off	Blink 1 Hz 50%
Recovery Mode Pending	This state is triggered when the button is held at boot-time or for at least 7 seconds from any Operation Modes substate.  If the button is released within 5 seconds after the LED pattern has started and the button was pressed while booting, the Mediatrix unit enters the <i>RecoveryMode</i> state. If the button was pressed while in Operation Modes state, the Mediatrix unit resets before going to the <i>RecoveryMode</i> state.  If the button is not released for 5 seconds, the Mediatrix unit falls into the <i>DefaultSettings Pending</i> state.	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%
Default Settings Pending	This is when the button is not released while in the <i>RecoveryModePending</i> state.  If the button is released within 5 seconds, the Mediatrix unit applies the default settings, otherwise the action is cancelled and the Mediatrix unit goes back to Operation Modes state or it resets.	On	On	On	On
Image DownloadIn Progress	A software image is downloaded into the Mediatrix unit and written to persistent storage.	All LEDs are blinking at 1 Hz, <i>one at a time</i> , from left to right.			
Image Download Error	This state is triggered after a failure of an image download operation to indicate that the operation failed. After 4 seconds, the Mediatrix unit resets.	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%

**Table 65:** States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
InitFailed	<p>This state is triggered when bad initialization parameters are detected and the Mediatrix unit cannot boot correctly.</p> <p>For example, the Mediatrix unit enters the <i>InitFailed</i> state when it cannot be reached from the IP network due to bad network parameters.</p> <p>However, there is an exception for network parameters: if the configuration is dynamic, the Mediatrix unit stays in the <i>Booting</i> state and continues to query the DHCP until it receives valid values. If the configuration is static, the LED pattern indicates that the Mediatrix unit must be reset to default settings or put into recovery mode for maintenance and correction of network values.</p>	Off	Off	Blink 4 Hz 50%	Off
DiagFailed	This state is triggered at boot-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%

**NormalMode  
LED Pattern  
Description**

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

**Table 66:** LED Patterns in Operation Mode

LED	Pattern	Meaning
Ready	Steady On	All ports are enabled (operational state).
	Steady Off	All ports are disabled (operational state).
	Blink 0.25 Hz 75%	At least one port is enabled and at least one port is disabled (operational state).
In Use	Steady On	At least one analog port is busy (usage state).
	Steady Off	All analog ports are not busy (usage state).
LAN (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected.
	Blinking (variable rate)	Ethernet activity detected.

**Table 66:** LED Patterns in Operation Mode (Continued)

LED	Pattern	Meaning
Power	Steady On	Power is On.
	Steady Off	Power is Off.

### Ready LED

The *Ready* LED provides an “at-a-glance” view of the Mediatrix unit’s 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 *ifAdminOpState* column is “enabled” and at least one element is “disabled”.

The *ifAdminOpState* column has the following OID in the *ifAdminMIB*: 1.3.6.1.4.1.4935.5.8.1.10.1.4. Refer to the *MIB Reference Manual* for more details on the *ifAdminOpState* variable. Patterns and meanings of the *Ready* LED are described in [Table 66 on page 138](#).

### 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”. This column has the following OID in the *ifAdminMIB*: 1.3.6.1.4.1.4935.5.8.1.10.1.5. Refer to the *MIB Reference Manual* for more details on the *ifAdminState* variable. Patterns and meanings of the *In Use* LED are described in [Table 66 on page 138](#).

### LAN LED

The *LAN* LED provides the status of the network connected to the Ethernet port. Typically, Ethernet ports are characterized by using two status LEDs: Link and Heartbeat. For the Mediatrix units, a single LED represents these two link attributes. 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 66 on page 138](#).

## Power LED

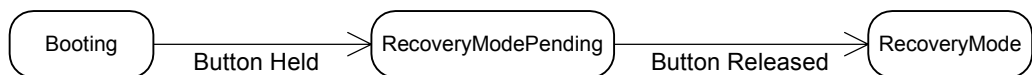
The *Power* LED indicates whether the unit is operational at its most basic level or not. It does not imply that the unit can be used, only that it is capable of being used. Healthy operation would be steady ON. Patterns and meanings of the *Power* LED are shown in [Table 66 on page 138](#).

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

### At Boot-Time

When pressing the button at boot-time, the state sequence goes as follows:

**Figure 13: LED Pattern at Boot-Time**



This leads to the following LED patterns:

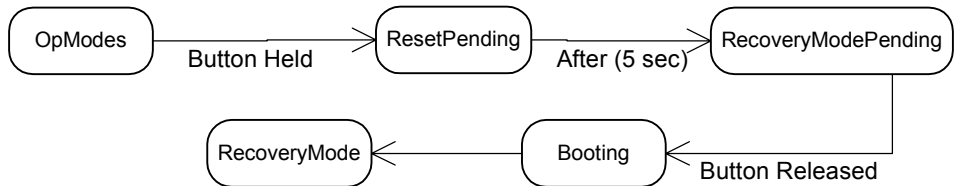
**Table 67: LED Patterns at Boot-Time**

State	LEDs Pattern			
	Ready	In Use	LAN	Power
Booting	Off	Off	HW	On
RecoveryModePending	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%
RecoveryMode	Blink 0.5 Hz 75%	Off	Blink Hw	Blink 0.5 Hz 75%

### At Run-Time

When pressing the button at run-time, the state sequence goes as follows:

**Figure 14:** LED Patterns at Run-Time



This leads to the following LED patterns:

**Table 68:** LED Patterns at Run-Time

State	LEDs Pattern			
	Ready	In Use	LAN	Power
ResetPending	Off	Off	Off	Blink 1 Hz 50%
RecoveryModePending	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%	Blink 1 Hz 50%
Booting	Off	Off	HW	On
RecoveryMode	Blink 0.5 Hz 75%	Off	HW	Blink 0.5 Hz 75%



# Country Specific Parameters

The following parameters differ depending on the country you are in. Note that the *On – Off* sequence should be read as follows:

- ▶ **1.0 – 0.85** means that the sequence is 1.0 second On and 0.85 second Off.

## Australia

The following parameters apply if you have selected Australia as location.

**Table 69: Australia 1 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	<b>CONTINUOUS</b>	-18 dBm
Busy Tone	425 Hz	<b>0.375 – 0.375</b>	-18 dBm
Ringing Tone	425 Hz * 25	<b>0.4 – 0.2, 0.4 – 2.0</b>	-18 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.333</b> <b>0.333</b> <b>0.333 – 1.0</b>	-20 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>0.4 – 0.2, 0.4 – 2.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-Impedance	$Z_N = 600 \Omega$		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-9 dBr

**Table 70: Australia 2 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	<b>CONTINUOUS</b>	-18 dBm
Busy Tone	425 Hz	<b>0.375 – 0.375</b>	-18 dBm
Ringing Tone	425 Hz * 25	<b>0.4 – 0.2, 0.4 – 2.0</b>	-18 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.333</b> <b>0.333</b> <b>0.333 – 1.0</b>	-20 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>0.4 – 0.2, 0.4 – 2.0</b>	
Impedance	$Z_R = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
Tbri-Impedance	$Z_N = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-9 dBr

**Austria**

The following parameters apply if you have selected Austria as location.

**Table 71: Austria Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	1.0 – 0.85	-20 dBm
Busy Tone	450 Hz	0.45 – 0.45	-20 dBm
Ringing Tone	450 Hz	1.0 – 4.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	1.0 – 5.0	
Impedance	$Z_R = 270 \Omega + 750 \Omega // 150 \text{ nF}$		
Tbri-Impedance	$Z_N = 600 \Omega$		
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 72: China Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	<b>CONTINUOUS</b>	-10 dBm
Busy Tone	450 Hz	0.35 – 0.35	-10 dBm
Ringing 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
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	1.0 – 4.0	
Impedance	$Z_R = 600 \Omega$		
Tbri-Impedance	$Z_N = 600 \Omega$		
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 73: France Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	330 Hz	<b>CONTINUOUS</b>	-16.9 dBm
Busy Tone	440 Hz	<b>0.5 – 0.5</b>	-19.9 dBm
Ringing Tone	440 Hz	<b>1.5 – 3.5</b>	-19.9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-19.9 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	<b>1.5 – 3.5</b>	
Impedance	$Z_R = 215 \Omega + 1000 \Omega // 137 \text{ nF}$		
Tbri-Impedance	$Z_N = 600 \Omega$		
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.

**Table 74: Germany 1 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>0.2 – 0.3, 0.2 – 0.3, 0.2 – 0.8</b>	-16 dBm
Busy Tone	425 Hz	<b>0.17 – 0.43</b>	-16 dBm
Ringing Tone	425 Hz	<b>1.0 – 4.0</b>	-16 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-16 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 4.0</b>	
Impedance	$Z_R = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
Tbri-Impedance	$Z_N = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-10 dBr

**Table 75: Germany 2 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>0.2 – 0.3, 0.2 – 0.3, 0.2 – 0.8</b>	-16 dBm
Busy Tone	425 Hz	<b>0.17 – 0.43</b>	-16 dBm

**Table 75: Germany 2 Parameters (Continued)**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Ringing Tone	425 Hz	1.0 – 4.0	-16 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-16 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Impedance	$Z_R = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
Tbri-Impedance	$Z_N = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
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 76: Hong Kong Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350 + 440 Hz	<b>CONTINUOUS</b>	-13 dBm
Busy Tone	480 + 620 Hz	0.5 – 0.5	-13 dBm
Ringing 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
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	0.4 – 0.2, 0.4 – 3.0	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
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 77: Indonesia Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>CONTINUOUS</b>	-9 dBm
Busy Tone	425 Hz	<b>0.5 – 0.5</b>	-9 dBm
Ringing Tone	425 Hz	<b>1.0 – 4.0</b>	-9 dBm
Special Information Tone	425 Hz	<b>0.33 – 0.03, 0.33 – 0.03, 0.33 – 1.03</b>	-9 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 4.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
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 78: Israel Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	<b>CONTINUOUS</b>	-15 dBm
Busy Tone	400 Hz	<b>0.5 – 0.5</b>	-15 dBm
Ringing Tone	400 Hz	<b>1.0 – 3.0</b>	-15 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.333 0.333 0.333 – 1.0</b>	-15 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 3.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
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 79: Italy Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	0.6 – 1.0, 0.2 – 0.2	-13 dBm
Busy Tone	425 Hz	0.5 – 0.5	-13 dBm
Ringing 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
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.0 – 4.0	
Impedance	$Z_R = 180 \Omega + 630 \Omega // 60 \text{ nF}$		
Tbri-impedance	$Z_N = 750 \Omega // 18 \text{ nF}$		
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 80: 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
Ringing Tone	400 Hz * 16	1.0 – 2.0	-16 dBm
Special Information Tone	400 Hz	0.1 – 0.1	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	1.0 – 2.0	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
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 81: Malaysia Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>CONTINUOUS</b>	-14 dBm
Busy Tone	425 Hz	<b>0.5 – 0.5</b>	-18 dBm
Ringing Tone	425 Hz	<b>0.4 – 0.2, 0.4 – 2.0</b>	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	<b>1.0 1.0 1.0 – 1.0</b>	-14 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	<b>0.4 – 0.2, 0.4 – 2.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

**North America**

The following parameters apply if you have selected North America as location.

**Table 82: North America 1 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels (Level / Frequency)
Dial Tone	350+440 Hz	<b>CONTINUOUS</b>	-17 dBm
Busy Tone	480+620 Hz	<b>0.5 – 0.5</b>	-21 dBm
Ringing Tone	440+480 Hz	<b>2.0 – 4.0</b>	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33 0.33 0.33 – 1.0</b>	-14 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	<b>2.0 – 4.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-Impedance	$Z_N = 600 \Omega$		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-3 dBr

**Table 83: North America 2 Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels (Level / Frequency)
Dial Tone	350+440 Hz	<b>CONTINUOUS</b>	-17 dBm
Busy Tone	480+620 Hz	<b>0.5 – 0.5</b>	-21 dBm

**Table 83:** North America 2 Parameters (Continued)

Parameter	Value	On – Off Sequence (s)	Elect. Levels (Level / Frequency)
Ring 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
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	2.0 – 4.0	
Impedance	$Z_R = 600 \Omega$		
Tbri-Impedance	$Z_N = 350 \Omega + 1000 \Omega // 210 \text{ nF}$		
FXS Line Attenuation (Input)			0 dB
FXS Line Attenuation (Output)			0 dB

## Spain

The following parameters apply if you have selected Spain as location.

**Table 84:** Spain Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	0.2 – 0.3, 0.2 – 0.3, 0.2 – 0.8	-10 dBm
Busy Tone	425 Hz	0.2 – 0.2	-13 dBm
Ring Tone	425 Hz	1.5 – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 0.33 – 1.0	-20 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	1.5 – 3.0	
Impedance	$Z_R = 220 \Omega + 820 \Omega // 120 \text{ nF}$		
Tbri-Impedance	$Z_N = 220 \Omega + 820 \Omega // 120 \text{ nF}$		
FXS Line Attenuation (Input)			0 dB
FXS Line Attenuation (Output)			-7 dB

**Sweden**

The following parameters apply if you have selected Sweden as location.

**Table 85: Sweden Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>CONTINUOUS</b>	-12.5 dBm
Busy Tone	425 Hz	<b>0.25 – 0.25</b>	-12.5 dBm
Ringing Tone	425 Hz	<b>0.45 – 5.0, 1.0 – 5.0</b>	-12.5 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-22 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 5.0</b>	
Impedance	$Z_R = 200 \Omega + 1000 \Omega // 100 \text{ nF}$		
Tbri-impedance	$Z_N = 900 \Omega // 30 \text{ nF}$		
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 86: Switzerland Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	<b>CONTINUOUS</b>	-8 dBm
Busy Tone	425 Hz	<b>0.5 – 0.5</b>	-13 dBm
Ringing Tone	425 Hz	<b>1.0 – 4.0</b>	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 4.0</b>	
Impedance	$Z_R = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
Tbri-impedance	$Z_N = 220 \Omega + 820 \Omega // 115 \text{ nF}$		
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 87: Thailand Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 * 50 Hz	<b>CONTINUOUS</b>	-16 dBm
Busy Tone	400 Hz	<b>0.5 – 0.5</b>	-10 dBm
Ringing Tone	400 Hz	<b>1.0 – 4.0</b>	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-15 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>1.0 – 4.0</b>	
Impedance	$Z_R = 600 \Omega$		
Tbri-impedance	$Z_N = 600 \Omega$		
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 88: UK Parameters**

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350+440 Hz	<b>CONTINUOUS</b>	-22 dBm
Busy Tone	400 Hz	<b>0.375 – 0.375</b>	-19 dBm
Ringing Tone	400+450 Hz	<b>0.4 – 0.2, 0.4 – 2.0</b>	-22 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	<b>0.33</b> <b>0.33</b> <b>0.33 – 1.0</b>	-19 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	<b>0.4 – 0.2, 0.4 – 2.0</b>	
Impedance	$Z_R = 300 \Omega + 1000 \Omega // 220 \text{ nF}$		
Tbri-impedance	$Z_N = 370 \Omega + 620 \Omega // 310 \text{ nF}$		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-9 dBr



# Standards Compliance

This Appendix lists the various standards compliance of the Mediatrix 1102.

## Standards Supported

The Mediatrix 1102 complies to the following standards:

**Table 89:** Standards Compliance

Category	Specification
Agency approvals	<ul style="list-style-type: none"> <li>cULus</li> <li>European Union, CE mark (Declaration of Conformity)</li> </ul>
Safety standards	<ul style="list-style-type: none"> <li>UL60950 3<sup>rd</sup> Edition (2000)</li> <li>CAN/CSA-C22.2 No. 60950-00</li> <li>IEC 60950 (3<sup>rd</sup> Edition (1999) with all national deviation)</li> </ul>
Emissions	<ul style="list-style-type: none"> <li>FCC (47 CFR Part 15) Subpart B 1994 Class B</li> <li>EN55022 (1994) Class B</li> <li>AS/NZS 3548:1995 Class B</li> <li>EN61000-3-2 Harmonic current emissions</li> <li>EN61000-3-3 Voltage fluctuations and flicker</li> </ul>
Immunity	EN55024:1998 including the following: <ul style="list-style-type: none"> <li>EN61000-4-2, ESD</li> <li>EN61000-4-3, Radiated RF</li> <li>EN61000-4-4, Burst Transients</li> <li>EN61000-4-5, Surge</li> <li>EN61000-4-6, Conducted RF</li> <li>EN61000-4-11, Voltage Dips and Interruptions</li> </ul>



**Note:** The standards compliance of the Mediatrix 1102 are printed on a sticker located on the bottom of the unit.

---

## Disclaimers

The following are the disclaimers related to the Mediatrix 1102.

### 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 Mediatrix Telecom, Inc. could void the user's authority to operate the equipment.

---

### CE Marking



#### DECLARATION OF CONFORMITY

We Mediatrix Telecom, Inc. 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 Mediatrix Telecom, Inc. at the above address.

**10 BaseT** An Ethernet local area network which works on twisted pair wiring.

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

**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 ( $\mu$ )-law standard. See also *mu ( $\mu$ )-law*.

**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 (3) digits and is used with a NXX (office code) number. For example, in the North American telephone number 561-955-1212, the numbers are defined as follows:

**Table 90:** 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 defined as xZABPQ 12 34, where:

**Table 91:** France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.
Z	(regional) geographical zone of the number (in France, there are 5 zones). It has two (2) digits.
ABPQ	First 4 digits corresponding to a local zone defined by central offices.

**Table 91:** France Numbering Plan (Continued)

No.	Description
12 34	Unique number to reach a specific destination.

In this context, the area code corresponds to the Z portion of the numbering plan. Since 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.

**Battery feed, Over-voltage protection, Ringing, Signalling, Coding, Hybrid, and Testing (BORSCHT)**

A group of functions provided to an analog line from a line circuit of a digital central office switch.

**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.

**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 example, 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.

---

<b>Dynamic Host Configuration Protocol (DHCP)</b>	TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.
<b>Echo Cancellation</b>	Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.
<b>Far End Disconnect</b>	This term 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 clear-down tone, or a wink.
<b>Federal Communications Commission (FCC)</b>	U.S. government regulatory body for radio, television, and interstate telecommunications services and international services originating in the United States.
<b>Foreign Exchange Service/Station (FXS)</b>	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. A FXS line is normally connected to a standard telephone, fax or modem.
<b>G.711</b>	ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48, 56, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.
<b>G.723.1</b>	A codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.
<b>G.729/G.729A</b>	A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).
<b>Gateway</b>	A device that links two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).
<b>International Telecommunication Union (ITU)</b>	Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

- 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 neighboring 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** It includes a web-based provisioning client, a 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.

- Mu ( $\mu$ )-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).
- 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. UNIX was selected as the basis for a standard system interface partly because it was "manufacturer-neutral." However, several major versions of UNIX existed so there was a need to develop a common denominator system.
- 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.
- Proxy Server** An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.
- Public Switched Telephone Network (PSTN)** The local telephone company network that carries voice data over analog telephone lines.
- Quality of Service (QoS)** Quality of Service is a measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).
- Real Time Control Protocol (RTCP)** RTCP is the control protocol designed to work in conjunction with RTP. It is standardized in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.
- Realtime Transport Protocol (RTP)** An IETF standard for streaming realtime multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.
- Registrar Server** A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.
- 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, for example a Windows NT Server.
- Session Initiation Protocol (SIP)** A protocol for transporting call setup, routing, authentication, and other feature messages to endpoints within the IP domain, whether those messages originate from outside the IP cloud over SCN resources or within the cloud.
- Simple Network Management Protocol (SNMP)** A standard of network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol / Internet Protocol (TCP/IP) suite and defined in RFC 1157.
- Simple Network Time Protocol (SNTP)** SNTP, which is an adaptation of the Network Time Protocol (NTP), is widely used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time- synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronization source and network paths.
- 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.

---

<b>Terminal</b>	Device capable of sending or receiving data over a data communications channel.
<b>Transmission Control Protocol/Internet Protocol (TCP/IP)</b>	A suite of communications protocols developed by the Department of Defense in the 1970s that connects hosts on the Internet and provides the standards for transmitting data over networks.
<b>Trivial File Transfer Protocol (TFTP)</b>	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.
<b>User Datagram Protocol (UDP)</b>	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.
<b>Voice Over IP (VoIP)</b>	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.
<b>Wide Area Network (WAN)</b>	A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

# List of Acronyms

AWG	American Wire Gauge
BORSCHT	Battery feed, Over-voltage protection, Ringing, Signalling, Coding, Hybrid, and Testing
CE	Cummunauté européenne (French)
CNG	Comfort Noise Generator
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DTMF	Dual Tone Multi-Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
FXS	Foreign Exchange Service/Station
GMT	Greenwich Mean Time
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITSP	Internet Telephony Service Provider
kbps	Kilobits Per Second
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Media Access Control
Mb/s	Megabits Per Second
MIB	Management Information Base

---

ms	millisecond
NAT	Name Address Translation
PBX	Private Branch eXchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comment
RTCP	Real-Time Control Protocol
RTP	Real-Time Protocol
SCN	Switched Circuit Network
SIP	Session Initiation Protocol
SLIC	Subscriber's Line Interface Circuit
SME	Small and Medium-sized Enterprise
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UL	Underwriters Laboratories Incorporated
UTC	Universal Time Coordinated
VAD	Voice Activity Detection
VBD	Voice Band Data
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	eXtensible Markup Language

# Index

## Numerics

- 10 BaseT 5, 14, 41
  - defined 155
- 100 BaseT 5, 14, 41
  - defined 155
- 802.1q, in QoS 118

## A

- acronyms 163
- A-Law 63
  - defined 155
- analog modem, feature 2
- area code
  - defined 155
- authentication information 77
- automatic speed dialing 105

## B

- BORSCHT
  - defined 156

## C

- call
  - forward
    - on busy 98
    - on no answer 100
    - unconditional 97
  - hold 96
  - placing 49
  - second 103
  - transfer
    - attended 104
    - blind 103
    - waiting 101
- caller ID
  - DTMF signalling 28
  - FSK generation 48
- codec, setting 63
- comfort noise 61
- compliance to standards. *See standards compliance*
- configuration
  - file 44
  - using a GUI 8, 44
- configuring the software
  - changing parameters 8
  - configuration file 44
  - IP addresses 43

- configuring the software (*continued*)
  - MIB. *see SNMP*
  - subnet mask 43
  - using DHCP (dynamic) 27
  - using Static 27
- connecting the unit 14
- connectors
  - Computer 5
  - Default Settings 6
  - Network 5
  - Phone/Fax 6
  - power 6
- country specific parameters 143
  - setting 46
- current drop, detecting 67

## D

- Default Settings
  - factory settings procedure 20
  - in recovery mode 18
- DHCP server
  - configuring 25
  - defined 157
  - entering IP addresses 37
  - network configuration 26
  - requirement 11
  - site specific option 33
  - vendor class ID 35
  - vendor specific option 35
- Dial Map. *see digit map*
- Differentiated Services (DS) Field, in QoS 117
- digit map
  - # and \* characters 87
  - combining two expressions 87
  - definition 85
  - examples
    - PBX emulation 93
    - standard calls 91
  - refused 90
  - rules 88
  - special characters 86
  - timer 87
  - using 86
  - validating 88
- DNS
  - defined 156
  - requirement 11
- downloading software 51
- DTMF
  - defined 156

DTMF (*continued*)  
out-of-band, feature 3

## E

echo cancel 61  
emergency software download 56  
end user technical support xviii  
Ethernet connection, setting speed of 41

## F

factory settings, reverting to 20  
far-end disconnect  
defined 157  
fax  
disabling the call waiting tone 101  
feature 2  
user gain vs communication quality 62  
features  
analog modem 2  
Ethernet ports 2  
fax interface 2  
FXS port 2  
out-of-band DTMF 3  
RTCP 3  
flash hook, setting 123  
Foreign Exchange Service/Station (FXS)  
defined 157  
FSK generation, caller ID 48

## G

G.711 63  
defined 157  
G.723.1 63  
defined 157  
G.729AB 63  
defined 157  
gateway  
defined 157  
GUI, using a 8, 44

## H

hardware  
cleaning 129  
condensation 129  
front indicators 4  
proper location 129  
rear connections 5  
hold, putting a call on 96  
humidity level 12

## I

IEEE 802.1q, in QoS 118  
indicators of the hardware 4  
installation  
connecting the hardware 14  
setting up the unit for the first time 15  
verifying 21  
intended audience xiii  
Internet Protocol (IP)  
defined 158  
IP address  
defining  
decimal 23  
hexadecimal 24  
octal 24  
entering 37  
locating 23  
Management Server 113  
SIP outbound proxy 73  
SIP Proxy server 71  
SIP Registrar server 69  
SNTP server 107  
syslog daemon 121  
TFTP server 51  
using DHCP 27  
using static 27  
vocal identification of 17  
IP address call 106

## J

jitter  
buffer protection 59  
defined 158

## L

LAN  
cable 21  
defined 158  
LEDs  
behavior in boot mode 17  
behavior in download mode 56  
defined 158  
In Use 139  
LAN 139  
patterns  
AdminMode 136  
Booting 136  
DefaultSettings ending 137  
DiagFailed 138  
ImageDownloadError 137  
ImageDownloadInProgress 137

LEDs (*continued*)

## patterns

- InitFailed 138
- NormalMode 136, 138
- recovery mode 140
- RecoveryMode 136
- RecoveryModePending 137
- ResetPending 137

Power 140

Ready 139

states 135

location, setting country 46

loop current, setting 67

**M**

MAC address 15

defined 158

vocal identification of 17

Management Server

defined 158

using 113

using DHCP information 114

using Static information 114

MIB

defined 158

in SNMP protocol 7

see *parameters*

mounting

on a wall 13

Mu ( $\mu$ )-Law 63

defined 159

**N**

NAT/Firewall

setting IP address of 80

traversal scheme 80

**O**

operating temperature 12

out-of-band DTMF feature 3

overview of the product 1

**P**

package contents 12

packetization time, setting for codecs 65

parameters

modifying 8

using a GUI 8, 44

placing a call 49

ports

defined 159

DSP variables

comfort noise 61

echo cancel 61

jitter buffer protection 59

voice activity detection 60

locking/unlocking 59

setting codecs 63

packetization time 65

preferred codec 64

user gain variables 62

voice variables 59

product overview 1

provisioning

configuration file 44

initial sequence 16

MIB files 46

restart handler 46

**Q**

QoS

defined 160

Differentiated Services (DS) Field 117

IEEE 802.1q 118

VLAN 120

**R**

rear connections 5

recovery mode

LED patterns 140

resetting in 18

related documentation xiv

Replaces header, in SIP 81

requirements 11

restart

software-initiated 21

RTCP, feature 3

**S**

safety recommendations xvii, 12

safety warnings

Circuit Breaker (15A) xvi

LAN Port xvii

No. 26 AWG xvi

Product Disposal xvi

Socket Outlet xvii

TN Power xvi

session timer

enabling 76

- session timer (*continued*)
    - session expiration delay
      - maximum 76
    - version supported, setting 83
  - signaling protocol
    - SIP. see *SIP, setting*
  - SIP server
    - requirement 11
  - SIP, setting
    - configuration 69
    - NAT traversal scheme 80
    - NAT/Firewall 80
    - replaces configuration 81
    - session timer 76
      - session expiration delay, maximum 76
      - session expiration delay, minimum 76
      - version supported 83
    - SIP outbound proxy
      - using DHCP information 73
      - using Static information 74
    - SIP Proxy server
      - using DHCP information 71
      - using Static information 72
    - SIP Registrar server
      - using DHCP information 69
      - using Static information 70
    - SIP User Agents
      - authentication information 77
      - display name 75
      - main user name 75
      - other accepted user names 75
      - setting information 75
    - transmission timeout 83
    - urgent gateway
      - enabling 78
  - site specific information 33
  - site, selecting for unit 12
  - SNMP
    - configuring 29
    - defined 161
    - definition 6
    - MIB 7
    - versions 7
  - SNTP
    - defined 161
    - enabling 106
    - time zone
      - defining custom 108
    - using DHCP information 107
    - using static information 107
  - software
    - configuring 8, 43
    - downloading
      - configuring TFTP server 51
  - software (*continued*)
    - downloading
      - DHCP vs. Static Configuration 51
      - emergency procedure 56
      - LED states 56
      - procedure 54
      - zip file 51
    - special vocal features 17
      - IP address 17
      - MAC address 17
    - speed dialing, automatic 105
    - standards compliance
      - agency approvals 153
      - CE marking 154
      - emissions 153
      - FCC Part 15 disclaimer 154
      - immunity 153
      - safety standards 153
    - statistics
      - RTP 125
      - setting how to collect 125
      - viewing 125
    - subnet mask, configuring 43
    - Syslog daemon
      - configuring 123
      - definition 121
      - enabling 121
      - requirement 11
      - using DHCP information 121
      - using static information 122
- ## T
- T.38
    - defined 161
    - not supported by other endpoint 130
  - technical support for end user xviii
  - telephony services
    - automatic speed dialing 105
    - call forward
      - on busy 98
      - on no answer 100
      - unconditional 97
    - call transfer - attended transfer 104
    - call transfer - blind transfer 103
    - call waiting 101
    - conference call 104
    - hold 96
    - IP address call 106
    - second call 103
    - temperature, operating 12
    - TFTP server
      - configuring 51
      - defined 162

TFTP server (*continued*)  
    requirement 11  
    using DHCP information 52  
    using Static information 53  
time zone  
    defining custom 108  
transfer  
    version supported, setting 82  
transmission timeout, setting 83  
troubleshooting  
    all LED's are off 130  
    cannot establish a call to endpoint 130  
    cannot make a call 130  
    cannot set a variable 133  
    DHCP unreachable 131  
    download path not recognized 132  
    poor line condition during fax transmission 131  
    SNMP network management software cannot access  
    the unit 133  
    solving general operations problems 130  
    solving software problems 132  
    there is no response when trying to access the unit 133  
    traps are not received by the SNMP network manager  
    133  
    unit unreachable after changing Ethernet speed 131  
    when viewing a table, the unit does not respond 134

## U

using the unit 43  
using this manual xiv

## V

vendor specific information 35  
verifying the installation 21  
viewing the statistics and performances 125  
VLAN, in QoS 120  
vocal features, special 17  
    IP address 17  
    MAC address 17  
voice activity detection 60

## W

wall-mounting the unit 13  
what's new in this version xiii



## READER'S FEEDBACK

Mediatrix Telecom, Inc. 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:

Mediatrix Telecom, Inc.  
Attention: Documentation Department  
4229, Garlock Street  
Sherbrooke, Quebec Canada J1L 2C8  
FAX: +1 (819) 829-5100

Manual Name: *Mediatrix 1102 Administration Manual (SIP Version)*  
Software Version: 4.3 Revision: L Date: January 14, 2003

	Excellent	Good	Fair	Poor
How would you rate the manual overall?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the <i>Installation instructions</i> effective?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the <i>Configuration instructions</i> effective?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the manual properly <i>organized</i> ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the <i>diagrams</i> clear, easy to understand and useful?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the <i>suggested</i> and <i>default values</i> useful?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the <i>index</i> useful?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the <i>glossary</i> accurate?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Did you find any errors in the manual? (Please reference page, paragraph, table, or figure number) \_\_\_\_\_

\_\_\_\_\_

How might we improve this manual? \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Name \_\_\_\_\_ Title \_\_\_\_\_

Company Name \_\_\_\_\_

Address \_\_\_\_\_ Telephone ( ) \_\_\_\_\_

\_\_\_\_\_

Thank you for taking the time to fill out this form.

