EMPOWERING THE EDGE OF THE IP NETWORK

Mediatrix® 2102

Reference Manual

SIP Version

Product Version 5.0

Document Revision 06

March 3, 2005

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

Mediatrix® 2102 Reference Manual (SIP Version)

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

Supplementary Copyright Information

CMU/UCD copyright notice: (BSD like)

Networks Associates Technology, Inc copyright notice (BSD)

Cambridge Broadband Ltd. copyright notice (BSD)

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.
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 (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@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).

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 (eay@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)"

Contents

Preface

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 15

Chapter 16

Chapter 17

Chapter 18

Chapter 19

Chapter 20

Chapter 21

Chapter 22

Chapter 23

Chapter 24

Chapter 25

Chapter 26

Chapter 27

Chapter 28

Appendix A

Appendix B

Appendix C

Appendix D

Appendix E

Appendix F

Appendix G

PREFACE

P

About this Manual

Thank you for purchasing the Mediatrix 2102 from Mediatrix.

The Mediatrix 2102 offers two Ethernet connectors switches enabling to establish two connections between conventional analog telephones or Group 3 fax machines and either a WAN, a LAN or a personal computer. It can be used to provide connectivity to broadband access equipment for a Service Provider's IP Telephony offering to residential or SME markets.

To ensure maximum flexibility, the Mediatrix 2102 can:

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

Document Objectives

The *Mediatrix 2102 Reference Manual* provides technical information for the Mediatrix 2102.

Use the *Mediatrix 2102 Reference Manual* in conjunction with the appropriate publications listed in "Related Documentation" on page xx.

New Documentation

This new version of the Mediatrix 2102 introduces changes to the documentation. The information formerly in the User's Manual has now been included in this *Reference Manual*.

If you are an end-user who is looking for information on how to use the features on your telephone, refer to the following chapters:

Table 1: End-User Information

Information	Where to get it
Call processes, how to make calls, and emergency calls	"Chapter 19 - Telephony Features" on page 197
How to use the subscriber services such as call forward, call transfer, etc.	"Chapter 20 - Subscriber Services" on page 203
How to use the telephony attributes such as an automatic call, IP address call service, etc.	"Chapter 21 - Telephony Attributes" on page 217

What's New in this Version

- Possibility to define a substitute VLAN tagging. See "VLAN Substitution" on page 231 for details.

Intended Audience

This manual provides all the technical information needed to install and manage the Mediatrix 2102. It is intended for network administrators and system managers who install and set up network equipment; consequently, it assumes a basic working knowledge of LANs.

From the perspective of the LAN administrator, a Mediatrix 2102 presents itself like another device to add to the LAN. It requires the same kind of TCP/IP addressing. The Mediatrix 2102 can also use a DHCP server on the LAN to automatically receive its IP configuration assignment.

Related Documentation

In addition to this manual, the Mediatrix 2102 document set includes the following:

- *MIB Reference Manual*

  Lists and explains all parameters in the MIB structure.

- *Mediatrix 2102 Hardware Installation Guide*

  This printed booklet allows you to quickly setup and work with the Mediatrix 2102.

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

Document Structure

The Mediatrix 2102 Reference Manual contains the following information.

Table 2: Mediatrix 2102 Reference Manual Chapter/Appendices

Title	Summary
“Chapter 1 - Installation” on page 1	Describes the various installation scenarios of the Mediatrix 2102. Also presents the possible states and LED patterns of the Mediatrix 2102, as seen from an operator perspective.
“Chapter 2 - Web Interface” on page 25	Describes how to access the embedded web server of the Mediatrix 2102 to set parameters by using the HTTP protocol.
“Chapter 3 - MIB Structure and SNMP” on page 39	Describes how the Mediatrix 2102 uses the SNMP protocol for its configuration.
“Chapter 4 - IP Address and Network Configuration” on page 51	Describes how to set IP information in the Mediatrix 2102 and how to configure a DHCP server.
“Chapter 5 - SIP Servers” on page 71	Describes how to configure the Mediatrix 2102 to properly use the SIP servers.
“Chapter 6 - DNS SRV Configuration” on page 79	Describes the Mediatrix 2102’s behaviour with a DNS SRV.
“Chapter 7 - Country-Specific Configuration” on page 83	Describes how to set the Mediatrix 2102 with the proper country settings.
“Chapter 8 - Transparent Address Sharing” on page 87	Explains how to properly configure the Transparent Address Sharing service for a cable or DSL modem.

Table 2: Mediatrix 2102 Reference Manual Chapter/Appendices (Continued)

Title	Summary
“Chapter 9 - Configuration File Download” on page 107	Describes how to use the configuration file download feature to update the Mediatrix 2102 configuration.
“Chapter 10 - Software Download” on page 125	Describes how to download a software version available on the designated software server into the Mediatrix 2102.
“Chapter 11 - Line Configuration” on page 139	Describes the features available on the lines connected to the Mediatrix 2102.
“Chapter 12 - Voice Transmissions” on page 145	Describes the various codecs the Mediatrix 2102 supports for transmitting audio signals.
“Chapter 13 - Fax Transmission” on page 157	Describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 2102.
“Chapter 14 - Bypass Configuration” on page 161	Describes the Bypass feature that can be used in the event of a power failure or network failure.
“Chapter 15 - SIP Protocol Features” on page 163	Describes the SIP-specific feature to set up to properly use the SIP signalling programs and information defined in the Mediatrix SIP stack.
“Chapter 16 - STUN Configuration” on page 181	Describes how to configure the STUN client of the Mediatrix 2102.
“Chapter 17 - SNTP Settings” on page 183	Describes how to configure the Mediatrix 2102 to enable the notion of time (date, month, time) into it.
“Chapter 18 - Digit Maps” on page 187	Describes how to use a Digit Map to compare the number users dialed to a string of arguments.
“Chapter 19 - Telephony Features” on page 197	Explains how to perform basic calls with the Mediatrix 2102 and set the telephony variables of the unit to define the way it handles calls.
“Chapter 20 - Subscriber Services” on page 203	Describes how to set and use the subscriber services available on the user’s telephone.
“Chapter 21 - Telephony Attributes” on page 217	Describes the telephony attributes available on the Mediatrix 2102.
“Chapter 22 - Message Waiting Indicator” on page 221	Explains how to set the Mediatrix 2102 to use the Message Waiting Indicator service.
“Chapter 23 - Management Server Configuration” on page 225	Describes how to configure the Mediatrix 2102 to connect to a module or software that is used to remotely set up Mediatrix units.
“Chapter 24 - Quality of Service (QoS)” on page 227	Defines the QoS (Quality of Service) features available on the Mediatrix 2102.
“Chapter 25 - Syslog Daemon” on page 233	Describes how to configure and use the Syslog daemon.
“Chapter 26 - Statistics” on page 237	Defines the statistics the Mediatrix 2102 can collect.
“Chapter 27 - Maximum Transmission Unit (MTU)” on page 241	Describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 2102.

Table 2: Mediatrix 2102 Reference Manual Chapter/Appendices (Continued)

Title	Summary
"Chapter 28 - Troubleshooting" on page 243	Examines some of the problems you may experience when connecting the Mediatrix 2102 to the network and provides possible solutions.
"Appendix A - Standards Compliance and Safety Information" on page 255	Lists the various standards compliance of the Mediatrix 2102.
"Appendix B - Standard Hardware Information" on page 261	Lists the technical hardware information of the Mediatrix 2102.
"Appendix C - Cabling Considerations" on page 267	Describes the pin-to-pin connections for cables used with the Mediatrix 2102.
"Appendix D - Country-Specific Parameters" on page 269	Lists the various parameters specific to a country such as loss plan, tones and rings, etc.

Document Conventions

The following information provides an explanation of the symbols that appear on the Mediatrix 2102 and in the documentation for the product.

Warning Definition

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

Where to find Translated Warning Definition

For safety and warning information, see "Appendix A - Standards Compliance and Safety Information" on page 255.

This Appendix describes the international agency compliance and safety information for the Mediatrix 2102. It also includes a translation of the safety warning listed in the previous section.

Other Conventions

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

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

☞ **Note:** Note indicates important information about the current topic.

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

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

SCN vs PSTN

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

Standards Supported

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

The Mediatrix 2102's implementations are ***based*** on the standards, so it's possible that some behaviour differs from the official standards.

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

Obtaining Documentation

These sections explain how to obtain documentation from Mediatrix.

World Wide Web

Registered Mediatrix Partners can access and download the most current Mediatrix documentation on the World Wide Web from the Mediatrix Partner Support Site at http://www.mediatrix.com/support_login.php. To access the site, you need a user name and a password.

If you are not a Registered Mediatrix Partner and would like to become one, there are two possibilities:

- If you have purchased your units from Mediatrix, contact your Mediatrix sales representative.
- If you don't have a Mediatrix sales representative, contact sales@mediatrix.com to request information on how to become a Registered Mediatrix Partner.

Documentation CD-ROM

The Mediatrix 2102 documentation is available in a Documentation CD-ROM package that you can order at any time.

You can order Mediatrix documentation in these ways:

- If you have purchased your units from Mediatrix, contact your Mediatrix sales representative.
- If you don't have a Mediatrix sales representative, contact sales@mediatrix.com to request information on how to order a Documentation CD-ROM.

Documentation Feedback

Mediatrix 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

We appreciate your comments.

Mediatrix Products

Mediatrix VoIP products and solutions are designed for immediate deployment within existing network architectures – delivering on the promises of VoIP today. Mediatrix has achieved seamless interoperability with softswitches, SIP servers, H.323 gatekeepers and MGCP call agents of leading VoIP vendors.

Analog Series

Mediatrix analog series access devices and gateways connect conventional telephones, fax machines, legacy PBX and Key Systems to an IP network, as well as provide SCN connectivity to next-generation IP PBX and Key Systems.

Mediatrix 1102 – Two-Port FXS Access Device

VoIP access device equipped with two FXS ports and two 10/100 BaseT Ethernet ports. It serves as an ideal CPE platform for integration with an existing IP telephony architecture deployed by service providers, carriers or system integrators.

Mediatrix 1104 – Four-Port FXS Access Device

VoIP access device equipped with four FXS ports and one 10/100 BaseT Ethernet port. It is functionally designed for desktop or wiring closet installation and is an ideal enterprise CPE platform for integration with an existing IP telephony architecture.

Mediatrix 1124 – 24-Port FXS Access Device

VoIP access device equipped with a single RJ-21 TELCO connector providing twenty-four FXS extensions and one 10/100 BaseT Ethernet port. It is designed for multi-dwelling unit / multi-tenant unit (MDU/MTU) applications and is an ideal solution for legacy integration with an existing IP telephony architecture.

Mediatrix 1204 – Four-Port FXO Analog Gateway

Analog VoIP gateway equipped with four FXO ports and one 10/100 BaseT Ethernet port. It can connect analog SCN lines and legacy PBX Systems to an IP telephony network. It is a cost-effective gateway suitable for small and medium size enterprises.

Mediatrix 2102 – Two-Port FXS Access Device

VoIP Adapter that connects up to two analog phones or fax machines to a broadband access equipment, allowing Service Providers to offer IP telephony services to residential users.

Digital Series

Mediatrix digital series gateways and routers connect ISDN BRI (Basic Rate Interface) and ISDN T1/E1 PRI (Primary Rate Interface) interfaces of the SCN and of legacy PBX and Key Systems to an IP network. The routers can connect a local LAN to provide a comprehensive voice and data solution in one box.

Mediatrix 1400 – BRI VoIP Gateways

The Mediatrix 1400 series BRI VoIP gateways provide four (Mediatrix 1402) or eight (Mediatrix 1404) VoIP channels to allow enterprises to lower communications costs over any IP link. They constitute an ideal solution for LAN based voice applications or for connecting to a service provider’s network.

Mediatrix 1500 – T1 PRI VoIP Gateways

The Mediatrix 1500 series T1 PRI VoIP gateways provide 23 (Mediatrix 1531) or 46 (Mediatrix 1532) VoIP channels to allow enterprises to lower communications costs over any IP link. They constitute an ideal solution for enterprise voice applications or for connecting to a service provider’s network.

Mediatrix 1600 – E1 PRI VoIP Gateways

The Mediatrix 1600 series E1 PRI VoIP gateways provide 30 (Mediatrix 1631) or 60 (Mediatrix 1632) VoIP channels to allow enterprises to lower communications costs over any IP link. They constitute an ideal solution for enterprise voice applications or for connecting to a service provider's network.

Mediatrix 2400 – BRI IP Routers

The Mediatrix 2400 series BRI IP routers combine VoIP and call switching with QoS access routing and VPN tunnelling to provide a comprehensive and complete enterprise solution. The Mediatrix 2400 series units are integrated IP routers with two Ethernet ports and two (Mediatrix 2402) or four (Mediatrix 2404) ISDN BRI ports. They constitute an ideal solution for office networks or for connecting to a service provider's network.

Mediatrix 2500 – T1 PRI IP Routers

Designed to address the voice, fax and data transmission needs of enterprises, the Mediatrix 2500 series T1 PRI IP routers combine VoIP and call switching with QoS access routing and VPN. The Mediatrix 2500 series units are integrated IP routers with two Ethernet ports, a serial V.35/X.21 port and one (Mediatrix 2531) or two (Mediatrix 2532) ISDN T1 ports. They constitute an ideal solution for enterprise networks or for connecting to a service provider's network.

Mediatrix 2600 – E1 PRI IP Routers

Designed to address the voice, fax and data transmission needs of enterprises, the Mediatrix 2600 series E1 PRI IP routers combine VoIP and call switching with QoS access routing and VPN. The Mediatrix 2600 series units are integrated IP routers with two Ethernet ports, a serial V.35/X.21 port and one (Mediatrix 2631) or two (Mediatrix 2632) ISDN E1 primary rate interface ports. They constitute an ideal solution for enterprise networks or for connecting to a service provider's network.

Software Applications

Mediatrix Software Applications produce substantial benefits and provide a value-added enhancement to solutions making use of Mediatrix access devices and gateways.

IP Communication Server – SIP Server

The IP Communication Server translates phones numbers into their corresponding network locations. It looks up its database of registered SIP users, or administrator-defined call routing mechanism and rules, to find the network location associated with the called party and returns the information to the calling party.

SIP services are essential components of the IP Communication Server architecture. However, the Route Manager module provides additional intelligence enabling various dial maps and digit manipulation scenarios. For example, calls can be routed to SCN gateways, IVRs or other SIP servers.

Unit Manager Network – Element Management System

User-friendly element management system designed to facilitate the deployment, configuration and provisioning of Mediatrix access devices and gateways.

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

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

- Controlled Implementation of new software.
- Supports SNMP requests: GET, GET NEXT, GET TABLE, GET WALK, SET, TRAP.
- SNMP abstraction layer: configuration can be changed without SNMP MIB knowledge.

The demo version of the Unit Manager Network is located on the Documentation CD-ROM.

See the *Unit Manager Network Administration Manual* for more details on how to use it to configure any Mediatrix 2102 unit on the network.

End User Technical Support

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

CHAPTER

1

Installation

This chapter describes the installation and the initial provisioning of the Mediatrix 2102.

Requirements

The Mediatrix 2102 requires the following items to work properly:

Table 3: Mediatrix 2102 Required Items

Item	Description
Access Concentrator	Supplies PPP settings for the PPPoE connection type.
DHCP Server (optional)	Supplies all network parameters to the Mediatrix 2102 such as the IP address and subnet mask. It is used for automatic configuration. This applies to the DHCP connection type (usually with a cable modem installation).
DNS Server (optional)	Translates domain names into IP addresses.
SIP Server	Manages the active calls of the Mediatrix 2102.
Management Server (optional)	Module or software used to remotely manage and configure the Mediatrix 2102. Such software could be the Mediatrix Unit Manager Network. See "Unit Manager Network – Element Management System" on page xxv for more details.
TFTP Server or HTTP Server	Necessary for software updates.
Syslog Daemon (optional)	Receives all status messages coming from the Mediatrix 2102.

Safety Recommendations

To ensure general safety, follow these guidelines:

- Do not open or disassemble the Mediatrix 2102.
- Do not get the Mediatrix 2102 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 2102 package contains the following items:

- the Mediatrix 2102 unit
- a power cord for the country in which you are using the Mediatrix 2102
- a universal power supply
- a 10/100 BaseT Ethernet RJ-45 cable

- a Quick Start booklet

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

Overview

The Mediatrix 2102 is a standalone Internet telephony access device that connects to virtually any business telephone system supporting standard analog lines.

The Mediatrix 2102 can be used to connect up to two analog phones or fax machines to a broadband access equipment for a Service Provider's IP Telephony offering to residential users.

This version of the Mediatrix 2102 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 2102

The Mediatrix 2102:

- 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 (µ-law, A-law)
    - G.723.1A
    - G.729 A rev. B
    - T.38 (fax) over UDP or TCP
- Supports Quality of Service technologies.
    - Differentiated Services (DS) Field
    - IEEE 802.1q user priority tagging
- Offers an intuitive Web-based management interface to simplify operation and support.

Placing a Call

You can place a call from a telephone or fax connected to a Mediatrix 2102. The unit automatically detects if the call originates from a voice or fax transmission and acts accordingly.

When placing a call, the Mediatrix 2102 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.

When placing an Internet telephony call from one location to another, the voice signals pass through the Mediatrix 2102. 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, and then fed into the corresponding endpoint.

The Mediatrix 2102 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 2102 customers cannot tell that their conversation is being carried over a packet network rather than the traditional SCN.

You can dial on a telephone/fax machine connected to the Mediatrix 2102 as you normally do. Please refer to "Chapter 19 - Telephony Features" on page 197 for more information and call processes examples.

Management Choices

The Mediatrix 2102 offers various management options to configure the unit.

Table 4: Management Options

Management Choice	Description
Web Interface	The Mediatrix 2102 web interface offers the following options: • Password-protected access via basic HTTP authentication, as described in RFC 2617 • User-friendly GUI Refer to "Chapter 2 - Web Interface" on page 25 for more details.
SNMPv1/2/3	The Mediatrix 2102 SNMP feature offers the following options: • Password-protected access • Remote management • Simultaneous management Refer to "Chapter 3 - MIB Structure and SNMP" on page 39 for more details.
Auto-Update	The Mediatrix 2102 auto-update options are as follows: • Frequent polling • Automatic software and configuration files downloads • Configuration file encryption Refer to "Chapter 10 - Software Download" on page 125 and "Chapter 9 - Configuration File Download" on page 107 for more details.

Panels

This section provides an overview of the front and rear panels of the Mediatrix 2102.

Front Indicators

Figure 1 shows the four visual indicators located on the front of the Mediatrix 2102.

Figure 1: Front Panel Indicators

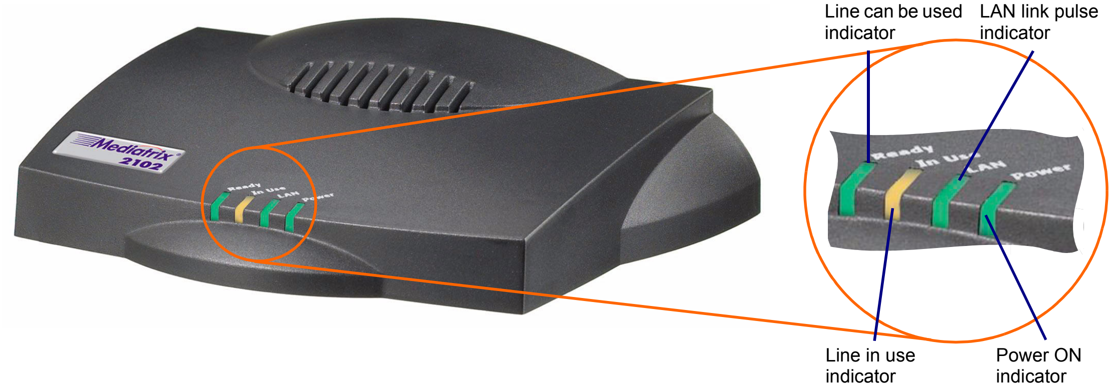


Table 5 describes the LEDs on the front panel of the Mediatrix 2102.

Table 5: Front Panel Indicators

Indicator	Description
Ready	When lit, the Mediatrix 2102 is ready to initiate or receive a call. The unit does not have to be registered to a server.
In Use	When lit, at least one of the FXS lines is in use.
LAN	Provides the state of the network connected to the *Network* connector.
Power	When lit, power is applied to the Mediatrix 2102.

See “LED Indicators” on page 15 for a detailed description of the LED patterns the Mediatrix 2102 may have and the states they represent.

Rear Connectors

The Mediatrix 2102 has several connections that must be properly set. Figure 2 shows the back panel of the Mediatrix 2102.

Figure 2: Back Panel Connectors

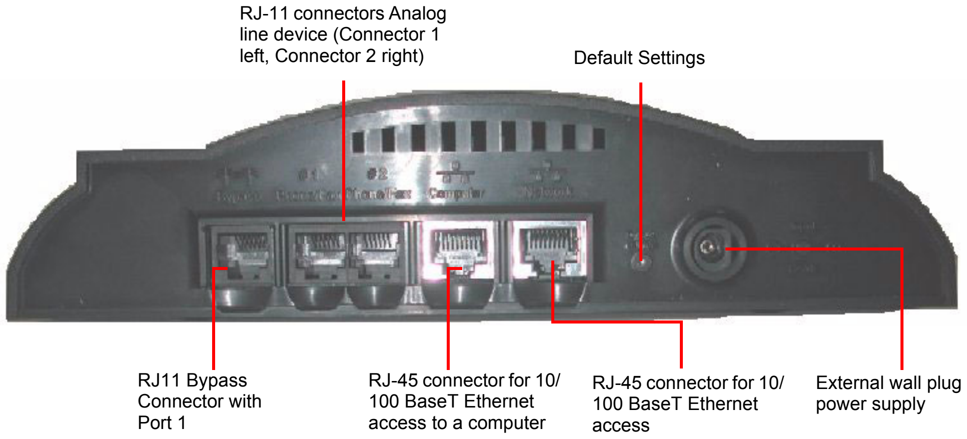

RJ-11 connectors Analog line device (Connector 1 left, Connector 2 right)
Default Settings
RJ11 Bypass Connector with Port 1
RJ-45 connector for 10/100 BaseT Ethernet access to a computer
RJ-45 connector for 10/100 BaseT Ethernet access
External wall plug power supply

Table 6 describes the back panel connections.

Table 6: Back Connections of the Mediatrix 2102

Connection	Description
Network	A 10/100 BaseT Ethernet RJ-45 connector for access to a LAN, WAN or computer.
Computer	A 10/100 BaseT Ethernet RJ-45 connector that can be connected into the network card of a computer.
Bypass	Allows its users to make emergency calls and maintain telephone services in the event of a power outage or network failure. **Note**: This connector is not available on all Mediatrix 2102 units
Phone/Fax	Two RJ-11 connectors to attach a conventional telephone or G3 fax machine. Connector 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 wall plug power supply. The voltage differs depending on the hardware revision of your unit: • Mediatrix 2102 with hardware revision 7: 12 Vdc at 8 W. • Mediatrix 2102 with hardware revision 6: 24 Vdc at 13.2 W.
Default Settings switch	Resets configuration parameters of the Mediatrix 2102 to default (known) values. It can be used to reconfigure the unit. **Warning**: Read Section "Default Settings Switch" on page 20 before attempting to reset the unit.

Choosing a Suitable Installation Site

The Mediatrix 2102 is suited for use in an office or residential environment where it can be wall-mounted or free standing.

Warning: The analog lines of the Mediatrix 2102 are not intended for connection to a telecommunication network that uses outside cable.

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

Location

Install the Mediatrix 2102 in a well-ventilated location where it will not be exposed to high temperature or humidity. Do not install the Mediatrix 2102 in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components.

When deciding where to position the Mediatrix 2102, ensure that:

- The Mediatrix 2102 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 2102.
- The airflow is not restricted around the Mediatrix 2102 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^{o}C and 40^{o}C.
- The humidity is not over 85% and is non-condensing.

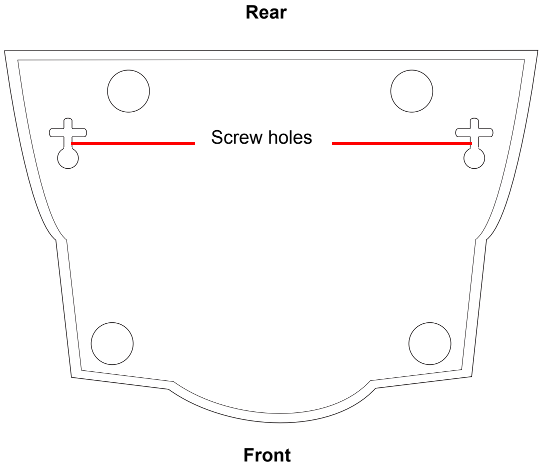
Wall-Mounting

The Mediatrix 2102 has two screw holes on its bottom surface, allowing a single unit to be wall-mounted.

▶ **To wall-mount the Mediatrix 2102:**

1. Disconnect all of the cables from the Mediatrix 2102 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 2102 against the wall (or plywood) as illustrated in Figure 3.

Figure 3: Bottom View - Wall Mounting Screw Holes



You can position the Mediatrix 2102 any way you want. However, Mediatrix 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 2102 over the screws installed in the previous step.
6. Proceed to “Hardware Connection” on page 8.

Free Standing Unit

When installing the Mediatrix 2102 on a desk or table, it should be located at least 20 cm from your monitor, computer casing or other peripherals, including speakers. Never put books or paper on the Mediatrix 2102.

Condensation

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

Cleaning

To clean the Mediatrix 2102, wipe with a soft dry cloth. Do not use volatile liquids such as benzine and thinner that are harmful to the unit casing.

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

Hardware Connection

The Mediatrix 2102 may be installed in various ways. This section describes two of these installations: in a single computer configuration without a router and multi-computer configuration with a router.

Warning: Do not connect the Mediatrix 2102 directly to Analog Telephone Systems.

See “Appendix C - Cabling Considerations” on page 267 for more details on the cables the Mediatrix 2102 uses.

Reserving an IP Address

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

Before connecting the Mediatrix 2102 to the network, Mediatrix strongly recommends that you reserve an IP address in your DHCP server – if you are using one – for the unit you are about to connect. This way, you know the IP address associated with a particular unit.

DHCP servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The Mediatrix 2102 unique identifier is its media access control (MAC) address. You can locate the MAC address as follows:

- It is printed on the label located on the bottom side of the unit.
- It is located in the *sysMgmtMIB* under the *sysMacAddress* variable.
- You can dial the following digits on a telephone connected to the Mediatrix 2102:

  `*#*1`

  The Mediatrix 2102 answers back with its MAC address. See “Special Vocal Features” on page 15 for more details.

Before Proceeding

Most computers are configured by default to automatically obtain an IP address via DHCP. If the computer connected to the Mediatrix 2102 is set with a static IP address, you must change the setting. Please refer to your operating system’s documentation to perform this task.

10/100 BaseT Ethernet RJ-45 Cable

When connecting an Ethernet cable to the Mediatrix 2102, use a standard telecommunication cord with a minimum of 26 AWG wire size.

It is possible to use either a crossover or straight Ethernet cable to connect in the *Network* or *Computer* connectors. These connectors perform automatic MDI / MDIX detection, meaning that they adapt to the type of cable connected to them.

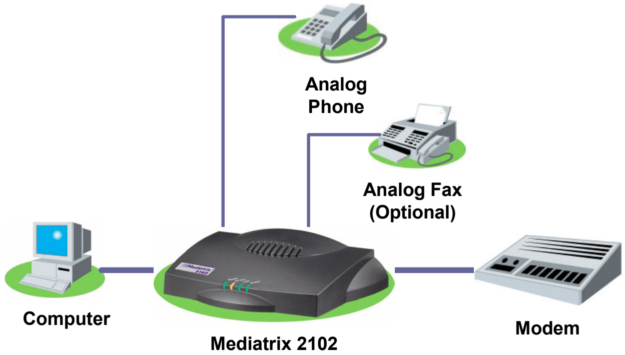
The auto MDI / MDIX feature works only when the connectors are configured in auto detect mode (see “Ethernet Connection Speed” on page 69 for more details).

Whenever you force the Mediatrix 2102 to use a specific Ethernet mode (for example 100Mb Full Duplex), the type of cable to use depends on the other peer. For example, a straight cable is required to connect the Mediatrix 2102 to a hub or a switch, while a crossover cable is required to connect the Mediatrix 2102 to a PC. See “Appendix C - Cabling Considerations” on page 267 for more details.

Single Computer Installation

The following steps describe how to install the Mediatrix 2102 with a single computer. The installation may either be performed with a cable modem or a DSL modem. The resulting layout could be something similar to Figure 4.

Figure 4: Single Computer Network Configuration

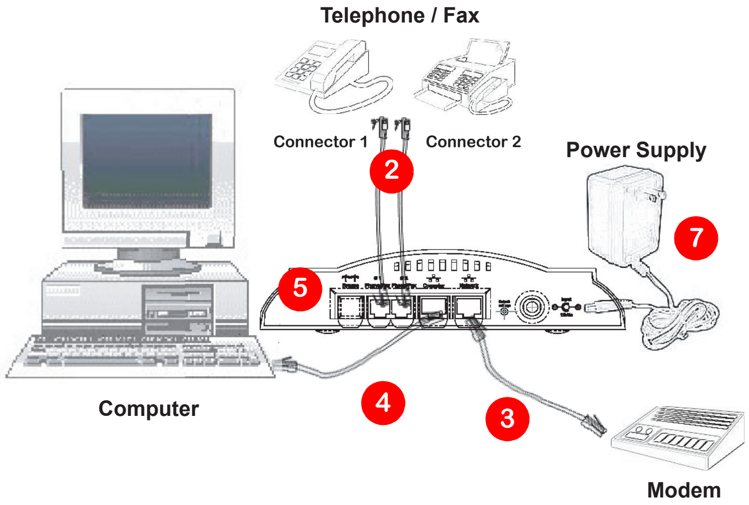


If your Internet connection requires PPPoE authentication, enter a PPPoE user name and password in the Mediatrix 2102 as described in "Administration Page" on page 29.

> **Note:** Do not set the PC to use PPPoE because the Mediatrix 2102 will take care of the authentication.

The following figure is a global illustration of the hardware connections.

Figure 5: Single Computer Installation



▶ **To install the Mediatrix 2102 with a single computer (Mediatrix 2102 312/322):**

1. Before you begin, be sure that all of your hardware is powered off, including the PC, modem, and Mediatrix 2102.
2. Connect analog telephones or fax machines into the *Phone/Fax* connectors.
3. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Network* connector of the Mediatrix 2102. Connect the other end to the cable or DSL modem.

   See "10/100 BaseT Ethernet RJ-45 Cable" on page 8 for more details on this cable.
4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Computer* connector of the Mediatrix 2102. Connect the other end to the network card of your computer.

   See "10/100 BaseT Ethernet RJ-45 Cable" on page 8 for more details on this cable.

5. Connect a SCN line into the *Bypass* connector of the Mediatrix 2102 (optional).

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

6. Power on the cable or DSL modem. Depending on your modem, you may have to wait a few minutes before it properly establishes the Internet connection. Refer to your modem's documentation for more details.

7. Once the modem is ready, connect the power cord to the Mediatrix 2102 and then connect the other end to an electrical outlet.

> **Warning:** The electrical outlet must be installed near the Mediatrix 2102 so that it is easily accessible.

This turns the Mediatrix 2102 on. You should not unplug it when not in use.

- If the *Power* LED is steady on, proceed with the next step.
- If the *Power* LED is blinking, wait until the *In Use* LED blinks before proceeding with the next step. This may take up to three minutes before the Mediatrix 2102 is ready.

Most DSL users will need to enable PPPoE after they have installed the Mediatrix 2102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to "Chapter 2 - Web Interface" on page 25.

8. Power on the PC.

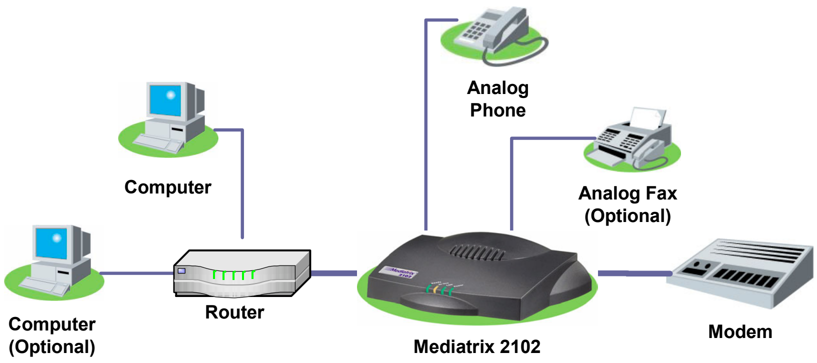
   Your computer does not have to be turned on for the telephone or fax services.

   Mediatrix suggests to access the unit's web interface to configure its basic uplinks parameters. See "Chapter 2 - Web Interface" on page 25 for more details.

Multiple Computer Installation

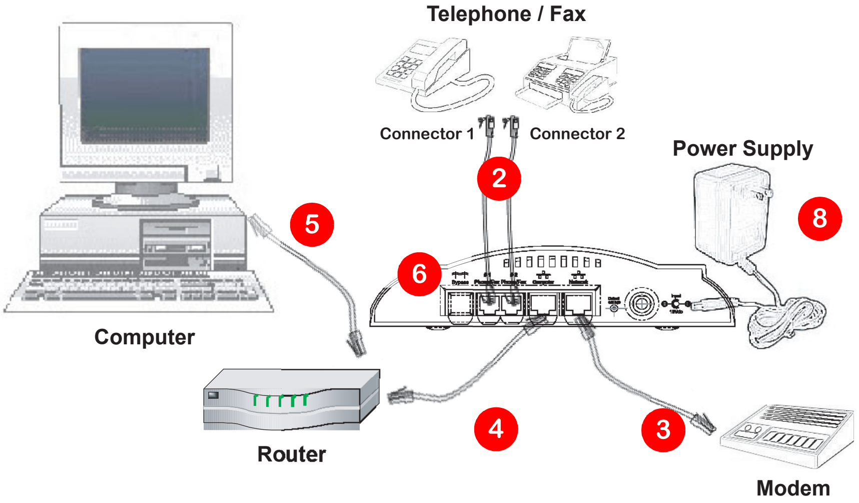
You can use a router with the Mediatrix 2102 to provide Internet connectivity to more than one PC or other device. The following steps describe how to install the Mediatrix 2102 with a router. The installation may either be performed with a cable modem or a DSL modem. The resulting layout could be something similar to Figure 6.

Figure 6: Router Network Configuration



The following figure is a global illustration of the hardware connections.

Figure 7: Router Installation



If your Internet connection requires PPPoE authentication, enter a PPPoE user name and password in the Mediatrix 2102 as described in “Administration Page” on page 29.

> **Note:** Most home routers are configured by default to automatically obtain an IP address via DHCP. If the router connected to the Mediatrix 2102 is set with a static IP address, you must change the setting. Please refer to your router’s documentation to perform this task.

▶ **To install the Mediatrix 2102 with a router:**

1. Before you begin, be sure that all of your hardware is powered off, including the PC, router, modem, and Mediatrix 2102.
2. Connect analog telephones or fax machines into the *Phone/Fax* connectors.
3. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Network* connector of the Mediatrix 2102. Connect the other end to the cable or DSL modem.

   See “10/100 BaseT Ethernet RJ-45 Cable” on page 8 for more details on this cable.

4. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Computer* connector of the Mediatrix 2102. Connect the other end to the WAN / Uplink connector of the router.

   See “10/100 BaseT Ethernet RJ-45 Cable” on page 8 for more details on this cable.

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

   See “10/100 BaseT Ethernet RJ-45 Cable” on page 8 for more details on this cable.

6. Connect a SCN line into the *Bypass* connector of the Mediatrix 2102 (optional).

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

7. Power on the cable or DSL modem. Depending on your modem, you may have to wait a few minutes before it properly establishes the Internet connection. Refer to your modem’s documentation for more details.

8. Once the modem is ready, connect the power cord to the Mediatrix 2102 and then connect the other end to an electrical outlet.

STOP **Warning:** The electrical outlet must be installed near the Mediatrix 2102 so that it is easily accessible.

This turns the Mediatrix 2102 on. You should not unplug it when not in use.

- If the *Power* LED is steady on, proceed with the next step.
- If the *Power* LED is blinking, wait until the *In Use* LED blinks before proceeding with the next step. This may take up to three minutes before the Mediatrix 2102 is ready.

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

   Most DSL users will need to enable PPPoE after they have installed the Mediatrix 2102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to “Chapter 2 - Web Interface” on page 25.

10. Power on the PC.

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

    Mediatrix suggests to access the unit’s web interface to configure its basic uplinks parameters. See “Chapter 2 - Web Interface” on page 25 for more details.

Starting the Mediatrix 2102 for the First Time

This step depends on the WAN connection type set in the web interface (see "Chapter 2 - Web Interface" on page 25).

Most DSL users will need to enable PPPoE after they have installed the Mediatrix 2102. The *Ready* LED will remain off until this setting has been changed. For more informations, refer to "Chapter 2 - Web Interface" on page 25.

If you are using a cable modem, the Mediatrix 2102 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 4 - IP Address and Network Configuration" on page 51 for more details.

If you are experiencing problems, or if you do not want to use a DHCP server, perform a Recovery Mode procedure, as explained in "Recovery Mode" on page 21.

Initial Provisioning Sequence

When starting the Mediatrix 2102 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 2102 hardware as per "Hardware Connection" on page 8.

The Mediatrix 2102 requests its configuration only on the first restart. You can change the configuration at will after the initial provisioning and the provisioning system can refresh the Mediatrix 2102 configuration. The provisioning system consists of the Management Server and a DHCP server. The Management Server includes a provisioning client, provisioning server, and SNMP proxy server.

Provisioning Sequence with a Cable Modem

The following describes the initial provisioning sequence of a Mediatrix 2102 that uses a cable modem.

▶ **Initial provisioning sequence:**

1. When the Mediatrix 2102 starts, it broadcasts a message requesting DHCP services (if the unit is configured to start in DHCP mode).
2. The DHCP server responds with a set of IP addresses and network parameters, one of which is the Mediatrix 2102 IP address.

   The following are some of the network parameters assigned via DHCP:
   - Mediatrix 2102 IP address
   - Subnet Mask
   - Default Router IP address
   - Primary DNS IP address
   - Secondary DNS IP address
   - Management Server IP address and port number (optional)
   - Configuration file server IP address and port number (optional)
   - SIP Servers IP address and port number
3. The Mediatrix 2102 may request its configuration in two ways:
   - by using the IP address of the Management Server to request its configuration.
   - by using a configuration file.

Provisioning Sequence with a DSL Modem

If the WAN connection type is set to PPPoE for a DSL modem (see "Chapter 2 - Web Interface" on page 25), the Mediatrix 2102 does not use a DHCP server to get its network information. It rather discovers a PPP access concentrator and establishes a PPP session with it. This access concentrator sends the following information to the unit:

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

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

Refer to "Chapter 8 - Transparent Address Sharing" on page 87 for more details.

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

▶ **To set static information:**

1. In the *ipAddressConfig* folder, locate the *localHostSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group).
2. Set this variable to **static**.
3. Set a static value for the following network parameters:

Table 7: Network Parameters Static Variables

Variable	Default Static Value
localHostPrimaryDns[a]	"192.168.0.10"
localHostSecondaryDns[a]	"192.168.0.10"
localHostSubnetMask	"255.255.255.0"

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

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

Caution: These variables are vital to the proper operation of the Mediatrix 2102. If a variable of this group is not set properly, the unit may not be able to start or be contacted after it has started.

4. Set other static information as required.

   See "Services" on page 53 for more details.

   The next step would be to configure the IP routing information of the Mediatrix 2102 as described in "Chapter 8 - Transparent Address Sharing" on page 87.

Special Vocal Features

When entering special characters on your telephone pad, the Mediatrix 2102 talks back to you with relevant information.

▶ **To access special vocal features:**

1. Take one of the telephones connected to the Mediatrix 2102.
2. Dial one of the digits sequence on the keypad.

Table 8: Special Vocal Features

Digits to Dial	Information Vocally Sent by the Mediatrix 2102
*#*0	Current IP address of the Mediatrix 2102 (static or DHCP). **Note**: If you are using the Mediatrix 2102 in TAS mode, the LAN IP address is returned.
*#*1	MAC address of the Mediatrix 2102.
*#*2	Current WAN IP address of the Mediatrix 2102.

LED Behaviour in Starting Mode

When the Mediatrix 2102 starts 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 “Default Settings Switch” on page 20 for more details.

LED Indicators

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

Ready LED

The *Ready* LED provides an “at-a-glance” view of the Mediatrix 2102 operational status. It is an aid for installation and on-site support. This LED is:

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

Patterns and meanings of the *Ready* LED are described in Table 10 on page 18.

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

In Use LED

The *In Use* LED provides feedback of the activity on the line. If a line is ringing, off-hook, or displaying information (ADSI), then this LED is ON. The *In Use* LED is ON when at least one element in the *ifAdminUsageState* column is “busy”. Patterns and meanings of the *In Use* LED are described in Table 10 on page 18.

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

LAN LED

The *LAN* LED provides the status of the network connected to the Ethernet connector. Typically, Ethernet connectors are characterized by using two status LEDs: Link and Heartbeat. For the Mediatrix 2102, 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 10 on page 18.

Power LED

The *Power* LED indicates whether the Mediatrix 2102 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 10 on page 18.

LED Patterns

Table 9 describes the different states a Mediatrix unit can have and their associated LED patterns.

Table 9: States and LED Patterns

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
Booting	Follows a hardware start or a reset. If a software download has to take place, the unit enters the *ImageDownloadInProgress* state, otherwise the application is started. In both cases, the *Power* LED blinks while waiting for a DHCP offer, otherwise it is steady ON. If a recovery is in progress, the unit enters the *RecoveryMode* state or the *RecoveryMode Pending* state if the button is pressed, otherwise the *NormalMode* state is selected. **NOTE**: The *LAN* LED starts as Off until the software can activate the HW control.	Off	Off	Off then HW	On or Blink at 1 Hz 75%
Normal Mode	"Normal" state of the unit where calls can be initiated. Each LED has a separate behaviour. If the *groupAdminState* MIB variable is set to "locked", the Mediatrix 2102 enters the *Admin Mode* state.	See "NormalMode LED Pattern Description" on page 18			
AdminMode	"Administration" mode of the unit where calls are not permitted and maintenance actions can be performed. When the *groupAdminState* MIB variable returns to "unlocked", the unit goes back to the *NormalMode* state **NOTE**: The *Ready* and *Power* LEDs blink off phase in turns.	Blink 0.5 Hz 50%	Off	HW	Blink 0.5 Hz 50%

Table 9: States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
Recovery Mode	The IP addresses for local host, image server, syslog server, etc., are set to known values, allowing configuration of the unit. Calls are not allowed. The “known” addresses are temporary (non persistent). Resetting the unit returns it to the *NormalMode* state. **NOTE**: The *Ready* and *Power* LEDs are in phase.	Blink 0.5 Hz 75%	Off	HW	Blink 0.5 Hz 75%
Reset Pending	This is when the button is pressed and held for at least 2 seconds. If the button is released within 5 seconds, data is stored and the unit is reset, otherwise the unit triggers the *RecoveryModePending* state.	Off	Off	Off	Blink 1 Hz 50%
Recovery Mode Pending	Triggered when the button is held at start-time or for at least 7 seconds. If the button is released within 5 seconds after the LED pattern has started and the button was pressed while restarting, the unit enters the *RecoveryMode* state. If the button was pressed at run-time, the unit resets before going to the *RecoveryMode* state. If the button is released after 5 seconds or more, the unit falls into the *DefaultSettingsPending* 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 *RecoveryModePending* state. At run time, if the button is released within 5 seconds, the unit applies default settings, otherwise the action is cancelled and the unit goes back to the Operation Modes state or it resets. At start time, the unit stays in this state until the button is released. When the button is released, the unit applies the default settings and restarts.	On	On	On	On
Image DownloadIn Progress	A software image is downloaded into the unit and written to persistent storage.	All LEDs are blinking at 1 Hz, *one at a time*, from left to right.			
Image Download Error	Triggered after a failure of an image download operation to indicate that the operation failed. After 4 seconds, the unit restarts.	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%	Blink 2 Hz 50%

Table 9: States and LED Patterns (Continued)

State	Description	LEDs Pattern			
		Ready	In Use	LAN	Power
InitFailed	Triggered when bad initialization parameters are detected and the unit cannot start correctly. For instance, the unit enters the *InitFailed* state when it cannot be reached from the IP network because of bad network parameters. However, there is an exception for network parameters: if the configuration is dynamic, the unit stays in the *Booting* state and continues to query the DHCP until it receives valid values. If the configuration is static, the LED pattern indicates that the unit must be reset to default settings or put into recovery mode for maintenance and correction of network values.	Off	Off	Blink 4 Hz 50%	Off
DiagFailed	This state is triggered at start-time when the hardware or software diagnostic fails. This is a critical error and the unit may require RMA.	Off	Off	Off	Blink 4 Hz 50%

NormalMode LED Pattern Description

While in the *NormalMode* state, the LEDs of the Mediatrix 2102 behave independently; the following table indicates the behaviour for each LED.

Table 10: LED Patterns in Operation Mode

LED	Pattern	Meaning
Ready	Steady On	All lines are enabled (operational state).
	Steady Off	All lines are disabled (operational state).
	Blink 0.25 Hz 75%	At least one line is enabled and at least one line is disabled (operational state).
In Use	Steady On	At least one line is busy (usage state).
	Steady Off	All lines are not busy (usage state).
	Blinking 1 Hz 75%	The PPP connection could not be established.
LAN (HW Ctrl)	Steady On	Ethernet connection detected.
	Steady Off	Ethernet connection not detected.
	Blinking (variable rate)	Ethernet activity detected.
Power	Steady On	Power is On.
	Steady Off	Power is Off.
	Blinking 1 Hz 75%	Waiting for a DHCP answer.

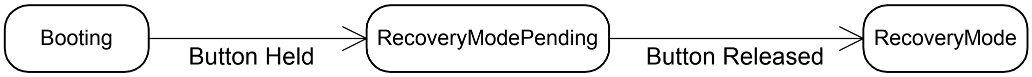
Recovery Mode LED Patterns

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

At Start-Time

When pressing the button at start-time, the state sequence goes as follows:

Figure 8: LED Pattern at Start-Time



This leads to the following LED patterns:

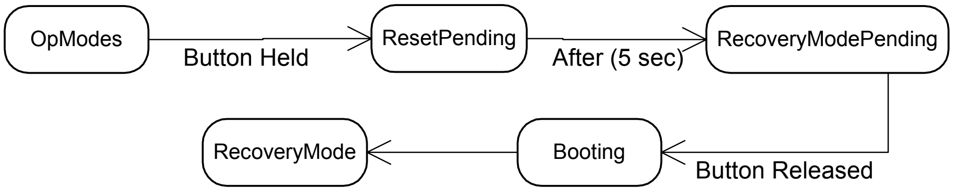
Table 11: LED Patterns at Start-Time

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 9: LED Patterns at Run-Time



This leads to the following LED patterns:

Table 12: 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%

Default Settings Switch

The *Default Settings* switch allows you to:

- Cancel an action that was started.
- Revert to known factory settings if the Mediatrix 2102 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 – you can press the switch while the Mediatrix 2102 is running without powering the unit off. Table 13 describes the actions you can perform in this case.

Table 13: Default Settings Switch Interaction

Default Settings Switch Pressed for:	Action	Comments	LEDs Pattern			
			Ready	In Use	LAN	Power
2 to 5 seconds	Restarts the Mediatrix 2102	No changes are made to the Mediatrix 2102 settings.	Off	Off	Off	Blink
5 to 10 seconds	Restarts the Mediatrix 2102 in Recovery Mode	Sets the Mediatrix 2102 IP address to its default value in the MIB and restarts the unit.	Blink	Blink	Blink	Blink[a]
10 to 15 seconds[b]	Restarts the Mediatrix 2102 in Factory Reset	Deletes the persistent MIB values, creates a new configuration file with the default factory values, and then restarts the unit.	On	On	On	On

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

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

At Start-Time

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

- Pressing the *Default Settings* switch at startup until all the LEDs start blinking restarts the Mediatrix 2102 in “Recovery Mode”.
- Pressing the *Default Settings* switch at startup until all the LEDs stop blinking and remain ON applies the “Factory Reset” procedure. This feature reverts the Mediatrix 2102 back to its default factory settings.

See “LED Indicators” on page 15 for a detailed description of the LED patterns related to the *Default Settings* switch.

Recovery Mode

The recovery mode provides a way to restart the Mediatrix 2102 in a known, static, and minimal state. It is used to recover from a basic configuration error that prevents you to reach the unit through the network. It may serve as a last resort before the Factory reset command. You must perform it in a closed network and on only one Mediatrix 2102 at a time, because the default IP address is the same on every unit.

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

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

▶ **To trigger the Recovery Mode:**

1. With a 10/100 Hub and two 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the hub; one of them is connected into the *Network* connector of the Mediatrix 2102 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 2102 and connect the other end to your computer.

2. Reconfigure the IP address of your computer to *192.168.0.10* and enter the Subnet Mask of *255.255.255.0*. Restart the computer.

3. Insert a small, unbent paper clip into the *Default Settings* switch hole located at the of the Mediatrix 2102.

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

5. Release the paper clip.

Only the *Power* and *Ready* LEDs should go on blinking to inform you that the recovery reset has been performed.

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

The following variables use their default values in the MIBs:

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

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

- imageConfigSource
- configFileFetchingConfigSource
- msConfigSource
- syslogConfigSource
- sntpConfigSource

All the persistent MIB values are kept.

In this mode, 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.

6. When the Mediatrix 2102 has finished its provisioning sequence, perform the changes, and then turn it off, plug it on the network, and turn it on again.

   When restarting, the Mediatrix 2102 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 45 for more details.

Note: The recovery mode does not alter any persistent configuration data of the Mediatrix 2102.

Factory Reset

The Factory reset reverts the Mediatrix 2102 back to its default factory settings. It deletes the persistent MIB values of the unit, including:

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

The Factory reset creates a new configuration file with the default factory values. It should be performed with the Mediatrix 2102 connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, it sends requests indefinitely.

You can disable the Factory reset to avoid users deleting the existing configuration. See "Disabling the Factory Reset" on page 23 for more details.

▶ **To trigger the Factory Reset:**

1. Power the Mediatrix 2102 off.
2. Insert a small, unbent paper clip into the *Default Settings* switch hole located at the rear of the Mediatrix 2102. While depressing the *Default Settings* switch, plug the power cord back in to power up the unit.

   Do not depress before all the LEDs stop blinking and are steadily ON.
3. Release the paper clip.

   The Mediatrix 2102 restarts.

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

   When the Mediatrix 2102 has finished its provisioning sequence, it is ready to be used with a DHCP-provided IP address and MIB parameters.

Note: The Factory reset alters any persistent configuration data of the Mediatrix 2102.

Disabling the Factory Reset

The Mediatrix 2102 offers the possibility to disable its factory reset procedure, even if users depress the *Default Settings* switch. Disabling the factory reset means that users will not be able to revert the Mediatrix 2102 back to its factory settings if there are configuration problems.

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

1. In the *sysAdminMIB*, set the *sysAdminDefaultSettingsEnable* variable to **disable**.

   In this case, users can only perform a Recovery Mode procedure. See "Default Settings Switch" on page 20 for more details.

Software Restart

You can initiate a software restart of the Mediatrix 2102 by using MIB parameters.

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

▶ **To perform a software restart:**

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

   The Mediatrix 2102 restarts.

Restart Behaviour

This feature affects the behaviour of the Mediatrix 2102 when it restarts.

You can instruct the Mediatrix 2102 to check its TCP/IP stack before declaring the restart successful.

This could be useful when the unit is subjected to a broadcast storm (such as a TCP/IP flood) while it is restarting. In this case, and when the TCP/IP stack check is enabled, the unit enters into the rescue mode and cannot be contacted through SNMP. You thus need to restart the Mediatrix 2102 manually. However, when the TCP/IP stack check is disabled, a broadcast storm during a restart will cause the unit to continuously restart until the storm subsides.

▶ **To define the restart behaviour:**

1. In the *bootBehaviorMIB*, enable the *checkTcpIpStackForSuccessfulBoot* variable.

   When the variable is enabled, the TCP/IP stack must initialize properly to consider the restart a success. In a flood scenario, the unit may end up in the rescue mode.

   When the feature is disabled, even if the TCP/IP stack fails to initialize during a TCP/IP flood, the restart is considered successful and the unit does not enter into the rescue mode.

Verifying the Installation

There are two ways to verify that the Mediatrix 2102 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 2102 you want to verify. If the Mediatrix 2102 does not respond, do the following:

- Verify that the LAN cable is securely connected to the Mediatrix 2102 and to the network connector.
- Be sure that you did not connect a crossover network cable.
- Verify the state of the IP network to ensure it is not down (the *LAN* LED should be ON or blinking).

CHAPTER
2

Web Interface

The Mediatrix 2102 contains an embedded web server to set parameters by using the HTTP protocol. This web server may either be accessed via the LAN or the WAN interface of the Mediatrix 2102, depending on the current access limitation. This access limitation may be modified in "Web Interface Access Limitation" on page 37.

Standards Supported	RFC 2616 – Hypertext Transfer protocol - HTTP/1.1.

Introduction

The web interface may be used to:

- View the status of the Mediatrix 2102.
- Set the basic uplink parameters of the Mediatrix 2102.
- Peruse syslog messages the Mediatrix 2102 sends.
- Upload a configuration file to the Mediatrix 2102.
- Modify the password required to access the web interface.

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

▶ To enable the web-based configuration service:

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

Using the Web Interface

To properly access the web interface, you need a web browser that supports frames and HTML 4.0. Suitable web browsers are:

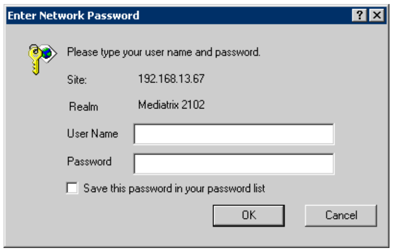
- Netscape® Navigator™ Version 4.7 or above
- Microsoft® Internet Explorer Version 5.0 or above

▶ To use the web interface configuration:

1. In your web browser's address field, type the default IP address of the Mediatrix 2102, which is **192.168.10.1**.

   The following opens:

Figure 10: Enter Network Password Window



Please type your user name and password.

Site: 192.168.13.67

Realm Mediatrix 2102

User Name

Password

☐ Save this password in your password list

2. Enter the proper user name and password.

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

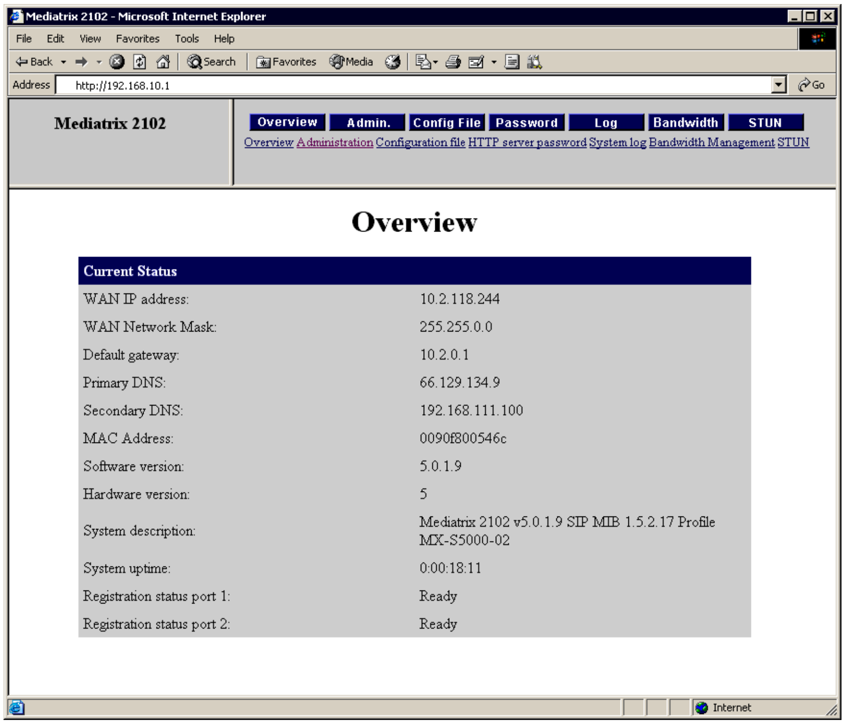
- **User Name**: admin
- **Password**: 1234

Once you have accessed the web interface, you can change the password as described in "HTTP Server Password Page" on page 33.

3. Click *OK*.

The *Overview* web page displays.It stays accessible for as long as the Internet browser used to access the Mediatrix 2102 web interface is opened.

Figure 11: Overview Web Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Mediatrix 2102
Overview
Admin.
Config File
Password
Log
Bandwidth
STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
Internet

Address: http://192.168.10.1

Overview

Current Status	
WAN IP address:	10.2.118.244
WAN Network Mask:	255.255.0.0
Default gateway:	10.2.0.1
Primary DNS:	66.129.134.9
Secondary DNS:	192.168.111.100
MAC Address:	0090f800546c
Software version:	5.0.1.9
Hardware version:	5
System description:	Mediatrix 2102 v5.0.1.9 SIP MIB 1.5.2.17 Profile MX-S5000-02
System uptime:	0:00:18:11
Registration status port 1:	Ready
Registration status port 2:	Ready

Status of the Mediatrix 2102

The *Overview* page displays the current status of the Mediatrix 2102.

Table 14: Status Page

IP Information	Description
WAN IP Address	Value of the *localHostWanAddress* MIB variable, which is the public IP address of the Mediatrix 2102.
WAN Network Mask	If the PPPoE service is enabled, displays an empty string because there is no concept of network mask in PPP links. Otherwise, displays the value of the *localHostSubnetMask* MIB variable.
Default gateway	Value of the *localHostDefaultRouter* MIB variable.
Primary DNS	Value of the *localHostPrimaryDns* MIB variable.
Secondary DNS	Value of the *localHostSecondaryDns* MIB variable.
MAC Address	MAC address of the Mediatrix 2102.
Software version	Software version of the Mediatrix 2102.
Hardware version	Version of the analog circuit board of the Mediatrix 2102.
System description	A textual description of the Mediatrix 2102. It usually includes the full name and version identification of its hardware type, software operating-system, and networking software.
System uptime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
Registration status port1 Registration status port2	May have one of the following: • ***Ready*** if the operational state of the current interface is enabled. • ***Not ready*** if the component is operationally non-functional because of an internal condition that would not allow it to participate in a normal VoIP call.

Menu Frame

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

Table 15: Menu Frame Links

Link	Description
Overview	Links to the *Overview* web page, which displays, in read-only format, the parameters and IP addresses used by the Mediatrix 2102.
Administration	Links to the *Administration* web page, which allows you to set the uplink information used by the Mediatrix 2102. See “Administration Page” on page 29 for more details.
Configuration file	Links to the *Configuration file upload* web page, which allows you to upload a configuration file from a computer to the Mediatrix 2102. See “Configuration File Upload Page” on page 32 for more details.
HTTP server password	Links to the *HTTP server password* web page, which allows you to change the password. See “HTTP Server Password Page” on page 33 for more details.
System log	Links to the *System log* page, which displays, in read-only format, the syslog messages the Mediatrix 2102 sends. See “System Log Page” on page 34 for more details.

Table 15: Menu Frame Links (Continued)

Link	Description
Bandwidth Management	Links to the *Bandwidth Management* page, which allows you to limit the upload bandwidth on the WAN interface. See "Bandwidth Management Page" on page 35 for more details..
STUN	Links to the *STUN* page, which allows you to configure the STUN client of the Mediatrix 2102. See "STUN Page" on page 36 for more details.

Content Frame

The Content frame is displayed in the lower part of the browser window. It contains the various web pages that allow you to manage the Mediatrix 2102.

Administration Page

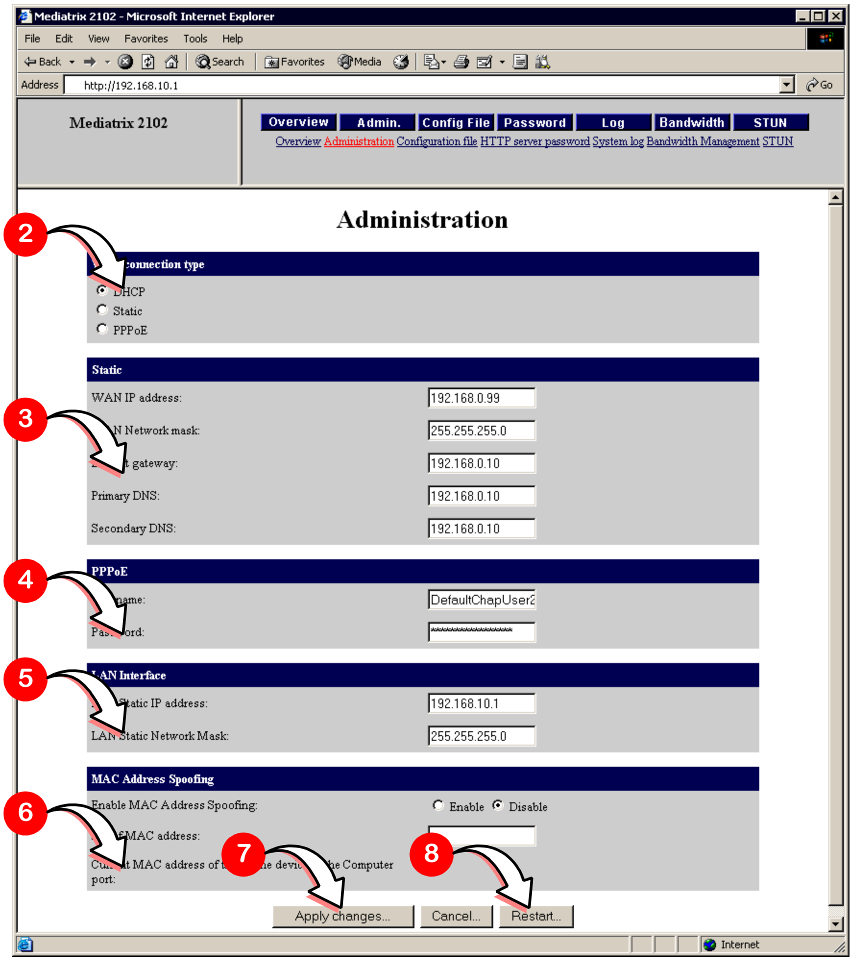
The *Administration* web page allows you to set the uplink connection and IP information the Mediatrix 2102 requires.

▶ **To set administration parameters:**

1. In the web interface, click the *Administration* link or the *Admin* button.

This links to the *Administration* web page.

Figure 12: Administration Web Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
2
3
4
5
6
7
8
Apply changes... Cancel... Restart...
Internet

Address: http://192.168.10.1

Mediatrix 2102

Administration

connection type

● DHCP
○ Static
○ PPPoE

Static

WAN IP address:	192.168.0.99
N Network mask:	255.255.255.0
t gateway:	192.168.0.10
Primary DNS:	192.168.0.10
Secondary DNS:	192.168.0.10

PPPoE

name:	DefaultChapUser2
Pas ord:	****************

AN Interface

tatic IP address:	192.168.10.1
LAN Static Network Mask:	255.255.255.0

MAC Address Spoofing

Enable MAC Address Spoofing:	○ Enable ● Disable
MAC address:	
Cu t MAC address of t e devic he Computer port:	

2. Set the *WAN connection type*.

You have the following choices:

Table 16: WAN Connection Type

Connection Type	Description
DHCP	**Connection to use with a cable modem.** This is the most common connection type with a cable modem. In this connection type, the PPPoE service (*pppoeEnable* variable) is disabled and the configuration source (*localHostSelectConfigSource* variable) is set to “DHCP”. However, some locations may require to manually enter static IP information instead. If this is the case, select the **Static** connection type and proceed to Step 3.
Static	This connection type may be used for locations where cable modems cannot use the DHCP connection type. You are thus required to manually provide the IP information. See Step 3. In this connection type, the PPPoE service (*pppoeEnable* variable) is disabled and the configuration source (*localHostSelectConfigSource* variable) is set to “static”.
PPPoE	**Connection to use with a DSL modem.** This is the most common connection type with a DSL modem. In this connection type, the PPPoE service (*pppoeEnable* variable) is enabled and the configuration source (*localHostSelectConfigSource* variable) is set to “static”. However, some DSL modems may require that you use the DHCP connection type instead.

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

Table 17: IP Addresses Parameters

Parameter	Definition
WAN IP Address	Public IP address of the Mediatrix 2102. This address is used for incoming signalling, media and management traffic.
WAN Network Mask	Subnet mask IP address used by the Mediatrix 2102. The subnet mask enables the network administrator to further divide the host part of the address into two or more subnets.
Default gateway	Default router IP address used by the Mediatrix 2102. A router is a device that connects any number of LANs.
Primary DNS	Primary Domain Name Server IP address used by the Mediatrix 2102. A DNS is an Internet service that translates domain names into IP addresses.
Secondary DNS	Secondary Domain Name Server IP address used by the Mediatrix 2102.

4. If the WAN connection type is **PPPoE** (as set in Step 2), set the PPPoE user name and password.

When connecting to an access concentrator, it may request that the Mediatrix 2102 identifies itself with a specific user name and password.

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

5. Set the static IP address and network mask of the LAN interface.

This is the IP information of the *Computer* connector, where you connect the PC or other IP equipment. The LAN interface is normally used to connect a PC that will have access to the WAN by sharing the Mediatrix 2102 WAN address. See “LAN Interface” on page 95 for more details.

6. If applicable, enable the MAC Address Spoofing feature.

Spoofing the MAC address is useful in the case of ISPs that use the MAC address of the device connected to the *Computer* interface of the Mediatrix 2102 (e.g., a PC) to identify the connection.

Enter the proper MAC address in the *Spoof MAC address* field. The current MAC address of the online device in the *Computer* connector is displayed below the field. A valid MAC address is a series of 12 alphanumeric characters without colons. See "MAC Address Spoofing" on page 95 for more details.

The following MAC addresses are not allowed:

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

7. Click *Apply changes*.

The Mediatrix 2102 validates the changes and a feedback message displays the applied value. The display format of the values is based on the validation results.

Table 18: Display Formats in Web Page

Format	Meaning
Normal text format	The new value is the same as the previous value entered via the web page.
Bold text format	The new value is valid and different from the previous value entered via the web page.
Text in an editable box	The new value is invalid.

Depending on validation results, some messages are displayed in addition to the configuration values.

- If at least one modified value is valid, a message informs you that new values are applied.
- If one or more non-dynamic value was changed, a message informs you that the Mediatrix 2102 must be restarted.
- If at least one modified value is invalid, a message informs you that some values are invalid.

Most changes are not dynamic and require to restart the Mediatrix 2102.

8. Click *Restart*.

This restarts the Mediatrix 2102. If the unit is in use when you click *Restart*, all calls are terminated.

Configuration File Upload Page

The *Configuration file upload* web page allows you to upload a configuration file from the computer connected to the *Computer* connector of the Mediatrix 2102 into the unit.

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

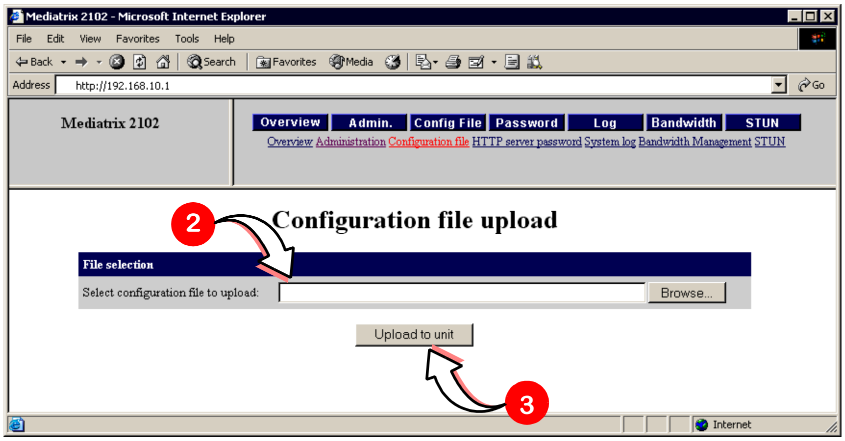
See “Chapter 9 - Configuration File Download” on page 107 for more information on configuration files.

▶ **To upload a configuration file:**

1. In the web interface, click the *Configuration* link or the *Config File* button.

   This links to the *Configuration file upload* web page.

Figure 13: Configuration file upload Web Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Mediatrix 2102
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
Configuration file upload
File selection
Browse...
Upload to unit
2
3
Internet

Address: http://192.168.10.1

Select configuration file to upload:

2. Select the configuration file you want to upload to the Mediatrix 2102 in the *Select configuration file to upload* field.

   You can click the *Browse* button to select a file. This button may not be available, depending on the web browser you are using.

3. Click the *Upload to unit* button.

   If a valid configuration file is successfully uploaded, then the Mediatrix 2102 automatically restarts to apply all the new settings. If the Mediatrix 2102 does not restart, this could mean the upload failed.

HTTP Server Password Page

Standards Supported	RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication

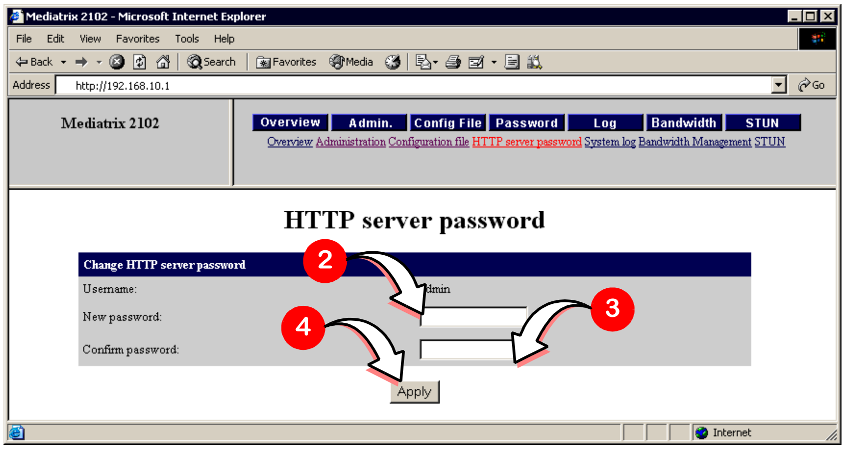
The *HTTP server password* page allows you to modify the default password to access the web interface. The Mediatrix 2102 supports basic HTTP authentication, as described in RFC 2617.

▶ **To change the password:**

1. In the web interface, click the *HTTP server password* link or the *Password* button of the Menu frame.

The following opens:

Figure 14: HTTP server password Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
Apply
Internet
2
3
4

Address: http://192.168.10.1

Mediatrix 2102

HTTP server password

Change HTTP server password

Username: dmin

New password:

Confirm password:

2. Enter the new password.

The password is case sensitive. It can be a string of 0 to 16 characters. All characters are allowed. However, some special characters, such as accented characters (é, à, etc.), may not work.

3. Retype the password in the *Confirm Password* field.

4. Click *Apply*.

The password resets back to the default value when:

- Resetting the password by using the *httpServerResetToDefaultPwd* variable (see "Default User Name and Password" on page 33 for more details).
- Performing a factory reset (see "Factory Reset" on page 22 for more details).

Default User Name and Password

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

▶ **To modify the default user name and password:**

1. In the *httpServerMIB*, set the default user name for the web interface access authentication in the *httpServerUsername* variable.

2. Set the default password for the web interface access authentication in the *httpServerDefaultPassword* variable.

Both changes are immediate and take effect on all new web accesses.

▶ **To reset the web authentication password to the default value:**

1. In the *httpServerMIB*, set the *httpServerResetToDefaultPwd* variable to **reset**.

   The web password is reset to the default value specified by the *httpServerDefaultPassword* variable. The change is immediate and takes effect on all new web accesses.

System Log Page

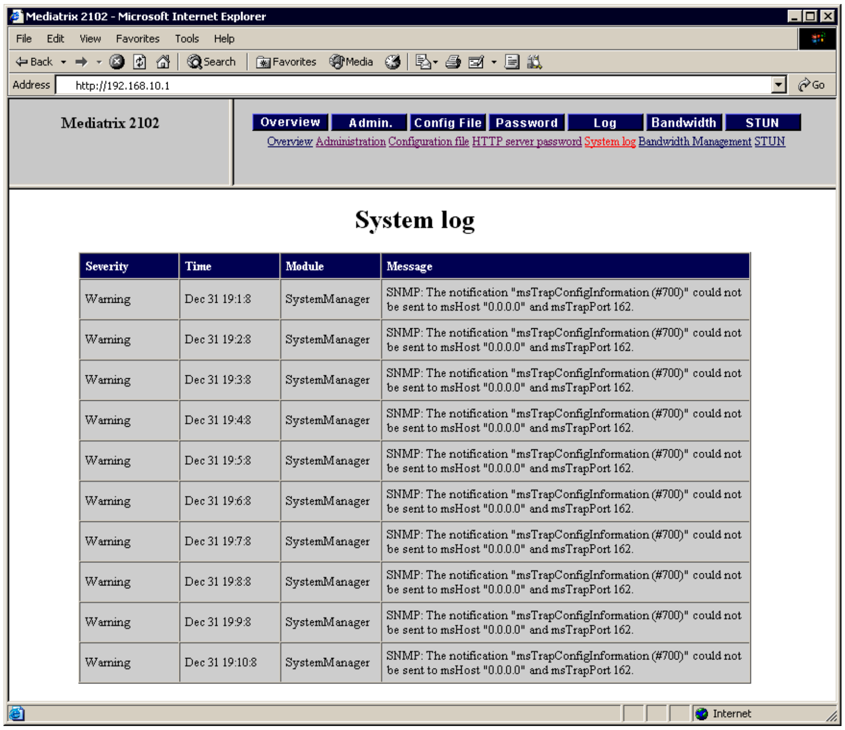
The *System log* page allows you to peruse the last *n* system log (syslog) messages sent by the Mediatrix 2102 since it last restarted.

▶ **To access the System log page:**

1. In the web interface, click the *System log* link or the *Log* button of the Menu frame.

   The following opens:

Figure 15: System log Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.10.1 Go
Mediatrix 2102
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
Internet

System log

Severity	Time	Module	Message
Warning	Dec 31 19:1:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:2:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:3:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:4:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:5:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:6:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:7:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:8:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:9:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.
Warning	Dec 31 19:10:8	SystemManager	SNMP: The notification "msTrapConfigInformation (#700)" could not be sent to msHost "0.0.0.0" and msTrapPort 162.

Please refer to “Local Syslog” on page 236 for information on how to set the system log parameters.

Bandwidth Management Page

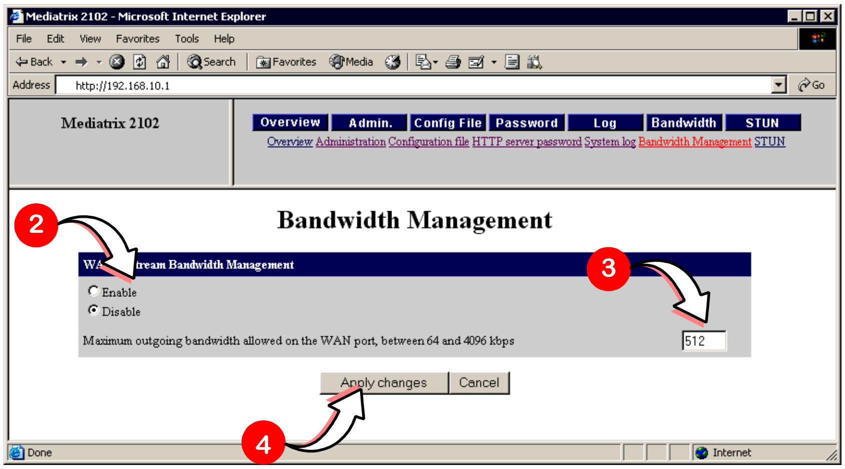
The *Bandwidth Management* web page allows you to limit the upload bandwidth on the WAN interface See "WAN Upstream Bandwidth Control" on page 97 for more information.

Note: Applies to the Mediatrix 2102 312/322 only.

▶ **To configure the bandwidth management:**

1. In the web interface, click the *Bandwidth Management* link or the *Bandwidth* button.
   This links to the *Bandwidth Management* web page.

Figure 16: Bandwidth Management Web Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.10.1 Go
Mediatrix 2102
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
2
3
4
Apply changes Cancel
Done
Internet

Bandwidth Management

WA tream Bandwidth Management

○ Enable
● Disable

Maximum outgoing bandwidth allowed on the WAN port, between 64 and 4096 kbps 512

2. Enable the Bandwidth Management feature by selecting the *Enable* option.
3. Set the maximum outgoing bandwidth allowed on the WAN port in the corresponding field.
   Available values are between 64 kbps and 4096 kbps.
4. Click *Apply changes*.
   The Mediatrix 2102 automatically restarts to apply all the new settings.

STUN Page

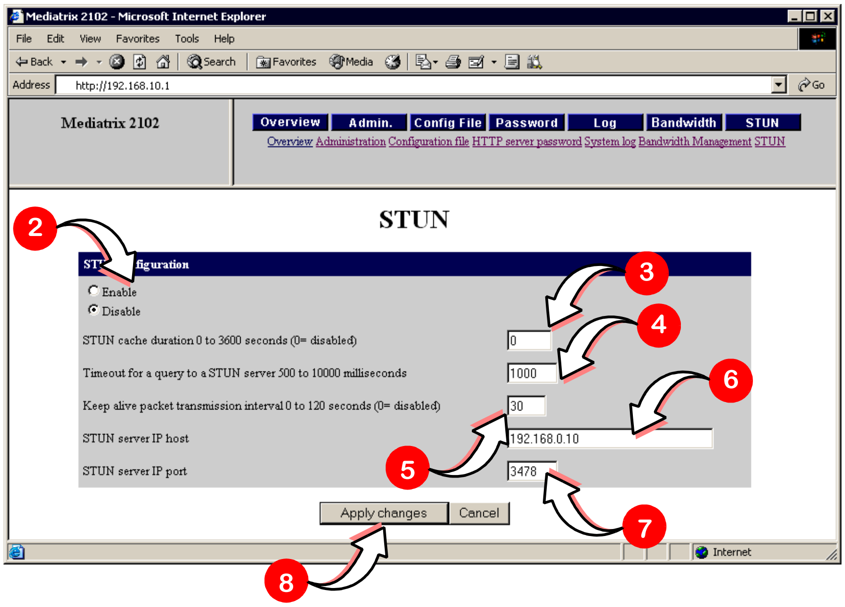
The *STUN* web page allows you to configure the STUN client of the Mediatrix 2102. See "Chapter 16 - STUN Configuration" on page 181 for more information.

▶ **To configure the STUN client of the Mediatrix 2102:**

1. In the web interface, click the *STUN* link or the *STUN* button.

   This links to the *STUN* web page.

Figure 17: STUN Web Page


Mediatrix 2102 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.10.1
Go
Mediatrix 2102
Overview Admin. Config File Password Log Bandwidth STUN
Overview Administration Configuration file HTTP server password System log Bandwidth Management STUN
Internet
2
3
4
5
6
7
8

STUN

STUN Configuration

○ Enable
● Disable

STUN cache duration 0 to 3600 seconds (0= disabled): 0

Timeout for a query to a STUN server 500 to 10000 milliseconds: 1000

Keep alive packet transmission interval 0 to 120 seconds (0= disabled): 30

STUN server IP host: 192.168.0.10

STUN server IP port: 3478

Apply changes | Cancel

2. Enable the STUN client by selecting the *Enable* option.

3. Set the amount of time, in seconds, the Mediatrix 2102 should keep a STUN query result in its internal cache in the *STUN cache duration* field.

   Keeping a query in a cache helps to reduce the amount of unnecessary STUN queries when an RTP or T.38 socket is re-used within a short period of time. Available values range from 0 s to 3600 s.

   When set to **0**, the cache is disabled and the unit performs a STUN query each time a socket needs to be used.

4. Set the maximum amount of time, in milliseconds, the Mediatrix 2102 should wait for an answer to a STUN query sent to a STUN server in the *Timeout for a query to a STUN server* field.

   Available values range from 500 ms to 10000 ms.

   Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure.

5. Define the interval, in seconds, at which the Mediatrix 2102 sends blank keepalive messages to keep a firewall hole opened in the *Keepalive packet transmission interval* field.

   Keepalive messages are used by both the signalling protocol socket and the RTP socket to keep those connections opened through a firewall. Available values range from 0 s to 120 s.

   When set to **0**, no keepalive packet is sent.

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

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

   The default value is **3478**.
8. Click *Apply changes*.

   The Mediatrix 2102 automatically restarts to apply all the new settings.

Web Interface Access Limitation

Access to the web interface can be limited to only one of the Mediatrix 2102's interface or all its interfaces. This can be modified only by using the proper MIB variable.

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

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

   You have the following choices:

Table 19: Web Access Limitation Parameters

Access	Description
lanOnly	You can access the web interface from the LAN side, which is usually associated with the *Computer* connector.
wanOnly	You can access the web interface from the WAN side, which is usually associated with the *Network* connector.
all	You can access the web interface from both the LAN and WAN sides.

The change is immediate and takes effect on all new web accesses.

☞ **Note:** This variable is modified to **all** if Transparent Address Sharing is disabled. See "Configuring TAS" on page 93 for more details.

CHAPTER 3

MIB Structure and SNMP

This chapter describes how the Mediatrix 2102 uses the SNMP protocol for its configuration.

SNMP Overview

The Mediatrix 2102 uses the Simple Network Management Protocol (SNMP) for initial software configuration provisioning and subsequent software configuration.

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

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

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

Definitions

Structure of Management Information (SMI)

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

Management Information Base (MIB)

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

Object Identifier (OID)

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

SNMP Versions

The Mediatrix 2102 supports three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. SNMP defines a few types of messages that are exchanged between the manager and agent.

SNMPv1 Messages

The following messages are specific to SNMPv1.

Table 20: SNMPv1 Message Types

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

SNMPv2c Messages

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

Table 21: SNMPv2 Message Type

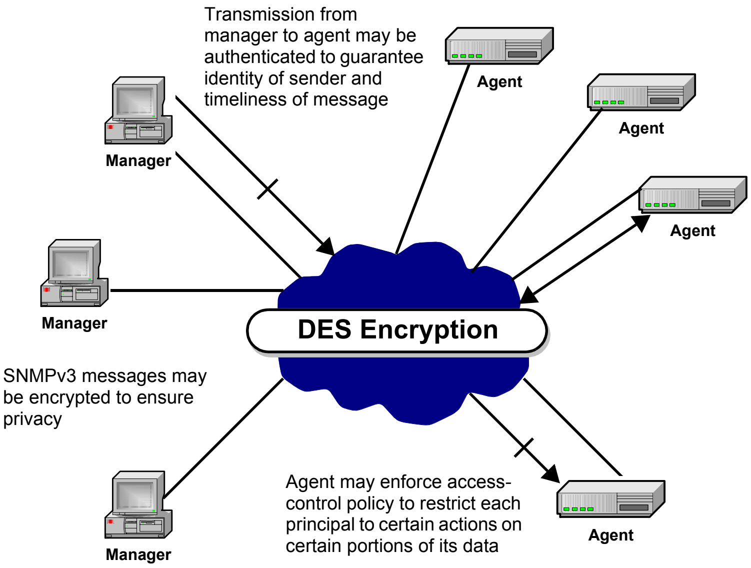
Operator	Description
get-bulk	Uses BULK Requests to query for a tree of information about a network entity. A variable put in command line specifies which portion of the object identifier space will be searched using BULK Requests. All variables in the subtree below the given variable are queried as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

This message is sent from the manager to the agent.

SNMPv3 Messages

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

Figure 18: SNMPv3 Services


Transmission from manager to agent may be authenticated to guarantee identity of sender and timeliness of message
Agent
Agent
Manager
Agent
Manager
DES Encryption
SNMPv3 messages may be encrypted to ensure privacy
Agent may enforce access-control policy to restrict each principal to certain actions on certain portions of its data
Agent
Manager

SNMP Behaviour

When using SNMP, the following rules apply:

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

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

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

Non-Secure Management Mode

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

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

Secure Management Mode

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

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

Note: If you forget or lose a password, perform a Factory Reset to reset the unit to the non-secure management mode. See “Factory Reset” on page 22 for more details.

Notes

- When using SNMPv3 with encryption (DES), you may experience delays when accessing MIB variables. This is normal because encrypting an IP packet takes in general longer than sending it over IP. If you experience any timeout, add some seconds to the timeout period of your MIB browser, and then try to reach the unit again.
- Suppose that the Mediatrix 2102 accepts requests with authentication only. If you perform requests by using encryption and authentication, assuming that the authentication password is valid, the SNMP agent still responds as if the requests were only authenticated.
- If you clone an SNMPv3 user, and then remove authentication or privacy for it, ensure that a row in *vacmGroupName* matches its new constraints. If not, the unit is not accessible by using the new clone parameters.

SNMPv3 Special Behaviour

Mediatrix units coming out of factory are set so that you can use all MIB variables by using SNMPv1, SNMPv2c, or SNMPv3. However, you can decide to accept only SNMPv3 access by using passwords known by administrators only for enhanced security. In this case, you should manually disable SNMPv1 / SNMPv2 so that SNMPv3 works properly. The Mediatrix 2102 thus refuses any SNMPv1 or SNMPv2 request it receives.

You can disable / enable SNMPv1 / SNMPv2 by using the MIB Browser included in the Mediatrix Unit Manager Network (or any other MIB Browser) to modify the permissions related to SNMPv1 / SNMPv2 (security model). These permissions are located in the *VacmAccessTable* of the SNMP-VIEW-BASED-ACM-MIB (RFC 2575).

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

- usmUserTable
- vacmSecurityToGroupTable
- vacmAccessTable
- vacmViewTreeFamilyTable

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

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

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

MIB Structure

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

Table 22: Structure of Management Information

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

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

Textual Conventions

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

Table 23: Textual Conventions

Type	Definition
MxIpHostName	Represents an IP address or a domain name.
MxIpAddress	Represents an IP address.
MxIpPort	The TCP or UDP port number range. Values can be between 1 and 65535.
MxIpSubnetMask	Represents an Internet subnet mask.
MxIpSelect ConfigSource	Indicates the source to use during the next restart sequence for the provisioning of the localHost MIB objects. • static: uses static values provided by the user (such as DNS addresses, router, etc.). • dhcp: uses the DHCP server to retrieve the configuration of the localHost MIB objects.
MxIpConfigSource	Indicates the source used during the last restart sequence for the provisioning of the localHost MIB objects. • static: the user provided static values such as DNS addresses, router, etc. • dhcp: the DHCP server was used to retrieve the configuration of the localHost MIB objects. • Default: hardcoded values for recovery mode were used.
MxIpDhcpSite SpecificCode	Represents a DHCP site specific code. Values can be between 128 and 254 or 0. You can enter this code in your DHCP server to define IP addresses. Refer to “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.
MxFloatingPoint	Represents a floating point number.
MxAdvancedIpPort	The TCP or UDP port number range. Values can be between 0 and 65535. The port number value 0 is used for special functionality defined in the variable definition.
MxEnableState	Represents an enabled/disabled state (boolean value).
MxActivationState	Represents an active/inactive state (boolean value).
MxSignalingAddress	Represents a valid signalling address.
MxDigitMap	A digit map is a sequence used to determine when the dialing of DTMFs is completed. See “Chapter 18 - Digit Maps” on page 187 fore more details.

Objects, Conformance, and Events

Each MIB may have three types of data.

Table 24: MIB Data Types

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

IP Addresses

The MIB structure contains many IP addresses that can be set or viewed. See “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.

Persistence

A variable may either be persistent or volatile.

Table 25: Storage Clauses

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

Changing a Parameter Value

The Mediatrix 2102 software parameters are fully programmable by using the SNMP protocol. There are two ways to set up and configure a unit:

- By using a SNMP browser to contact the MIBs of the Mediatrix 2102. It is assumed that you have basic knowledge of TCP/IP network administration.

  You can use the MIB browser built in the Mediatrix’ Unit Manager Network. See “Unit Manager Network – Element Management System” on page xxv for more details.

  You can also use any third-party SNMP browser or network management application running the SNMP protocol to monitor and configure the Mediatrix 2102. However, the information may not be presented in the same manner depending on the SNMP browser used.

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

  The Management Server could be Mediatrix’s Unit Manager Network. See “Unit Manager Network – Element Management System” on page xxv for more details.

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

Locate the proper parameter to modify and change (SET) its value. Most of the parameters require to restart the Mediatrix 2102 unit. A restart may be software-initiated or manually initiated by unplugging the unit. It deletes all statistics stored and overwrites all volatile parameter values in the configuration file. A restart also reinitiates the entire unit’s initial provisioning sequence.

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

Tables

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

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

Generic Variables

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

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

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

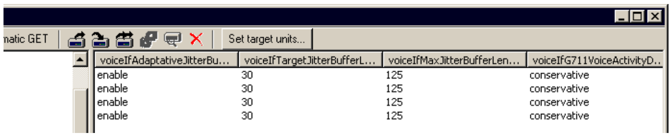
Table 26 gives an example of the *ifTable*.

Table 26: ifTable Example

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

Figure 19 shows a table built in the Unit Manager Network from the *voiceifTable* parameters.

Figure 19: voiceIftable Example



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

You can perform GET and SET operations on these parameters.

Variables for Administrative Commands

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

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

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

groupAdmin Table

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

Table 27: groupAdmin Parameters

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

ifAdmin Table

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

Table 28: ifAdmin Parameters

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

SNMP Access Limitation

The SNMP access to the Mediatrix 2102 can be limited to only one of its interface or all interfaces.

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

1. In the *snmpAgentMIB*, select the interface where the Mediatrix 2102 can be accessed via SNMP in the *snmpAgentAccess* variable.

You have the following choices:

Table 29: SNMP Access Limitation Parameters

Access	Description
lanOnly	SNMP connections are only permitted on the LAN side, which is usually associated with the *Computer* connector. The LAN IP address is provisioned by the *lanStaticAddress* variable.
wanOnly	SNMP connections are only permitted on the WAN side, which is usually associated with the *Network* connector. However, if the WAN interface is down and the unit reverts to its LAN configuration, the SNMP agent can access the Mediatrix 2102 on its LAN interface.
all	SNMP connections are permitted on both the LAN and WAN sides.

Current MIB Version

You can find out the version of the MIB currently in the Mediatrix 2102.

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

This variable displays the current version of the MIB.

Sending Configuration Data to the Mediatrix 2102

The configuration data can be provisioned into the Mediatrix 2102 in two ways:

- as a configuration file sent from the Management Server to the Mediatrix 2102 via TFTP
- as a MIB sent from the Management Server to the Mediatrix 2102 via SNMP

Configuration File

The configuration file is the fastest way to deliver the necessary information. This may be important when initializing a large number of units at the same time. The configuration file is mostly used for the initial provisioning sequence (see “Initial Provisioning Sequence” on page 13 for more details).

For more information on how to use a configuration file for updating the Mediatrix 2102, see “Chapter 9 - Configuration File Download” on page 107.

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 2102 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.

CHAPTER

4

IP Address and Network Configuration

The Mediatrix 2102 must be provisioned with various IP addresses and network parameters to be fully functional. This occurs each time the Mediatrix 2102 is started or when an IP address value is changed in the MIB. The Mediatrix 2102 can use static network parameters as well as parameters provided by a DHCP server, an access concentrator, or even a DNS.

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

This chapter also refers to the MIB structure of the configuration variables. Refer to "Chapter 3 - MIB Structure and SNMP" on page 39 for more details.

IP Addresses

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

Table 30: IP Addresses Folders

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

IP Addresses Formats in the DHCP Server

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

Table 31: IP Addresses Formats in DHCP Server

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

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

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

Provisioning Source

The Mediatrix 2102 IP address information may come from a variety of sources.

Table 32: IP Address Provisioning Sources

Source	Description
Static	You manually enter the value and it remains the same every time the Mediatrix 2102 restarts. If you do not specify a value, a default static value applies.
DHCP	The value is obtained at start-time by querying a DHCP server and using standard DHCP fields or options. See RFC 2131 section 2 and RFC 2132.
DHCP – Site specific options	The value is obtained at start-time by querying a DHCP server and using a non-standard option specific to the site where the Mediatrix 2102 is used. See “Site Specific Options” on page 65 for more details.
DHCP – Vendor specific options	The value is obtained at start-time by querying a DHCP server and using a standard option that is reserved for storing vendor specific information. See “Vendor Specific Options” on page 64 for more details.
DNS	The value is obtained at start-time by querying a DNS server.
None	The value is not provisioned. The application provides an acceptable default.
Automatic	The configuration source is selected by the Mediatrix 2102, following a preference order and the availability of some services.
PPP-IPCP[a]	The value is obtained during the PPP network-layer protocol phase from the IPCP configuration options.

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

Services

This section describes the services the Mediatrix 2102 uses and their settings. Most of these services require that you define their IP address and, if required, port number. See "DHCP Server Configuration" on page 63 for more details.

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

Configuration Source

The configuration your Mediatrix 2102 uses can either be:

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

DHCP Configuration

Using DHCP-assigned IP addresses ensures that the Mediatrix 2102 receives the addresses that are stored in the DHCP server. This assumes that you have previously set the DHCP server with the proper values. See "DHCP Server Configuration" on page 63 for more details.

The Mediatrix 2102 can receive numerous information from the DHCP server, including the vendor or site specific information. Note that the Mediatrix 2102 does not make a DHCP request in the following cases:

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

When the Mediatrix 2102 uses a DHCP server for network parameters, it must always have at least the following three valid parameters:

- IP Address
- Subnet Mask
- Default Gateway

If the parameters are not valid (i.e., the default gateway is not in the same subnet as the IP address), the Mediatrix 2102 will not work properly.

Verifying the DHCP-Assigned IP Addresses

You can query the MIB structure to see the IP addresses that have been assigned to the Mediatrix 2102. 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:

- Connect a telephone into one of the FXS ports of the Mediatrix unit, dial "*#*0" and listen for the IP address that is given.
- Use the autodetect feature of the Mediatrix Unit Manager Network product. See "Unit Manager Network – Element Management System" on page xxv for more details.

Static Configuration

Using static IP addresses allows you to bypass the DHCP server or still be able to use the Mediatrix 2102 if you are not running a DHCP server.

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

The reason for this delay is that the Mediatrix 2102 cannot function as configured if part of its configuration (the DHCP information) is unavailable. To avoid this problem, you can set all configuration sources the Mediatrix 2102 supports to “static”.

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

▶ **To set all configuration sources to static:**

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

Local Host

The *ipAddressConfigLocalHost* group allows you to set the IP information the Mediatrix 2102 needs to work properly. This group is vital to the proper operation of the Mediatrix 2102. If a variable of this group is not properly set, the Mediatrix 2102 may not be able to restart and be contacted after it has restarted.

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

▶ **To select the local host configuration source:**

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

Table 33: Local Host Variables

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

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

b. If you are not using a default router, set the variable to **0.0.0.0**. Setting the default router IP address to “0.0.0.0” may lead to software download problems. See the troubleshooting section “Software Upgrade Issues” on page 251 for more details.

> **Note:** If the *localHostDnsOverrideEnable* or *telephonyDnsOverrideEnable* variable is enabled, the primary and secondary DNS addresses are set with static values. See “Static DNS” on page 55 for more details.

In the table above, the only variables that allow an empty string are: localHostPrimaryDns, LocalHostSecondaryDns and LocalHostDefaultRouter.

3. Restart the Mediatrix 2102 so that the changes may take effect.

Static DNS

By default, the Mediatrix 2102 and the networked PC (linked in a LAN with the unit) receives DNS IP addresses according to the configuration source you have defined in the *localHostSelectConfigSource* variable. In general, these addresses are provided by an ISP (Internet Service Provider) via PPPoE or DHCP.

However, you may require that the Mediatrix 2102 and the networked PC use different DNS addresses. If that is the case, you can set static values for the primary and secondary DNS IP addresses, even when the Mediatrix 2102 is set by DHCP. These static values can thus override PPPoE and DHCP provisioning. This feature could be useful in the case where your ISP (Internet Service Provider) and your ITSP (Internet Telephony Service Provider) use different DNS IP addresses or when a Mediatrix 2102 and a networked PC need to use a different DNS.

The Mediatrix 2102 may receive DNS addresses from three sources:

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

Table 34 explains how DNS addresses are attributed to the Mediatrix 2102 and the networked PC.

Table 34: DNS Addresses Possibilities

localHostDns OverrideEnable	telephonyDns OverrideEnable	DNS address of Mediatrix 2102	DNS address of the Networked PC
disabled	disabled	DNS from ISP	DNS from ISP
disabled	enabled	static telephony DNS	DNS from ISP
enabled	disabled	static local host DNS	static local host DNS
enabled	enabled	static telephony DNS	static local host DNS

▶ To use static DNS IP addresses:

1. In the *ipAddressConfig* folder, set the *localHostDnsOverrideEnable* variable (under the *ipAdressConfigLocalHost* group) to **enable**.

   The primary DNS and secondary DNS addresses are set with the static values defined in the *localHostStaticPrimaryDns* and *localHostStaticSecondaryDns* variables.

   If you set the variable to **disable**, the primary DNS and secondary DNS addresses provisioning depends on the setting of the *telephonyDnsOverrideEnable* variable.

2. In the *ipAddressConfig* folder, set the *telephonyDnsOverrideEnable* variable (under the *ipAddressConfigTelephonyDns* group) to **enable**.

   The primary DNS and secondary DNS addresses are set with the static values you define in the next step.

3. Set the *telephonyDnsStaticPrimaryDns* and *telephonyDnsStaticSecondaryDns* variables with the proper static DNS IP addresses of your ITSP.

   If you set the *telephonyDnsOverrideEnable* variable to **disable**, the primary DNS and secondary DNS addresses provisioning depends on the setting of the *localHostDnsOverrideEnable* variable.

4. Restart the Mediatrix 2102 so that the changes may take effect.

WAN Address Configuration Source

The Wide Area Network (WAN) address is the public IP address attributed to the Mediatrix 2102. This address is used for incoming signalling, media and management traffic.

▶ **To set the WAN IP address configuration source:**

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

   This variable indicates the source to be used for the provisioning of the WAN address. It offers the following choices:

Table 35: WAN IP Address Source Settings

Option	Description
localAddress	The Mediatrix 2102 is not part of a WAN. The public address is the same as the *localHostAddress*.
static	The Mediatrix 2102 has a static WAN address. The address is configured in the *localHostStaticWanAddress* variable. Note that this setting allows a limited NAT traversal scheme.
pppoe	The Mediatrix 2102 uses the PPP interface’s address as the WAN address. The PPPoE service must be enabled for the WAN address to be configured.
automatic	If the PPPoE service is enabled, the Mediatrix 2102 uses *pppoe* as the configuration source. Otherwise it uses *localAddress*.

Table 36: WAN IP Address Source

Variable	Default Static Value	DHCP Source
LocalHostWanAddress	“192.168.0.1”	Option IP-Address

2. Restart the Mediatrix 2102 so that the changes may take effect.

LAN Interface Configuration

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

Table 37: LAN Interface Source

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

SNMP Configuration

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

Table 38: SNMP Source

Variable	Default Static Value	DHCP Source
LocalHostSnmpPort	161	N/A

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

The Mediatrix 2102 uses the SNMP protocol for software configuration. Set the following SNMP-related variable to properly use the protocol.

Table 39: SNMP Configuration Variables

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

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

- localHostSnmpPort
- msTrapPort

Image

The *ipAddressConfigImage* group provides the configuration necessary to download applications into the Mediatrix 2102. This includes emergency downloads in case of repetitive failure to start the main application.

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

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

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

Table 40: Image Information Source

Variable	Default Static Value	DHCP Source
imagePrimaryHost	"192.168.0.10"	Use option specified in variable *imageDhcpPrimarySiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 117, bytes 0-3.
imagePrimaryPort	69[a]	Use option specified in variable *imageDhcpPrimarySiteSpecificCode*, bytes 4-5. If not specified (0), use option 43, sub-option 117, bytes 4-5. If bytes 4-5 are not present, use the default static value.
imageSecondaryHost	"192.168.0.10"	Use option specified in variable *imageDhcpSecondarySiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 118, bytes 0-3.
imageSecondaryPort	69[a]	Use option specified in variable *imageDhcpSecondarySiteSpecificCode*, bytes 4-5. If not specified (0), use option 43, sub-option 118, bytes 4-5. If bytes 4-5 are not present, use the default static value.

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

Management Server

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

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

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

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

Table 41: Management Server Source

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

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

Configuration File Fetching

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

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

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

Table 42: Configuration File Fetching Source

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

3. Restart the Mediatrix 2102 so that the changes may take effect.

Syslog

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

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

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

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

Table 43: Syslog Source

Variable	Default Static Value	DHCP Source
syslogHost	“192.168.0.10”	Use option specified in variable *syslogDhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 110, bytes 0-3.

Table 43: Syslog Source (Continued)

Variable	Default Static Value	DHCP Source
syslogPort	514[a]	Not provided by the DHCP, use the default static value.

[a] The port number is as per RFC 1340.

SIP Servers

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

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

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 port is 0, then the host and port for this server are obtained through a DNS SRV request. See “Chapter 6 - DNS SRV Configuration” on page 79 for more details.

▶ **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 44: SIP Servers Source

Variable	Default Static Value	DHCP Source
sipHomeDomain ProxyHost	“192.168.0.10”	Use option specified in variable *sipHomeDomainProxyDhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 204, bytes 0-3
sipHomeDomain ProxyPort	0	Use option specified in variable *sipHomeDomainProxyDhcpSiteSpecificCode*, 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.
sipOutboundProxy Host	“0.0.0.0”	Use option specified in variable *sipOutboundProxyDhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 205, bytes 0-3.
sipOutboundProxy Port	0	Use option specified in variable *sipOutboundProxyDhcpSiteSpecificCode*, 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.

Table 44: SIP Servers Source (Continued)

Variable	Default Static Value	DHCP Source
sipRegistrarHost	“192.168.0.10”	Use option specified in variable *sipRegistrarDhcpSiteSpecificCode*, bytes 0-3. If not specified (0), use option 43, sub-option 203, bytes 0-3.
sipRegistrarPort	0	Use option specified in variable *sipRegistrarDhcpSiteSpecificCode*, 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 “Chapter 17 - SNTP Settings” on page 183 for more details), the DHCP server already has options that can be set to provide time server addresses, and the order in which clients use them to attempt to discover servers.

The Mediatrix 2102 uses *Option 42* to specify the IP address corresponding to the server that provides NTP/SNTP (RFC 1769).

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

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

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

Table 45: 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.

DHCP Server Configuration

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

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

DHCP servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The Mediatrix 2102 unique identifier is its media access control (MAC) address.

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

You can locate the MAC address as follows:

- on the label located on the bottom side of the unit.
- in the *sysMgmtMIB* under the *sysMacAddress* variable.
- You can dial the following digits on a telephone connected to the Mediatrix 2102:

  `*#*1`

  The Mediatrix 2102 answers back with its MAC address. See “Special Vocal Features” on page 15 for more details.

Mediatrix recommends to reserve an IP address with an infinite lease for each Mediatrix 2102 on the network.

Connection to the DHCP Behaviour

When the Mediatrix 2102 restarts, it requests a DHCP offer to get its IP addresses and network information. The Mediatrix 2102 waits four seconds before sending another request. The delay between each request is increased exponentially after each request up to a maximum delay of 64 seconds, and then restarts at a 4 seconds delay.

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

The Mediatrix 2102 stops broadcasting as soon as it receives at least one reply. If the offer is valid, the Mediatrix 2102 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 2102 makes its DHCP request that will be released immediately.

Network Configuration

Table 46 lists some of the network options to configure in the DHCP server:

Table 46: Network Configuration

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

Vendor and Site Specific DHCP Options

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

This section briefly describes vendor and site specific DHCP options. Most of the MIB variables described in "Services" on page 53 require that you define their IP address and, if required, port number. When defining these variables, you can do so in two ways: via vendor specific options or site specific options.

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

If you want to use site specific codes instead, change the value of the *xxSiteSpecificCode* MIB variables from the default value (0) to the value you select in the DHCP server. See "Settings Example" on page 67 for an example of vendor specific and site specific settings.

Vendor Specific Options

Standards Supported	RFC 2132 – DHCP Options and BOOTP Vendor Extensions, section 8.4 ("Vendor-specific options")

The vendor specific DHCP option is a standard DHCP option used to store information specific to the vendor of the DHCP client. The vendor specific option code is 43. Because there are different information elements that can be stored in this option, each element has been allocated a "sub-option" number. See Table 47 on page 66 for the complete list.

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

The data is organized as a series of sub-options, each of them laid-out like a regular option (code, len, data). The codes can be anything between 1 and 254, and the vendor, Mediatrix, chooses these codes. See Table 47 on page 66 for actual codes.

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

Figure 20: General Layout of a Vendor Specific Information Option

43	Len	Data	Data	Data	Data	…

Figure 21: Layout for Encapsulated Vendor Specific Options

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

Figure 22 on page 65 is an example of a vendor specific option containing an *msHost* IP address (192.168.1.2).

Figure 22: Example of Encapsulated Vendor Specific Option

43	6	200	4	192	168	1	2

Mediatrix units store one type of information 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 66.

Vendor Class ID

When using the vendor specific option, first define a Vendor Class ID for the Mediatrix 2102 (not supported in Windows NT servers). A Vendor Class ID can be used by DHCP clients to identify their vendor type and configuration. When using this option, vendors can define their own specific identifier values to convey a particular hardware or operating system configuration or other identifying information.

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

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

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

Note: The class to add is *Mediatrix 2102*.

Creating Vendor Specific Information

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

If the option is not in the DHCP server, the Mediatrix 2102 uses an invalid value (0.0.0.0:0).

Please refer to your DHCP server's documentation to learn how to create vendor specific information. See "Entering IP Addresses" on page 66 for more details on the syntax to use.

Site Specific Options

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

Site specific options are non-standard DHCP options specific to the network where the Mediatrix 2102 is used. You are responsible to allocate an option number (between 128 and 254) for each information element to be stored.

Mediatrix units store one type of information 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 66.

Figure 23 is an example of site specific option #146, containing address 192.168.0.1.

Figure 23: Site Specific Option Example

146	4	192	168	0	1

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

Please refer to your DHCP server's documentation to learn how to create site specific information. See "Entering IP Addresses" on page 66 for more details on the syntax to use.

Option Codes

This table summarises all vendor specific sub-option codes.

Table 47: Sub-Option Codes

Code		Description
Decimal	**Hexadec.**	
117	0x75	Image Primary Server host address and port. The default port number is **69** if you are using TFTP as protocol. The default port number is **80** if you are using HTTP as protocol.
118	0x76	Image Primary Server host address and port. The default port number is **69** if you are using TFTP as protocol. The default port number is **80** if you are using HTTP as protocol.
200	0xC8	Management Server SNMP Trap host address and port.
201	0xD2	Configuration file fetching host. The default port number is **69** if you are using TFTP as protocol. The default port number is **80** if you are using HTTP as protocol.
203	0xCB	SIP Registrar host address and port.
204	0xCC	SIP Home Domain Proxy address and port.
205	0xCD	SIP Outbound Proxy address and port.

Entering IP Addresses

In the DHCP server, IP addresses can be entered in decimal, hexadecimal or octal format. See “IP Addresses” on page 51 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 48: Address String Formats

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

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

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

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

The site specific options can have only one information per option:

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

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

Example

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

Figure 24: Example – Short Address String

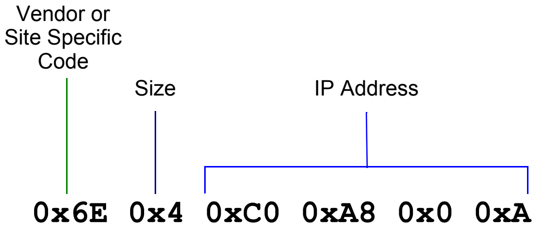
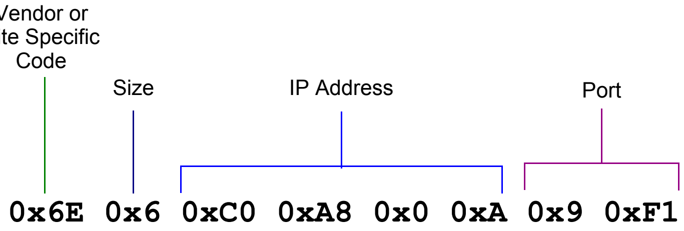


Figure 25: Example – Long Address String


Vendor or Site Specific Code
Size
IP Address
Port
0x6E 0x6 0xC0 0xA8 0x0 0xA 0x9 0xF1

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 49: Hexadecimal Sequence - Option 43

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

Table 49: Hexadecimal Sequence - Option 43 (Continued)

Hexadecimal Part	Corresponding Information
0xA0x30x20xC9	IP address 10.3.2.201

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

Table 50: 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 51: Replacement Values for Error Recovery

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

DHCP Server Failures

If the Mediatrix 2102 cannot contact the DHCP server, it performs one of the following actions:

1. Retries contacting the DHCP server until it answers. The Mediatrix 2102 does not restart.
2. Uses the replacement value from Table 51 on page 68 for all variables that depend on the DHCP.

This assumes that the Mediatrix 2102 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 2102 uses the replacement value from Table 51 on page 68 for each variable that depends on missing vendor/site specific options.

DNS Failures

If the DNS cannot be contacted, the Mediatrix 2102 performs the following steps:

1. The Mediatrix 2102 sends a first request to the primary DNS server.
2. If the DNS server cannot be contacted within two seconds, the Mediatrix 2102 sends a request to the secondary DNS server.
3. If the secondary DNS server cannot be contacted, the Mediatrix 2102 uses the replacement value from Table 51 on page 68 for all variables that depend on the DNS.

Ethernet Connection Speed

You can set the speed of the Ethernet connection of the Mediatrix 2102.

▶ **To set the Ethernet connection speed:**

1. In the *sysConfigMIB*, set the Ethernet connection speed of the:

- *Network* connector in the *sysConfigNetworkEthernetSpeed* variable
- *Computer* connector in the *sysConfigComputerEthernetSpeed* variable.

The following values are available:

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

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

If unknown, set the variable to **Auto detect** so that the Mediatrix 2102 can automatically detect the network speed.

Caution: Whenever you force a connection speed / duplex mode, be sure that the other device and all other intermediary nodes used in the communication between the two devices have the same configuration. See “Speed and Duplex Detection Issues” on page 69 for more details.

Speed and Duplex Detection Issues

There are two protocols for detecting the Ethernet link speed:

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

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

The Mediatrix 2102 has the possibility to force the desired Ethernet link speed and duplex mode by disabling the auto-negotiation and selecting the proper setting (*sysConfigNetworkEthernetSpeed* or *sysConfigComputerEthernetSpeed* variable). When forcing a link speed at one end, be sure that the other end (a hub, switch, etc.) has the same configuration. To avoid any problems, the link speed and duplex mode of the other endpoint must be exactly the same.

CHAPTER
5

SIP Servers

The Mediatrix 2102 uses three types of servers:

- Registrar server
- Proxy server
- Outbound Proxy server

This chapter describes how to configure the Mediatrix 2102 to properly use these servers.

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.

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

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the Registrar server. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

Note: When defining whether the Mediatrix 2102 must get its SIP server configuration through a DHCP server or not, this is set for all the SIP servers. You cannot define a different configuration for each type of server.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See "Chapter 4 - IP Address and Network Configuration" on page 51 for more details.

To use DHCP-assigned information:

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

   This variable defines whether the Mediatrix 2102 must get its 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

3. Set how you want to define the registrar server information in the DHCP server.

Table 52: Registrar Server DHCP Information

To use a...	Set...
vendor specific code	The *sipRegistrarDhcpSiteSpecificCode* variable (under the *ipAddressConfigSipServer* group) to **0**. Set the registrar server IP address in the DHCP server inside the vendor specific sub-option 203 (hexadecimal 0xCB).
site specific code	The *sipRegistrarDhcpSiteSpecificCode* variable to any value between 128 and 254. Set the registrar server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *sipRegistrarDhcpSiteSpecificCode* variable in the unit's configuration).

Static Configuration

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

▶ **To use static information:**

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

   This variable defines whether the Mediatrix 2102 must get its registrar server configuration through a DHCP server or not.

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

3. Set the following variables:

Table 53: Registrar Server Static Information

Variable	Description
sipRegistrarStaticHost	Registrar server static IP address or domain name. **Default Value**: 192.168.0.10
sipRegistrarStaticPort	Registrar server static IP port number. **Note**: If this variable corresponds to a domain name that is bound to a SRV record, the port must be set to **0** for the unit to perform DNS requests of type SRV (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather use only requests of type A because it does not need to be specified which port to use. **Default Value**: 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.

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

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the proxy server. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

Note: When defining whether the Mediatrix 2102 must get its SIP server configuration through a DHCP server or not, this is set for all the SIP servers. You cannot define a different configuration for each type of server.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.

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

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

This variable defines whether the Mediatrix 2102 must get its 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 proxy server information in the DHCP server.

Table 54: Proxy Server DHCP Information

To use a...	Set...
vendor specific code	The *sipHomeDomainProxyDhcpSiteSpecific Code* variable (under the *ipAddressConfigSip Server* group) to **0**. Set the proxy server IP address in the DHCP server inside the vendor specific sub-option 204 (hexadecimal 0xCC).
site specific code	The *sipHomeDomainProxyDhcpSiteSpecificCode* variable (under the *ipAddressConfigSip Server* group) to any value between 128 and 254. Set the proxy server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *sipHomeDomainProxyDhcpSiteSpecificCode* variable in the unit's configuration).

Static Configuration

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

▶ **To use static information:**

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

   This variable defines whether the Mediatrix 2102 must get its proxy server configuration through a DHCP server or not.

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

3. Set the following variables:

Table 55: Proxy Server Static Information

Variable	Description
sipHomeDomainProxyStatic Host	Proxy server static IP address or domain name. **Default Value**: 192.168.0.10
sipHomeDomainProxyStatic Port	Proxy server static IP port number. **Note**: If this variable corresponds to a domain name that is bound to a SRV record, the port must be set to **0** for the unit to perform DNS requests of type SRV (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather use only requests of type A because it does not need to be specified which port to use. **Default Value**: 0

Outbound Proxy Server

An 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.

When the outbound proxy is enabled, the proxy is still used to create the *To* and the *From* headers, but the packets are physically sent to the outbound proxy.

The 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.

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the outbound proxy. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

> ☞ **Note:** When defining whether the Mediatrix 2102 must get its SIP server configuration through a DHCP server or not, this is set for all the SIP servers. You cannot define a different configuration for each type of server.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See "Chapter 4 - IP Address and Network Configuration" on page 51 for more details.

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

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

   This variable defines whether the Mediatrix 2102 must ask for its outbound proxy settings through a DHCP server or not.

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

   You can query the 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

SIP Outbound Proxy (From RFC 3261)

A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a user agent is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols.

When enabled, the initial route for all SIP requests containa the outbound proxy address, suffixed with the loose routing parameter "lr". The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy).

3. Set how you want to define the outbound proxy server information in the DHCP server.

Table 56: Outbound Proxy Server DHCP Information

To use a...	Set...
vendor specific code	The *sipOutboundProxyDhcpSiteSpecificCode* variable (under the *ipAddressConfigSipServer* group) to **0**. Set the outbound proxy server IP address in the DHCP server inside the vendor specific sub-option 205 (hexadecimal 0xCD).
site specific code	The *sipOutboundProxyDhcpSiteSpecificCode* variable (under the *ipAddressConfigSipServer* group) to any value between 128 and 254. Set the outbound proxy server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *sipOutboundProxyDhcpSiteSpecificCode* variable in the unit's configuration).

Static Configuration

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

▶ **To use static information:**

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

This variable defines whether the Mediatrix 2102 must ask for its outbound proxy settings through a DHCP server or not.

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

3. Set the following variables:

Table 57: Outbound Proxy Static Information

Variable	Description
sipOutboundProxyStaticHost	Static outbound proxy server IP address or domain name. **Default Value**: 192.168.0.10
sipOutboundProxyStaticPort	Static outbound proxy server IP port number. **Note**: If this variable corresponds to a domain name that is bound to a SRV record, the port must be set to **0** for the unit to perform DNS requests of type SRV (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather use only requests of type A because it does not need to be specified which port to use. **Default Value**: 0

▶ **To disable the outbound proxy:**

1. In the *ipAddressConfig* folder, set the *sipOutboundProxyStaticHost* variable to **0.0.0.0**.

To re-enable the outbound proxy, enter a valid IP address.

You can now specify if the outbound proxy uses a loose routing or strict routing type.

Loose Router Configuration

Standards Supported	RFC 3261 – SIP: Session Initiation Protocol, section 6 RFC 2543 – SIP: Session Initiation Protocol

You must specify the type of routing of the outbound proxy configured in *sipOutboundProxyHost* does.

> **Note:** This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See "MIB Structure" on page 43 for more details.

▶ **To set the outbound proxy router status:**

1. In the *sipMIB*, locate the *sipOutboundProxyConfig* variable.

   The following values are available:

Table 58: Outbound Proxy Router Status

Value	Description
looseRouter	This is the most current method for SIP routing, as per RFC 3261, and will become the standard behaviour once RFC 3261 compliance is achieved. See "SIP Outbound Proxy (From RFC 3261)" on page 75 for details.
strictRouter	Pre-RFC 3261, RFC 2543 compatible SIP routing. The initial route for all SIP requests contains the home domain proxy address (the Request-URI). Requests are directed to the outbound proxy. In other words, the Request-URI is constructed as usual, using the home domain proxy and the user name, but is used in the route set. The Request-URI is filled by the outbound proxy address.

Loose Router

A proxy is said to be loose routing if it follows the procedures defined in the *RFC 3261* specification (section 6) for processing of the *Route* header field. These procedures separate the destination of the request (present in the Request-URI) from the set of proxies that need to be visited along the way (present in the *Route* header field). A proxy compliant to these mechanisms is also known as a loose router.

CHAPTER 6

DNS SRV Configuration

This chapter describes the configuration required for the Mediatrix 2102 to work with a DNS SRV.

What is a DNS SRV?

Standards Supported	• RFC 2782 – A DNS RR for specifying the location of services (DNS SRV) • RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers

Currently, one must either know the exact address of a server to contact it, or broadcast a question.

DNS SRV is an extension of the standard DNS server. SRV (Service Record) is a type of entry a network administrator may put into the DNS answers. A DNS SRV is used to get one or more IP addresses of servers, each one having its own weight and priority.

Each server received when using DNS SRV, depending on its weight and priority, can be used as a primary or backup server or can be part of a load balancing system.

For instance, the client requests the SRV for SIP servers in some domain. The DNS server may return the A, B, and C addresses, which are all SIP servers. Each address has a weight and the client must choose one of those three addresses by using a random algorithm that considers the weight.

To use DNS SRV, an administrator must set a service records (SRV) into the DNS servers available on the network.

DNS SRV implementation should imply a shared database between servers since a REGISTER and an INVITE can be sent to any server, not necessarily the same one.

DNS SRV applies to both TCP and UDP transport types.

Priority vs Weight

A DNS SRV uses the *priority* and *weight* concepts to distribute the requests.

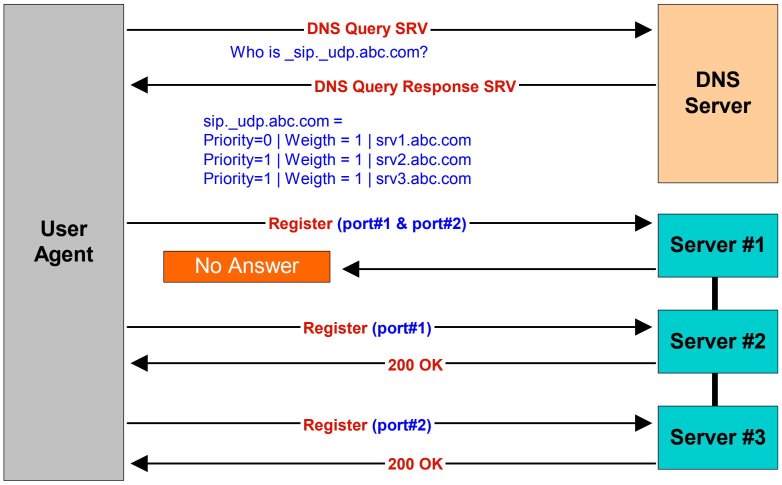
Table 59: Priority vs. Weight

Parameter	Description
Priority	A client must attempt to contact the target host with the lowest-numbered priority it can reach.
Weight	Specifies a relative weight for entries with the same priority. Larger weights should be given a proportionately higher probability of being selected.

DNS SRV Call Flow

The following is a standard DNS SRV call flow:

Figure 26: DNS SRV Call Flow


User Agent
DNS Server
DNS Query SRV
Who is _sip._udp.abc.com?
DNS Query Response SRV
sip._udp.abc.com =
Priority=0 | Weigth = 1 | srv1.abc.com
Priority=1 | Weigth = 1 | srv2.abc.com
Priority=1 | Weigth = 1 | srv3.abc.com
Register (port#1 & port#2)
Server #1
No Answer
Register (port#1)
Server #2
200 OK
Register (port#2)
Server #3
200 OK

Enabling DNS SRV on the Mediatrix 2102

If the address of a service corresponds to a domain name that is bound to a SRV record, the port this service uses must be set to **0** for the unit to perform DNS requests of type SRV (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather use only requests of type A because it does not need to be specified which port to use. See "Chapter 5 - SIP Servers" on page 71 for more details.

▶ **To enable DNS SRV:**

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

   This variable defines whether the Mediatrix 2102 must get its proxy server configuration through a DHCP server or not.

2. Set the *sipServerSelectConfigSource* variable to **static**.
3. Set one or more of the following variables to **0**:

Table 60: Variables to Enable DNS SRV

Server	Variable to enable
SIP Registrar server	sipRegistrarStaticPort
SIP Proxy server	sipHomeDomainProxyStaticPort
SIP Outbound Proxy server	sipOutboundProxyStaticPort

Note: Any "SRV enabled" service must have a host name recognized by the DNS SRV server. "*_sip._udp*" or "*_sip._tcp*" (depending on the transport type) is automatically added to the host name.

DNS SRV Record Lock

You can configure the Mediatrix 2102 to always use the same DNS SRV record for a SIP call ID. As a result, a call or registration always uses the same destination until the destination is unreachable or the unit receives a different DNS SRV result.

▶ **To enable the DNS SRV record lock feature:**

1. In the *sipInteropMIB*, set the *sipInteropLockDnsSrvRecordPerCallEnable* variable to **enable**.

   All messages during a call or registration use the same SRV record.

   If you set this variable to **disable** (which is the default value), the Mediatrix 2102 rather follows the behaviour as described in RFC 3263.

2. Restart the Mediatrix 2102 so that the changes may take effect.

DNS SRV-Oriented Settings

The following parameters have an effect on the DNS SRV behaviour.

Table 61: DNS SRV-Oriented Settings

Parameter	Description
sipInteropTransmissionTimeout	• Has a dramatic effect should a server time out, since a default 32 s delay would be introduced at every call. • Mediatrix recommends a maximum of 2-3 s when using DNS SRV. • See "Transmission Timeout" on page 171 for more details.
sipPenaltyBoxTime	If *sipPenaltyBoxEnable* is set to **enable**: • A "timed out" server is considered "not responding" for this amount of time. • Can be seen as the time it will take to retry a server that failed responding. • See "SIP Penalty Box" on page 173 for more details.
sipInteropReuseCredentialEnable	If *sipInteropReuseCredentialEnable* is set to **enable**: • If there is not a shared database between servers, this could lead to authentication problems because a REGISTER and an INVITE can be sent to any server, not necessarily the same one. • See "SIP Credential" on page 178 for more details.

CHAPTER

7

Country-Specific Configuration

This chapter describes how to set the Mediatrix 2102 with the proper country settings.

Caller ID Information

The caller ID is a generic name for the service provided by telephone utilities that supply information such as the telephone number or the name of the calling party to the called subscriber at the start of a call. In call waiting, the caller ID service supplies information about a second incoming caller to a subscriber already busy with a phone call. However, note that caller ID on call waiting is not supported by all caller ID-capable telephone displays.

In typical caller ID systems, the coded calling number information is sent from the central exchange to the called telephone. This information can be shown on a display of the subscriber telephone set. In this case, the caller ID information is usually displayed before the subscriber decides to answer the incoming call. If the line is connected to a computer, caller information can be used to search in databases and additional services can be offered.

The following basic caller ID features are supported:

- Date and Time
- Calling Line Identity
- Reason for Absence of Calling Line Identity
- Calling Party Name
- Reason for Absence of Calling Party Name
- Visual Indicator (MWI)

Caller ID Generation

There are two methods used for sending caller ID information depending on the application and country-specific requirements:

- caller ID generation using DTMF signalling
- caller ID generation using Frequency Shift Keying (FSK)

Both methods can be used on different lines at the same time.

The displayed caller ID for all countries may be up to 20 digits for numbers and 50 digits for names.

DTMF Signalling

The data transmission using DTMF signalling is performed during or before ringing depending on the country settings or line configuration. The Mediatrix 2102 provides the calling line identity according to the following standards:

- Europe: ETSI 300 659-1 January 2001 (Annex B) : Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 1: On-hook data transmission.
- Brazil: STD 220-250-713 Issue 01. November 1993: General specification “identification of the calling party for SPC with DTMF”.

> **Note:** For units in Brazil, set the *analogScnGwInterDigitDialDelay* and *analogScnGwDtmfDuration* value to **70** ms (in the *analogScnGwMIB*). This will ensure that the caller ID displays properly.

- Denmark: TDK-TS 900 301-1 January 2003: Public Switched Telephone Network (PSTN) Calling Line Identification presentation (CLIP) supplementary service Specification of the NTP.

FSK Generation

Different countries use different standards to send caller ID information. The Mediatrix 2102 is compatible with the following widely used standards:

- Bellcore GR-30-CORE
- British Telecom (BT) SIN227, SIN242
- UK Cable Communications Association (CCA) specification TW/P&E/312
- ETSI 300 659-1

Note: The compatibility of the Mediatrix 2102 is not limited to the above caller ID standards.

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

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

ADSI

ADSI (Analog Display Service Interface) is a telecommunications protocol standard that enables alternate voice and data capability over the existing analog telephone network. It is an extension to basic caller ID. To use ADSI, you would need an ADSI capable device.

ADSI can display the basic caller ID parameters and the following additional parameters:

- Call Type
- First Called Line Identity
- Number of Messages (MWI)
- Type of Forwarded Call
- Type of Calling User
- Redirecting Number
- Charge
- Duration of the Call
- Network Provider Identity

Note: Currently, very few ADSI-capable devices support these additional information.

Setting the Location (Country)

It is very important to set variables according to the country in which the Mediatrix 2102 is used because a number of parameter values are set according to this choice. These parameters are:

- Tones
- Rings
- Impedances
- Line Attenuations

See “Appendix D - Country-Specific Parameters” on page 269 for more information on these country-specific settings.

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

To set a country location:

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

This variable indicates the current country used by the Mediatrix 2102. It can also be used to select a caller ID standard in countries that support more than one caller ID standard.

2. Set the variable with one of the following parameters:

North America 1
North America 2
Austria
France
Germany 1
Germany 2
UK
Italy
Spain
Switzerland
Sweden
Australia 1
Australia 2
Australia 3
Japan
Israel
Thailand
Indonesia
China
Hong Kong
Malaysia
Russia
Netherlands
Brazil
Mexico
Denmark
New Zealand
uk-bellcore
uk-cca
uk-etsi-fsk
france-etsi-fsk
france-etsi-dtmf

3. Restart the Mediatrix 2102 so that the changes may take effect.

Caller ID Selection

In countries that support more than one caller ID standard, this standard can be selected with the *telephonyCountrySelection* variable. Be careful to properly select the option corresponding to your caller ID.

Table 62: Caller ID Mappings

Country	Caller ID	***telephonyCountrySelection* variable Mapping**
UK	British Telecom	uk
	Bellcore	uk-bellcore
	CCA	uk-cca
	ETSI-FSK	uk-etsi-fsk
France	Bellcore	france
	ETSI-FSK	france-etsi-fsk
	ETSI-DTMF	france-etsi-dtmf

See "Caller ID Information" on page 83 for more details.

CHAPTER 8

Transparent Address Sharing

This chapter explains how to properly configure the Transparent Address Sharing service for a cable or DSL modem. When the Mediatrix 2102 is set in this mode, it shares a public IP address with a networked PC or other IP equipment.

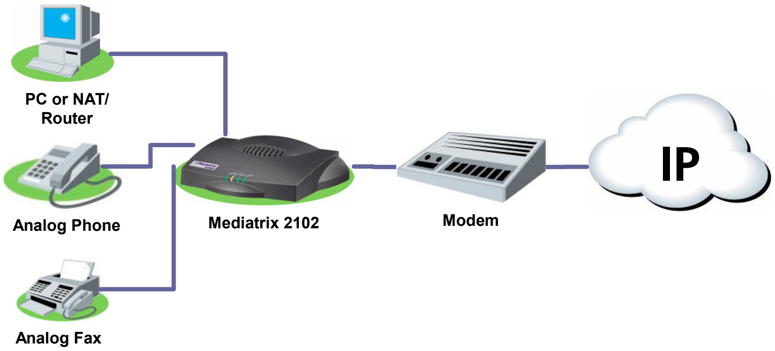
What is Transparent Address Sharing?

When in Transparent Address Sharing (TAS) mode, the Mediatrix 2102 creates a Local Area Network (LAN) between itself and the PC and routes IP packets between the LAN and the network providing the public address, generally a Wide Area Network (WAN).

The Mediatrix patent on transparent IP address sharing allows both WAN and LAN interfaces to be used with a single IP address from the service provider in a user-friendly way, without the configuration complexities of an integrated NAT.

The Mediatrix 2102 thus connects up to two analog phones or fax machines to a broadband access equipment, allowing Service Providers to offer IP telephony services to residential users.

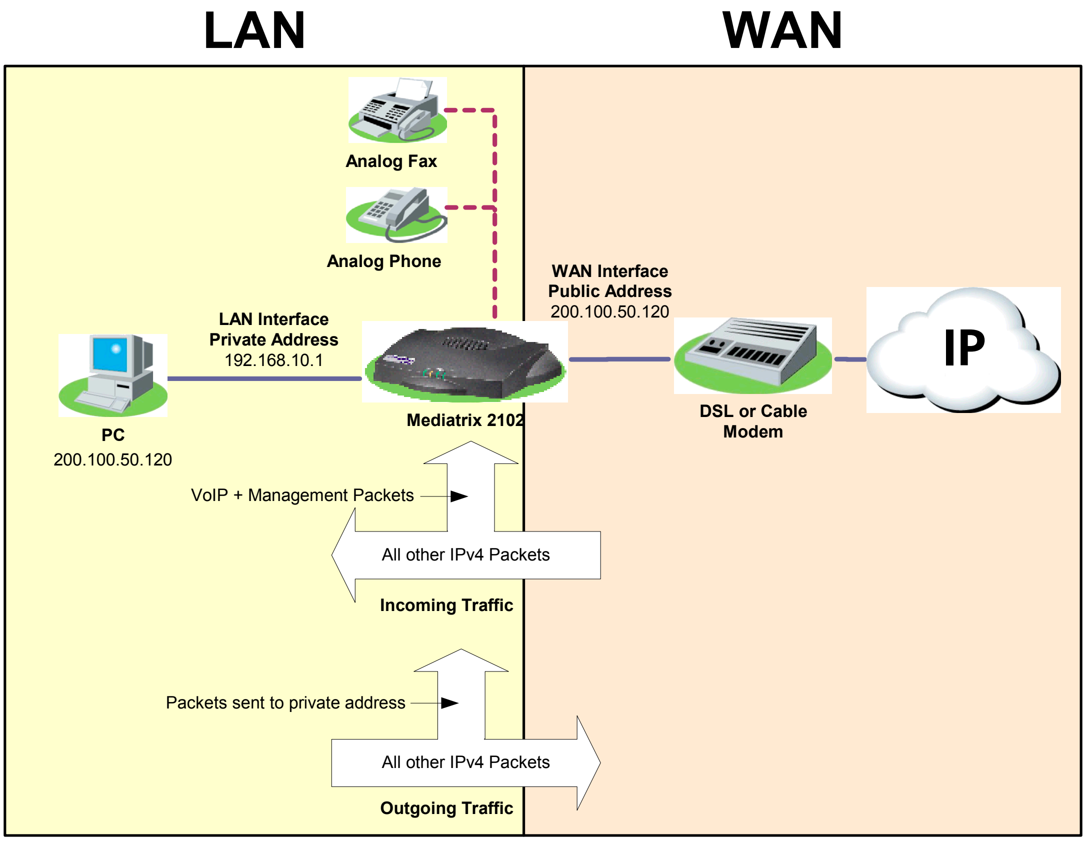
Figure 27: Mediatrix 2102 Residential Application Scenario



In a residential VoIP deployment, the WAN interface of the Mediatrix 2102 gets assigned a public IPv4 address by the ISP, either by a DHCP negotiation, or by establishing a point-to-point link (PPPoE), or by some other mechanism depending on the type of link.

The device on the LAN (e.g., the PC) gets assigned the same public IPv4 address as the Mediatrix 2102, by using the DHCP. The subnet mask given is the same as the one assigned by the ISP, or if it is not available (such as for a PPPoE connection), it uses the predefined subnet classes.

Figure 28: Transparent Address Sharing



The LAN interface of the Mediatrix 2102 is configured with a private IPv4 address. This address allows the device on the LAN to communicate with the Mediatrix 2102 as this would be otherwise impossible because both devices share the same public IPv4 address. The Mediatrix 2102 performs transparent routing by forwarding to the WAN any packet sent to any IPv4 address that is included in the public subnet.

Each packet received from the WAN is forwarded directly to the device on the LAN, except if it belongs to the hosted application, in this case, VoIP. In the other direction, each IPv4 packet received from the LAN is forwarded to the WAN, except for packets sent explicitly to the private address assigned to the Mediatrix 2102. The Mediatrix 2102 itself can initiate a communication with the device on the LAN, by using its private IPv4 address as the source address.

Router Mode

The router mode separates the two external interfaces of the Mediatrix 2102 (the *Computer* and *Network* connectors). The Mediatrix 2102 has two distinct network interfaces with one IP address for each of them. These interfaces are called LAN (*Computer* connector) and WAN (*Network* connector).

At the internal level, the interfaces are called “bcm0” and “bcm1” and the Mediatrix 2102 performs IP routing both ways.

The router mode is a requirement for the TAS to properly work. When enabling TAS, you also enable the Mediatrix 2102 in router mode.

The router mode is also a requirement for the Bandwidth Control feature (“WAN Upstream Bandwidth Control” on page 97).

In non-router mode, the interfaces are switched and the Mediatrix 2102 only has one network interface – called “bcm0”. Both external network interfaces generally have the same behaviour.

Cable vs DSL Modem

Most of the Mediatrix 2102 settings are the same no matter what the modem you are using. However, there are a few differences.

Table 63: Cable vs DSL Modem

Cable Modem	DSL Modem
You must configure the Mediatrix 2102 to use a DHCP server to get its IP information as per "DHCP Server Configuration" on page 63. However, some locations may require to manually enter static IP information instead. The easiest way to do so is to use the web interface. See "Chapter 2 - Web Interface" on page 25 for more details.	You must configure the PPPoE service as per "PPPoE Service" on page 90. However, some DSL modems may require that you configure the Mediatrix 2102 to use a DHCP server to get its IP information as per "DHCP Server Configuration" on page 63.

Multicast and IGMP

The Mediatrix 2102 does not support the IGMP (Internet Group Management Protocol) protocol, i.e., the PC connected to the *Computer* connector of the Mediatrix 2102 cannot register to IGMP services.

Multicast is communication between a single sender and multiple receivers on a network. IGMP is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content.

Configuration Steps

The following are the steps to follow to properly setup the TAS service and where to get information on each of these steps.

▶ **To setup the TAS service:**

1. Define the PPPoE parameters as described in "PPPoE Service" on page 90. **This only applies if you are using a DSL modem.**
2. Define the WAN IP address configuration source as described in "WAN Information Configuration Source" on page 92.
3. Configure the TAS mechanism as described in "Configuring TAS" on page 93.
4. Optionally, modify port allocation settings as described in "Ports Settings" on page 99.
5. Restart the Mediatrix 2102 so that the changes may take effect.

PPPoE Service

Standards Supported	• RFC 1332 – IP Control Protocol (IPCP) • RFC 1661 – Point to Point Protocol (PPP) • RFC 1334 – Password Authentication Protocol (PAP) • RFC 1994 – Challenge Handshake Authentication Protocol (CHAP) • RFC 2516 – PPP over Ethernet (PPPoE) • RFC 1471 – PPP Link control Protocol MIB (PPP-LCP-MIB) (with the exception of the LQR MIB) • RFC 1472 – PPP Security Protocols MIB (PPP-SEC-MIB) • RFC 1473 – PPP IP Network Control Protocol MIB (PPP-IP-NCP-MIB) • RFC 1877 – PPP IPCP Extentions for Name Server Address – with the exception of sections 1.2 and 1.4

The Mediatrix 2102 uses the PPPoE protocol to interact with a DSL broadband modem. It can discover a PPP access concentrator (AC) and establish a PPP session with it.

Note: This section applies only if you are using a DSL modem. If you are using a cable modem, go directly to “WAN Information Configuration Source” on page 92.

The PPPoE service is required to properly use the TAS service with DSL modems. You must perform the following tasks to configure the PPPoE service:

- Enable the PPPoE service.
- Set a user name and password.

Enabling the PPPoE Service

You must configure and enable the service to properly connect to an access concentrator.

You can also use the web interface to enable the PPPoE service. See “Administration Page” on page 29 for more details.

▶ To configure the PPPoE service:

1. In the *ipAddressConfig* folder, set the *localHostSelectConfigSource* variable (under the *ipAdressConfigLocalHost* group) to **static**.

   This is required to avoid conflicts with the PPPoE interface. See “Local Host” on page 54 for more details on the local host settings.

2. Set the *localHostStaticDefaultRouter* variable (under the *ipAddressConfigLocalHostStatic* group) to **0.0.0.0**.

3. In the *pppoeMIB*, set the *pppoeAcName* variable with the name of the access concentrator to which connect.

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

PPPoE

PPPoE (Point to Point Protocol over Ethernet) is a proposal specifying how a host personal computer interacts with a DSL broadband modem to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dialup Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

If you leave this variable empty, the Mediatrix 2102 accepts the first offer that it receives.

4. Set the *pppoeServiceName* variable with the name of the service requested to the access concentrator.

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

   If you leave this variable empty, the Mediatrix 2102 looks for any access concentrator.

5. Enable the PPPoE service by setting the *pppoeEnable* variable to **enable**.

Note: When establishing a PPPoE connection, the default router IP address is automatically overridden by the PPP connection's peer IP address.

6. If you do not need to configure other parameters, restart the Mediatrix 2102 as per "Restarting the Mediatrix 2102" on page 100.

Setting a User Name and Password

When connecting to an access concentrator, it usually requests that the Mediatrix 2102 identifies itself with a specific user name and password, also called ID and secret pair. This information is set in the standard *PPP-SEC-MIB* as described in RFC 1472.

You can also use the web interface to enter the PPPoE user name and password. See "Administration Page" on page 29 for more details.

▶ **To configure a user name and password:**

1. In the *PPP-SEC-MIB*, locate the *pppSecuritySecretsTable*.

   This table contains the ID (user name) and secret (password) pair that the Mediatrix 2102 advertises to the access concentrator.

Caution: When you are in a specific row and you set the *pppSecuritySecretStatus* variable of this row to **invalid**, the row is deleted and you cannot add it back. When the last remaining row is deleted, two rows are re-created with default passwords and user names.

2. Set the Identity (user name) of the ID/Secret pair in the *pppSecuritySecretsIdentity* variable.

   You can set an identity for both security protocols (CHAP and PAP) supported. The table contains one row for each protocol. The CHAP security protocol is described in RFC 1994, while the PAP security protocol is described in RFC 1334. If you want to exclusively use one of the security protocols, you can disable the other row.

3. Set the secret (password) of the ID/Secret pair in the *pppSecuritySecretsSecret* variable.

   You can set an identity for both security protocols (CHAP and PAP) supported. The table contains one row for each protocol. The CHAP security protocol is described in RFC 1994, while the PAP security protocol is described in RFC 1334. If you want to exclusively use one of the security protocols, you can disable the other row.

   For other standard settings, please refer to the MIBs described in RFC 1471 (with the exception of the LQR MIB), RFC 1472, and RFC 1473.

4. If you do not need to configure other parameters, restart the Mediatrix 2102 as per "Restarting the Mediatrix 2102" on page 100.

WAN Information Configuration Source

The Wide Area Network (WAN) address is the public IP address attributed to the Mediatrix 2102. This address is used for incoming signalling, media and management traffic. You can assign this information to the Mediatrix 2102 through an access concentrator (DSL modem) or DHCP server (cable modem).

▶ **To set the WAN IP address configuration source:**

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

   This variable indicates the source to be used for the provisioning of the WAN address. It offers the following choices:

   Table 64: WAN IP Address Source Settings

Option	Description
localAddress	The Mediatrix 2102 is not part of a WAN or the public address is the same as the *localHostAddress*.
static	The Mediatrix 2102 has a static WAN address. The address is configured in the *localHostStaticWanAddress* variable. Note that this setting allows a limited NAT traversal scheme.
pppoe	The Mediatrix 2102 uses the PPP interface’s address as the WAN address. **Note**: The PPPoE service must be enabled for the WAN address to be configured.
automatic	If the PPPoE service is enabled, the Mediatrix 2102 uses *pppoe* as the configuration source. Otherwise it uses *localAddress*.

2. Set the *localHostWanAddressSelectConfigSource* variable to **automatic**.

   You can query the actual configuration source used in the *localHostWanAddressConfigSource* read-only variable (in the *ipAddressStatus* folder).

   You can query the actual WAN IP address attributed to the Mediatrix 2102 in the *localHostWanAddress* read-only variable (in the *ipAddressStatus* folder).

3. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100.

Configuring TAS

The following steps describe how to properly setup and enable the Mediatrix 2102 in TAS mode. By enabling TAS, you also implicitely enable the Mediatrix 2102 in router mode. See “Router Mode” on page 88 for more details.

When the TAS service is enabled, it adds a network interface to the Mediatrix 2102. This means that two IP addresses may be attributed to the unit – the *Computer* and *Network* connectors of the Mediatrix 2102 each have an IP address.

> **Note:** When you dial the ***#*0** digits on a telephone connected to the Mediatrix 2102, the LAN IP address is returned. When you dial the ***#*2** digits on a telephone connected to the Mediatrix 2102, the WAN IP address is returned. See “Special Vocal Features” on page 15 for more details.

The *Computer* and *Network* connectors of the Mediatrix 2102 are allocated IP addresses differently depending on the scenario involved:

- **TAS disabled**

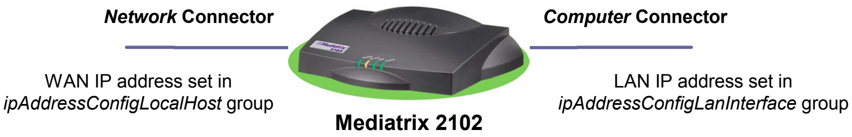
  The *Computer* and *Network* connectors use the same IP address as set in the *localHostAddress* variable. See “Local Host” on page 54 for more details.

- **TAS enabled - cable modem (PPPoE disabled)**

  The *Network* connector receives an IP address to access the WAN. This IP address is coming from the DHCP server and is stored in the *localHostAddress* variable. See “Local Host” on page 54 for more details.

  The IP address of the *Computer* connector (LAN interface) is configured statically, as described in “LAN Interface” on page 95.

Figure 29: Cable Modem IP Addresses


Network Connector
WAN IP address set in *ipAddressConfigLocalHost* group
Computer Connector
LAN IP address set in *ipAddressConfigLanInterface* group
Mediatrix 2102

For example:

- The Mediatrix 2102 is set up to get a WAN address via DHCP.
- The local host address is set to the DHCP-derived address (let’s say 10.40.40.53).
- The LAN side address is also 10.40.40.53. This is consistent with the transparent IP address sharing feature.

The *lanStaticAddress* variable is set by default to 192.168.10.1.

In summary:

a. WAN is good.

IP address 10.40.40.53 on both sides, WAN and LAN.

The web page of the Mediatrix 2102 is at 192.168.10.1.

b. WAN goes down.

The IP address 10.40.40.53 is not available on the WAN side.

The web page of the Mediatrix 2102 is still at 192.168.10.1.

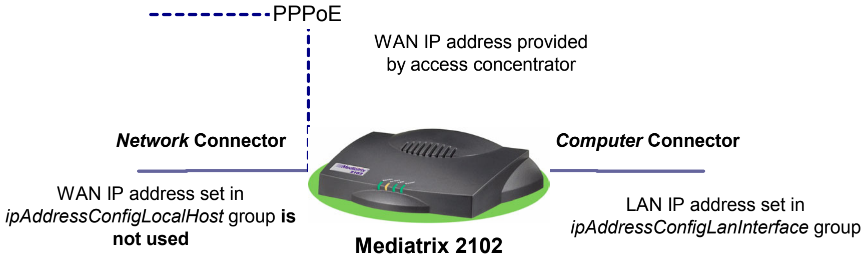
The IP address of the *Computer* connector is then IP address of the Mediatrix 2102 plus or minus 1, i.e., the IP address of the *Computer* connector is 192.168.10.0 or 192.168.10.2.

- **TAS enabled - DSL modem (PPPoE enabled)**

  The *Network* connector receives an IP address to access the WAN. This IP address is coming from the access concentrator and is stored in the *localHostWanAddress* variable. In this case, the IP address in the *localHostAddress* variable is not used.

  The IP address of the *Computer* connector (LAN interface) is configured statically, as described in “LAN Interface” on page 95.

Figure 30: DSL Modem IP Addresses (PPPoE)


PPPoE
WAN IP address provided by access concentrator
Network Connector
Computer Connector
WAN IP address set in *ipAddressConfigLocalHost* group **is not used**
Mediatrix 2102
LAN IP address set in *ipAddressConfigLanInterface* group

QoS Differentiated Services Fields

If you want to differentiate the packets sent by the PC from the packets sent by the Mediatrix 2102, you must substitute a configured value for the QoS Differentiated Services fields of the packets sent from the PC.

The goal is to prioritise the Mediatrix 2102’s packets over the PC’s packets. This allows to offer a quicker response time for the voice, for instance. However, the ISP’s network must support QoS routing. It must be configured accordingly and route according to the DiffServ it encounters.

See “Differentiated Services (DS) Field” on page 227 for more details on how to set the Mediatrix 2102 QoS Differentiated Services fields.

▶ **To configure a substitution value:**

1. In the *ipRoutingMIB*, set the substitution value in the *ipRoutingQosDiffServSubstitution* variable.

   This substitution value is used for the Differentiated Services fields of all packets. This value supersedes the TOS byte of the packets coming from the PC. The default value is **0**.

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

   When enabled, the QoS Differentiated Services fields of all packets are overwritten. If the variable is disabled, the QoS Differentiated Services fields of the packets are not modified.

3. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100.

LAN Interface

The Mediatrix 2102's two Ethernet connectors are used as follows:

- *Network* connector: WAN interface of the Mediatrix 2102 where you can connect your modem.
- *Computer* connector: LAN interface where you connect the PC or other IP equipment. The LAN interface is usually used to connect a PC that will have access to the WAN by sharing the Mediatrix 2102 WAN address.

Note: The LAN interface configuration settings are valid only when TAS is enabled.

You can also use the web interface to configure the LAN interface parameters. See "Administration Page" on page 29 for more details.

To configure the LAN interface settings:

1. In the *ipAddressConfig* folder, locate the *ipAddressConfigLanInterface* group).
2. Set the LAN IP address of the *Computer* connector in the *lanStaticAddress* variable.

   If TAS is disabled, the *Computer* connector rather uses the same address as the *Network* connector as set in the *localHostAddress* variable. See "Local Host" on page 54 for more details.
3. Set the LAN subnet mask of the *Computer* connector in the *lanStaticNetworkMask* variable.

   If TAS is disabled, the *Computer* connector rather uses the same network mask as the *Network* connector as set in the *localHostNetworkMask* variable. See "Local Host" on page 54 for more details.
4. If you do not need to configure other parameters, restart the Mediatrix 2102 as per "Restarting the Mediatrix 2102" on page 100.

MAC Address Spoofing

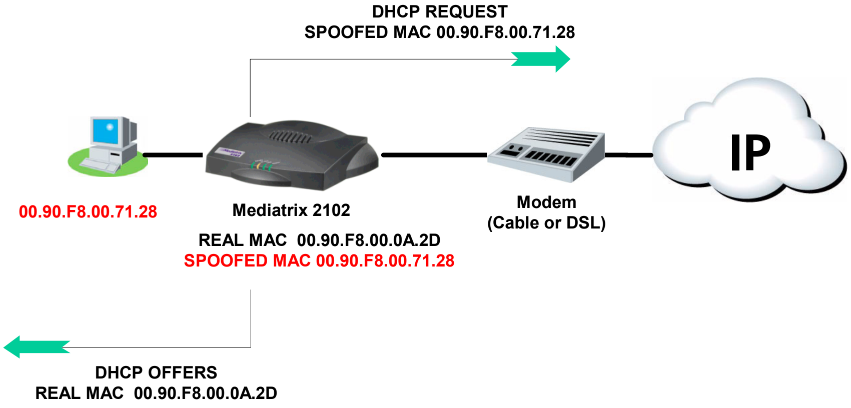
A number of ISPs control connections to their servers by monitoring the MAC address of the connecting device. If the MAC address does not match its database, it refuses the connection.

Consider the typical scenario in which a user of a Mediatrix 2102 is already subscribed to an ISP for a WAN access (i.e., the Internet). If the ISP monitors the MAC address, the user will not be able to connect to the WAN when using the Mediatrix 2102 in front of the usual device.

The workaround is to have the Mediatrix 2102 spoof its MAC address in messages destined to the WAN. The spoofed MAC address matches the ISP's database and the connection will be granted. However, the spoof is only performed on the WAN side of the Mediatrix 2102. The LAN (or private) side of the Mediatrix 2102 remains unchanged.

For example, DHCP requests sent by the Mediatrix 2102 on the WAN side would contain the spoofed MAC address, but DHCP offers returned by the Mediatrix 2102 to the device networked on the *Computer* connector will contain the real MAC address of the Mediatrix 2102.

Figure 31: MAC Address Spoofing


DHCP REQUEST
SPOOFED MAC 00.90.F8.00.71.28
IP
00.90.F8.00.71.28
Mediatrix 2102
Modem
(Cable or DSL)
REAL MAC 00.90.F8.00.0A.2D
SPOOFED MAC 00.90.F8.00.71.28
DHCP OFFERS
REAL MAC 00.90.F8.00.0A.2D

You can also use the web interface to enter the MAC address spoofing information. See “Administration Page” on page 29 for more details.

▶ **To spoof the MAC address:**

1. In the *ipRoutingMIB*, set the MAC address used to spoof the unit’s actual MAC address in the *ipRoutingMacSpoofAddress* variable.

A valid MAC address is a continuous series of 12 alphanumeric characters (i.e., without colons). An empty character string means that the spoofing is considered disabled, even though the *ipRoutingMacSpoofEnable* variable is set to **enable**.

> **Note:** The following MAC addresses are not allowed:
> - 000000000000
> - FFFFFFFFFFFF
> - 01xxxxxxxxxx, where x can be any digit or letter

The MAC address could be the one of the PC connected to the Mediatrix 2102. You can view the current MAC address of the online device in the *Computer* connector in the *ipRoutingMacAddress* variable (*ipRoutingMacSpoof* group of the *ipRoutingMIB*).

> **Note:** When dialing the ***#*1** digits on a telephone connected to the Mediatrix 2102, the real MAC address of the unit is returned, not the spoofed one. See “Special Vocal Features” on page 15 for more details.

2. Enable the MAC address spoofing by setting the *ipRoutingMacSpoofEnable* variable to **enable**.

The unit's MAC address used on the WAN side is the configured MAC address.

If you set the variable to **disable**, the unit’s MAC address used on the WAN side is the actual unit’s MAC address.

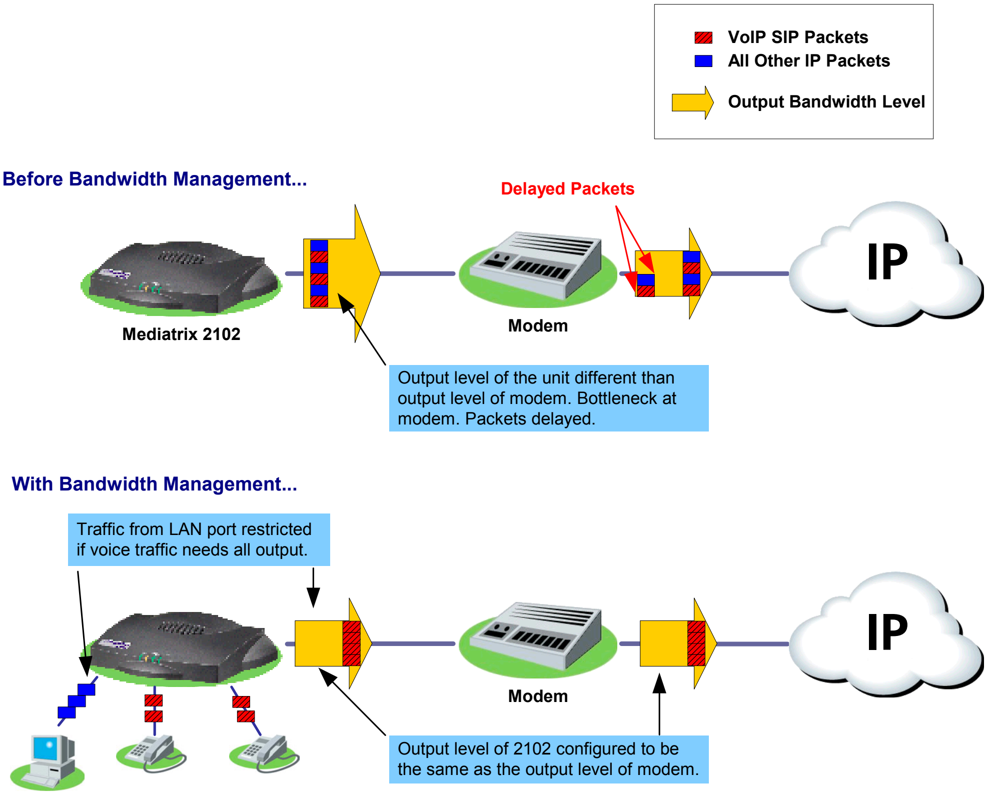
3. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100.

WAN Upstream Bandwidth Control

The bandwidth management feature limits the upload bandwidth on the WAN interface. This allows to optimize the voice quality over an Ethernet link; the Mediatrix 2102 knows the available bandwidth on its WAN interface and can slow down the traffic coming from its LAN interface to use all the available bandwidth for voice traffic first.

When the bandwidth control is enabled, packets sent from the PC or IP equipment to the WAN are limited in bandwidth. You can determine the maximum bandwidth. Excess packets coming from the LAN interface are dropped. The Mediatrix 2102 uses the priorities set in "IEEE 802.1q" on page 229 to determine which packets to drop first, even when 802.1q tagging is disabled.

Figure 32: Bandwidth Management


VoIP SIP Packets
All Other IP Packets
Output Bandwidth Level
Before Bandwidth Management...
Delayed Packets
IP
Mediatrix 2102
Modem
Output level of the unit different than output level of modem. Bottleneck at modem. Packets delayed.
With Bandwidth Management...
Traffic from LAN port restricted if voice traffic needs all output.
Modem
IP
Output level of 2102 configured to be the same as the output level of modem.

You can also use the web interface to configure the bandwidth management feature. See "Bandwidth Management Page" on page 35 for more details.

▶ To configure the WAN upstream bandwidth control:

1. In the *ipRoutingMIB*, set the maximum outgoing amount of data transferred (throughput) to the WAN interface in the *ipRoutingWanUpstreamBandwidth* variable.

   Outgoing traffic includes both traffic generated by voice calls from the Mediatrix 2102 and traffic coming from the PC or IP equipment on the LAN side. The value is expressed in kilobits per seconds.

   It applies only when the *ipRoutingBandwidthControlEnable* variable is set to *enable*. The default value is **512** kbps.

2. Enable the WAN upstream bandwidth control by setting the *ipRoutingBandwidthControlEnable* variable to **enable**.

   The Mediatrix 2102 will limit the outgoing throughput on the WAN interface. The unit must be in router mode to properly use the bandwidth control. See “Router Mode” on page 88 for more details.

> **Note:** If TAS is not enabled, the Mediatrix 2102 will still prioritize voice over the signalling and SNMP/HTTP information on a low bandwidth connection.

If you set the variable to **disable**, the bandwidth from the PC or IP equipment to the WAN is not limited.

Enabling TAS

Enabling TAS is essential to use a broadband connection. By enabling TAS, you also implicitely enable the Mediatrix 2102 in router mode. See “Router Mode” on page 88 for more details.

▶ **To configure TAS:**

1. In the *ipRoutingMIB*, set the duration, in seconds, of the lease offered by the DHCP server in the *ipRoutingDhcpServerLeaseTime* variable (in the *ipRoutingDhcp* group).

   The TAS service of the Mediatrix 2102 contains a DHCP server. Enabling TAS also enables this DHCP server, which allocates IP addresses to the PC or IP equipment located on the LAN.

> **Note:** The DHCP server embedded in the Mediatrix 2102 allocates only one address. To connect more PCs to the Mediatrix 2102, use a router.

The *ipRoutingDhcpServerLeaseTime* variable is the lease time given to the PC connected to the Mediatrix 2102.

- If the lease time is short, the PC will react faster to address changes, but it will have to renew its lease often.
- If the lease time is long, the PC will react more slowly to address changes.

2. Enable TAS by setting the *ipRoutingEnable* variable to **enable**.

   You may want to disable the factory reset procedure of the Mediatrix 2102, even if users depress the *Default Settings* switch. By default, the factory reset reverts the configuration of the system to default factory settings. See “Disabling the Factory Reset” on page 23 for more details.

3. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100

   Optionally, you may want to modify the port allocation settings.

Ports Settings

The Mediatrix 2102 allows you to define how to dynamically allocate the ports it uses. This allows for better NAT and firewall traversal capabilities.

UDP and TCP Ports

When needed, the TCP/IP implementation of the Mediatrix 2102 randomly selects a dynamic port amongst the free ports of the range.

Let’s say for instance that the dynamic ports range is from 41000 to 42000. The Mediatrix 2102 needs to download a new version of its software. The TCP/IP implementation selects a local UDP port for the TFTP client. The port is selected in the dynamic ports range so the port has a value between 41000 and 42000.

▶ **To set the range of the UDP and TCP ports:**

1. In the *sysConfigMIB*, set the lower boundary for the range of dynamic UDP and TCP ports in the *sysConfigMinDynamicPort* variable.

   The default lower boundary value is **31001**.

2. Set the upper boundary for the range of dynamic UDP and TCP ports in the *sysConfigMaxDynamicPort* variable.

   The default upper boundary value is **32000**.

3. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100.

Note: The smallest acceptable range – between the lower and upper boundaries – is 500.

T.38 Base Port Range

The T.38 ports are allocated starting from the base port. T.38 uses one port for each FXS interface.

▶ **To define a T.38 base port:**

1. In the *dataIfMIB*, set the *dataIfT38BasePort* variable with the port number you want to use as T.38 base port.

   The default T.38 base port is **6004**. In the case of the base port defined on 6004:

   - If there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it uses the T.38 port 6004.
   - If there is currently a call on FXS connector 1 and FXS connector 2 has an incoming or outgoing call, then FXS connector 2 uses the T.38 port 6005.

2. If you do not need to configure other parameters, restart the Mediatrix 2102 as per “Restarting the Mediatrix 2102” on page 100.

UDP and TCP Ports Ranges

The UDP and TCP ports are separated in three ranges: well-known ports (0 to 1023), registered ports (1024 to 49151) and dynamic ports (49152 to 65535). The IANA (Internet Assigned Numbers Authority, www.iana.org) assigns the well-known ports. The IANA also lists the registered ports. The dynamic ports are not under the authority of the IANA. Most TCP/IP implementations use the range 1025 to 65535 for dynamic ports instead of the range defined by the IANA.

RTP/RTCP Base Port Range

The RTP/RTCP ports are allocated starting from the base port. The Mediatrix 2102 may use two or four RTP/ RTCP ports for each FXS interface. It uses two ports in case of a standard call, while it uses four ports in other types of calls such as a conference call, a call transfer, etc.

▶ **To define a RTP/RTCP base port:**

1. In the *rtpMIB*, set the *rtpConfigBasePort* variable with the port number you want to use as RTP/ RTCP base port.

   The default RTP/RTCP base port is **5004**. In the case of the base port defined on 5004:

   - If there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it uses the RTP/RTCP ports 5004 and 5005.
   - If there is currently a standard call on FXS connector 1 and FXS connector 2 has a conference call, then FXS connector 2 uses the RTP/RTCP ports 5006, 5007, 5008, and 5009, which are the next available ports.

2. If you do not need to configure other parameters, restart the Mediatrix 2102 as per "Restarting the Mediatrix 2102" on page 100.

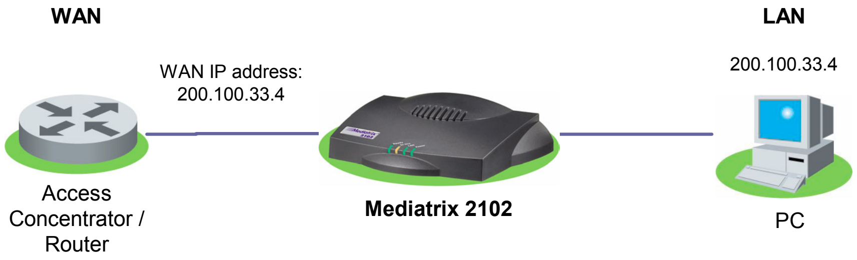
Restarting the Mediatrix 2102

Once all the mandatory and optional changes are done, you must restart the Mediatrix 2102 so that the changes may take effect.

If you are using a DSL modem, the Mediatrix 2102 tries to establish a PPP connection to the access concentrator and service defined in the above steps.

When the router is in "public" state, the IP address of the PC is set to be the exact same as the unit's WAN address. The DHCP server provides the IP address to the PC.

Figure 33: Network Layout with Addresses Example



DHCP Server

Enabling the TAS service also enables a DHCP server that allocates IP addresses to the PC located on the LAN.

DHCP Server Compliance

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

The DHCP server is compliant to RFC 2131, RFC 2132 with the following limitations:

- The pool of assignable IP addresses contains only one address. This means that only one DHCP client at a time can lease an address. All other lease requests are ignored.
- The DHCP server never accepts the IP address requested by the client (option 50) unless by coincidence.
- The DHCP server never accepts the lease time that is proposed by the client (option 51) unless by coincidence.
- The DHCP server returns only the options specified in "Supported DHCP Options" on page 101, all other parameter requests (as part of option 55) are ignored.

Supported DHCP Options

The DHCP server embedded in the Mediatrix 2102 supports the following options.

Table 65: Supported DHCP Option

Code	Description
1	Network Mask When the router state is public, returns a subnet mask that depends on the class of the WAN address, see RFC 791, section 3.2. When the router state is private, returns the network mask as configured in the MIB.
3	Router Option When the router state is public, returns the first address in the subnet. If this address correspond to the Mediatrix 2102 address, the default router's address is the last address in the subnet. When the router state is private, does not return a router IP address.
6	Domain Name Server Option Returns the list of DNS addresses as configured in the MIB.
42	Network Time Server Option Returns the SNTP server address as configured in the MIB. If the MIB contains a FQDN, option 42 contains the resolved IP address.
51	Lease Time Returns 20 seconds.
52	Option Overload Always set to "3".
53	DHCP Message Type
53	Server Identifier Returns the unit's LAN IP address.

DSL Modem Specific Information

The following sections apply only if you are using a DSL modem.

Establishing a Connection

When the Mediatrix 2102 restarts, it establishes the connection to the access concentrator in conformance with the RFCs listed in "PPPoE Service" on page 90.

When establishing a PPP connection, the Mediatrix 2102 goes through three distinct phases:

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

Discovery Phase

The Mediatrix 2102 broadcasts the value of the *pppoeServiceName* MIB variable (see "Enabling the PPPoE Service" on page 90 for more details).

The access concentrator with a matching service name answers the Mediatrix 2102.

- If no access concentrator answers, this creates a "PPPoE failure" error. The Mediatrix 2102 handles it as described in Table 66 on page 103.
- If more than one access concentrators respond to the discovery, the Mediatrix 2102 tries to establish the PPP connection with the first one that supports the requested service name.

Authentication Phase

If the access concentrator requests authentication, the Mediatrix 2102 sends the ID/secret pair configured in the *pppSecuritySecretsTable* (see "Setting a User Name and Password" on page 91 for details). If the access concentrator rejects the authentication, this creates an "authentication failure" error. The Mediatrix 2102 handles it as described in Table 66 on page 103.

Network-Layer Protocol Phase

The Mediatrix 2102 negotiates an IP address. The requested IP address is the one from the last successful PPPoE connection. If the Mediatrix 2102 never connected by using PPPoE (or after a factory reset), it does not request any specific IP address.

When the PPP connection is established, the access concentrator assigns an IP address to the Mediatrix 2102. This IP address may be used as the WAN IP address. See "WAN Information Configuration Source" on page 92 for details.

Primary and secondary DNS servers may be supplied by the access concentrator. If this is the case, the new DNS servers supersede the servers defined locally.

Configuration of DNS Servers

When the PPP connection is active, the DNS servers supplied by the access concentrator supersede the locally defined servers as follows:

- If the *localHostDnsOverrideEnable* variable is set to **enable**, the servers supplied by the access concentrator do not replace the *localHostPrimaryDns* or *localHostSecondaryDns* variables. See "Static DNS" on page 55 for more details.
- If the *localHostDnsOverrideEnable* variable is set to **disable**:
  - If no server is supplied by the access concentrator, the value of the *localHostPrimaryDns* and *localHost SecondaryDns* variables applies.
  - If one server is supplied by the access concentrator, it replaces the server defined in the *localHostPrimaryDns* variable.
  - If two servers are supplied by the access concentrator, they replace both the *localHostPrimaryDns* and *localHostSecondaryDns* variables.

Error Handling

The following describes the Mediatrix 2102 behaviour in case of error.

Table 66: Error Handling

On this error...	The Mediatrix 2102...
Authentication failure	**1.** Waits for 10 seconds. **2.** Retries to establish the connection as in "Establishing a Connection" on page 102.
PPPoE failure	**1.** Waits for 10 seconds. **2.** Retries to establish the connection as in "Establishing a Connection" on page 102.
Peer not responding	**1.** Retries to establish the connection as in "Establishing a Connection" on page 102.

Connection Unsuccessful

When the Mediatrix 2102 restarts, it tries to connect to an access concentrator. If the connection does not work for any reason, the unit continues its restart cycle, then retries to connect to an access concentrator indefinitely.

If the connection is successful at the first attempt, the Mediatrix 2102 goes on with its usual restart cycle. If the connection is successful only after the restart cycle is done, the Mediatrix 2102 restarts upon connecting because it does not support dynamic IP address change.

PPP Connection Loss

A network connection may abruptly shutdown for many reasons. One of the most common reasons is the maintenance of the network and its environment.

When the Mediatrix 2102 detects it has lost the PPP connection, it tries to re-establish the connection as in "Establishing a Connection" on page 102.

It is possible that the IP address assigned by the access concentrator changes after re-establishing a connection. In this case, the Mediatrix 2102 restarts because it does not support dynamic IP address change.

Routing Mechanism

Usually, the packets go through the Mediatrix 2102.

If the PC wants to directly contact the Mediatrix 2102, it must use the unit's LAN address (*localHostAddress* variable if TAS is disabled or *lanStaticAddress* if TAS is enabled).

Blocked Ports

The Mediatrix 2102 uses some ports for signalling, media transport and management purposes. Packets sent to these ports are blocked. Most of the ports can be configured by using a MIB variable.

Table 67: Blocked Ports

Port Description	Port Number	Configurable
SNMP	161 UDP	Yes
DHCP offer listening	68 UDP	No
TFTP server for configuration downloads. **Note**: This port is used only if the configuration download service is enabled, and only for the time it is required.	69 UDP	No
SIP	5060 UDP/ TCP	Yes
RTP/RTCP **Note**: The Mediatrix 2102 uses up to four UDP ports per FXS interface. See "RTP/RTCP Base Port Range" on page 100 for details.	5004+ UDP	Yes
T.38 **Note**: The Mediatrix 2102 uses one UDP port per FXS interface. See "T.38 Base Port Range" on page 99 for details.	6001+ UDP	Yes

Using the Mediatrix 2102 with a Low Bandwidth Connection

You can use the Mediatrix 2102 with a low bandwidth connection without any visible performance issues. This is true for both DHCP and PPPoE connections, with either a DSL or cable modem. However, you must configure the Mediatrix 2102 accordingly.

What is Considered a Low Bandwidth Connection?

Mediatrix considers that when the transmission of one or more large Ethernet packet takes more time than the time it takes for packetization, the process is not optimal. For instance, a 1518 bytes packet takes the following transmission time according to the bandwidth:

Table 68: Transmission Time vs. Bandwidth

Bandwidth (kbps)	Transmission Time (ms)
64	190
128	95
256	47
512	24
1024	12
2048	6
4096	3

One can see that from 128 kbps or less, the delay becomes significant, considering this is for one packet only. Mediatrix thus recommends to follow the configuration in the next section for a bandwith lower than 4096 kbps. This will ensure the best voice quality possible.

Configuration for a Low Bandwidth Connection

The following steps should allow you to use a low bandwidth connection.

▶ **To use the Mediatrix 2102 with a low bandwidth connection:**

1. Configure the “Bandwidth Management” feature as described in “WAN Upstream Bandwidth Control” on page 97.

   a. Set the maximum bandwidth in kilobits per seconds (kbps) in the *ipRoutingWanUpstreamBandwidth* variable.

   This value should be implemented or provided by your ISP. It must be between 64 kbps and 4096 kpbs.

   b. Enable the “Bandwidth Management” feature by setting the *ipRoutingBandwidthControlEnable* variable to **enable**.

2. Configure the Mediatrix 2102 in TAS mode as described in this chapter. Enable the TAS mode by setting the *ipRoutingEnable* variable to **enable**. See “Enabling TAS” on page 98 for more details.

3. In the *qosIeee8021q* group of the *qosMIB*, define a 802.1q priority for the voice and fax packets in the following variables.

   - *qosVoiceIeee8021qUserPriority* for voice priority
   - *qosT38FaxIeee8021qUserPriority* for fax priority

   The Mediatrix 2102 application uses 9 output queues with increasing priorities. The lowest priority queue is always used for the traffic coming from the LAN port and routed to the WAN port. You cannot change this priority level. The 8 other queues are used for the traffic the Mediatrix 2102 sends. By default, the lowest priority queue (of these 8 queues) is used for all traffic, and the other 7 are unused.

However, you can assign certain types of traffic to other queues of higher priority by configuring a 802.1q priority. It is not required to activate the packet tagging feature, only provide a priority to the protocol.

A good practice would be to always have a priority other than “0” for the voice and the fax. The signalling could also receive a higher priority. Thus, the SNMP and HTTP accesses performed from the WAN would be answered in lower priority.

See “IEEE 802.1q” on page 229 for more details on 802.1q priorities.

4. Set the value of the follolwing variables to **enable**:

- qosVoiceIeee8021qEnable
- qosT38FaxIeee8021qEnable

The corresponding user priority configuration is enabled.

5. Restart the Mediatrix 2102 so that the changes may take effect.

CHAPTER

9

Configuration File Download

The configuration file download feature allows to update the Mediatrix 2102 configuration by transferring a configuration file via TFTP or HTTP. The configuration file can either be transferred from the management server or from the configuration file download server. The main difference is the session initiator, which is respectively the management server and the Mediatrix 2102. The advantage of having the Mediatrix 2102 as the session initiator is to allow NAT traversal.

You can also manually upload a configuration file to the Mediatrix 2102 by using the web interface. See “Configuration File Upload Page” on page 32 for more details.

Configuration File Download Server

The service allows to download a unique file for each Mediatrix 2102, and/or a file shared among many units. These configuration files may be encrypted or not.

You have the choice to perform the configuration file download by using the TFTP protocol or the HTTP protocol. You can also configure the Mediatrix 2102 to automatically update its configuration.

To download a configuration file, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- SNTP server properly configured
- HTTP server with proper root path
- Configuration source
- Configuration file name and location

Configuring the TFTP Server

If you are to perform a configuration file download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server’s documentation.

Configuring the SNTP Server

If you are to use the automatic configuration file update feature (see “Automatic Configuration Update” on page 115 for more details), you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server’s documentation. You can also refer to “Chapter 17 - SNTP Settings” on page 183 for more details on how to configure the Mediatrix 2102 for a SNTP server.

Configuring the HTTP Server

If you are to perform a configuration file download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. It is assumed that you know how to set the root path. If not, refer to your HTTP server’s documentation.

Configuration File Server Settings

The Mediatrix 2102 must know the IP address and port number of its configuration file server. This server contains the configuration file the Mediatrix 2102 will download. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself in static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See "Chapter 4 - IP Address and Network Configuration" on page 51 for more details.

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

1. In the *ipAddressConfig* folder, locate the *configFileFetchingSelectConfigSource* variable (under the *ipAddressConfigFileFetching* group).

This variable defines whether the Mediatrix 2102 must ask for its configuration file server settings through a DHCP server or not.

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

You can query the configuration file server's IP address and port number assigned by the DHCP server in the following read-only variables (in the *ipAddressStatus* folder):

- configFileFetchingHost
- configFileFetchingPort

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

Table 69: Configuration File Server DHCP Information

To use a...	Set...
vendor specific code	The *configFileFetchingDhcpSiteSpecificCode* variable to **0**. Set the configuration file server IP address in the DHCP server inside the vendor specific sub-option 201 (hexadecimal 0xD2).
site specific code	The *configFileFetchingDhcpSiteSpecificCode* variable to any value between 128 and 254. Set the configuration file server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *configFileFetchingDhcpSiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 64 for more details.

Static Configuration

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

▶ **To use static information:**

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

This variable defines whether the Mediatrix 2102 must ask for its configuration file server settings through a DHCP server or not.

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

3. Set the following variables:

Table 70: Configuration File Server Static Information

Variable	Description
configFileFetchingStaticHost	Static configuration file server IP address or domain name to use when downloading a configuration file. This is the current address of the PC that hosts the configuration files. **Default Value**: 192.168.0.10
configFileFetchingStaticPort	Static configuration file server IP port number to use when downloading a configuration file. **Default Value**: 69

The default port value complies to RFC 1340 on the well-known ports (assigned numbers). This value applies to a TFTP server. It may be different for other servers. If you are using an HTTP server to perform the configuration file download, you must change the port value to 80.

Setting up the Configuration File Download

When performing a configuration file download, you can download two different files:

- A generic configuration file that should be used to update a large number of units with the same configuration.
- A specific configuration file that contains the configuration for a single unit, for instance the telephone numbers of its lines.

When both the generic and specific configuration files are downloaded, settings from the specific configuration file always override the settings from the generic configuration file. These files must be located in the same directory.

▶ **To setup the configuration file download:**

1. In the *configFileFetchingMIB*, set the *configFileFetchingFileLocation* variable with the path, on the remote server, of the directory where the configuration files are located.

The path is case sensitive hence it must be entered properly.

The path is relative to the root path of the transfer server (*configFileFetchingHost*). Use the “/” character when defining the path to indicate sub-directories.

Let’s consider the following example:

- The directory that contains the configuration file is called: **Config_File**.
- This directory is under **C:/Root/Download**.

Table 71: Path Configurations Example

TFTP/HTTP Root Path	Corresponding Path Name
c:/root/download	Config_File
c:/	root/download/Config_File
c:/root	download/Config_File

The following are some tips to help your download process:

- If available, use the *Browse* button (or equivalent) of the TFTP/HTTP server to select the directory, eliminating typographical errors.
- Use the “/” character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, use the “\” character.

- Use basic directory names, without spaces or special characters such as “~”, “@”, etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the image path of the Mediatrix 2102 (you may have to convert “\” into “/”) to eliminate typographical errors.

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

2. Set the *configFileFetchingFileName* variable with the name of the generic configuration file to download.

The file name is case sensitive hence it must be entered properly.

This file should be used to update a large number of units with the same configuration.

If you leave the variable empty, the Mediatrix 2102 does not download the generic configuration file.

3. Set the *configFileFetchingSpecificFileName* variable with the name of the specific configuration file to download.

The file name is case sensitive hence it must be entered properly.

This file should be used to update the configuration of a single unit.

This variable may contain macros that are substituted by actual values when downloading the configuration file. Supported macros are:

- %mac%: the MAC address of the unit
- %%: the character “%”

For instance:

- The “%mac%.xml” value for a Mediatrix 2102 with MAC address “0090F12345AB” will be “0090F12345AB.xml”.
- The value “Hello%%Hi” will result in “Hello%Hi”.
- The value “%%%mac%%%mac%.xml” will result in “%0090F12345AB%mac%.xml”.

  From left to right: the first macro encountered is first substituted, the second macro encountered is then substituted, etc.

When the character “%” is not part of a macro, it is not replaced. The following are examples:

- The value “%mac.xml” stays “%mac.xml”
- The value “Hello%Hi” stays “Hello%Hi”
- The value “%moc%.xml” stays “%moc%.xml”

If the variable is empty (after macro substitution), the Mediatrix 2102 does not download the specific configuration file.

Configuration Update Status

If valid configuration files are successfully downloaded, then the Mediatrix 2102 automatically restarts to apply all the new settings. If the Mediatrix 2102 does not restart, this could mean the download failed or that the configuration in the file is the same as the configuration in the unit.

You can validate the status of the configuration update in various ways.

MIB Variable

You can query the status of the last configuration file download in the *sysAdminDownloadConfigFileStatus* variable:

- idle: No configuration file download has been performed yet.
- fail: The last configuration file download failed.
- success: The last configuration file download succeeded.
- inProgress: A configuration file download is in progress.
- listening: The unit is listening and waiting for a configuration file to be sent by the management server.

Syslog Messages

A lot of information is transmitted as system log (syslog) messages. The following are some of the syslog messages sent by the unit:

Table 72: Configuration File Download Syslog Messages

Level	Message	Event
Informational	`The specific configuration update succeeded.`	The configuration update with the specific configuration file has been successful.
Error	`The specific configuration update failed.`	The configuration update with the specific configuration file experienced an error and has not been completed.
Informational	`The configuration file "XXX" was successfully fetched.`	A configuration file was successfully fetched.
Informational	`The unit configuration is not updated. The parameter values defined in the fetched configuration files are identical to the actual unit configuration.`	The parameter values defined in the fetched configuration files are identical to the actual unit configuration.
Informational	`The generic file \"%s\" parameter values are not applied. They are either identical to the unit configuration or overwritten by the specific file.`	The generic configuration file parameter values are either identical to the unit configuration or overwritten by the specific configuration file.
Warning	`None of the parameter values defined in the configuration file \"%s\" was successfully applied.`	No parameter value from a fetched configuration file was successfully applied (e.g., because of bad OIDs).
Informational	`Parameter values defined in the configuration file \"%s\" were successfully applied.`	A fetched configuration file was successfully applied.
Informational	`The unit is restarting to complete the configuration update.`	All necessary fetched configuration files were successfully applied.

You can view these messages in the web interface. See "System Log Page" on page 34 for more details.

Configuration Files Encryption

You can secure the exchange of configuration files between the server and the Mediatrix 2102. A privacy key allows the unit to decrypt a previously encrypted configuration file. This applies to files downloaded via TFTP or HTTP, but NOT on updates performed from the web interface.

To encrypt a configuration file (generic or specific), you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts files before sending them to the Mediatrix 2102 unit. Contact yoyr sales representative for more details.

Configuration File Decryption on the Mediatrix 2102

The following describes how to decrypt a previously encrypted generic or specific configuration file. You must have one key for the generic configuration file and another key for the specific configuration file.

▶ **To decrypt a configuration file:**

1. In the *configFileFetchingMIB,* set the proper decryption variable with the secret key used to decrypt the configuration file.

Table 73: Decryption Variables

Configuration File	Variable
Generic	configFilePrivacyGenericSecret
Specific	configFilePrivacySpecificSecret

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F. All other characters are not supported.

Each character encodes 4 bits of the key. For instance, a 32-bit key requires 8 characters.

- If you enter too many bits, the key is truncated to the first 448 bits.
- If you do not enter enough bits, the key is padded with zeros.

For instance, a 32-bit key could look like the following: A36CB299.

This key must match the key used for the encryption of the relevant configuration file.

If the variable is empty, the configuration file is not decrypted.

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

The Mediatrix 2102 will be able to decrypt the next encrypted generic or specific configuration file. If this variable is set to **disable**, the configuration file is not decrypted by the unit and the configuration update fails.

Configuration Download via TFTP

The following steps explain how to download configuration files by using the TFTP protocol.

☞ **Note:** The configuration download via TFTP can only traverse NATs of types “Full Cone” or “Restricted Cone”. If the NAT you are using is of type “Port Restricted Cone” or “Symmetric”, the file transfer will not work.

▶ **To download configuration files via TFTP:**

1. Set the configuration file server host and port as defined in “Configuration File Server Settings” on page 108.
2. Place the configuration files to download on the computer hosting the TFTP server.

   These files must be in a directory under the TFTP root path.
3. If not already done, set the configuration file path as described in “Setting up the Configuration File Download” on page 109.
4. In the *configFileFetchingMIB,* set the *configFileTransferProtocol* variable to **tftp**.
5. In the *groupAdminMIB*, set the *groupSetAdmin* variable to **ForceLock**.

   All activities in progress on the Mediatrix 2102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is “locked”). The configuration file download may take place.
6. In the *sysAdminMIB*, initiate the configuration file download via TFTP by setting the *sysConfigCommand* variable to **updateConfiguration**.

   The Mediatrix 2102 immediately downloads the configuration files. It is the initiator of the TFTP sessions.

NAT Variations

NAT treatment of UDP varies among implementations. The four treatments are:

- Full Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.
- Restricted Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.
- Port Restricted Cone: Similar to a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.
- Symmetric: All requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

For more details on NAT treatments, refer to RFC 3489.

Configuration Download via HTTP

The following steps explain how to download the configuration files by using the HTTP protocol.

▶ **To download the configuration files via HTTP:**

1. Set the configuration file server host and port as defined in "Configuration File Server Settings" on page 108.

> ⚠ **Caution:** When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).
>
> If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See "Configuration File Server Settings" on page 108 for more details.

2. Place the configuration files to download on the computer hosting the HTTP server.

   These files must be in a directory under the root path.

3. If not already done, set the configuration file path as described in "Setting up the Configuration File Download" on page 109.

4. In the *configFileFetchingMIB,* set the *configFileTransferProtocol* variable to **http**.

   Your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.

5. If your HTTP server requires authentication when downloading the configuration file, set the following:
   - The user name in the *configFileTransferUsername* variable.
   - The password in the *configFileTransferPassword* variable.

6. In the *groupAdminMIB*, set the *groupSetAdmin* variable to **ForceLock**.

   All activities in progress on the Mediatrix 2102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is "locked"). The configuration file download may take place.

7. In the *sysAdminMIB*, initiate the configuration file download via HTTP by setting the *sysConfigCommand* variable to **updateConfiguration**.

   The Mediatrix 2102 immediately downloads the configuration files. It is the initiator of the HTTP sessions.

Automatic Configuration Update

You can configure the Mediatrix 2102 to automatically update its configuration. This update can be done:

- Every time the Mediatrix 2102 restarts.
- At a specific time interval you can define.

Automatic Update on Restart

The Mediatrix 2102 may download new configuration files each time it restarts.

▶ To set the automatic update every time the Mediatrix 2102 restarts:

1. Set the configuration file server host and port as defined in "Configuration File Server Settings" on page 108.

Caution: When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).

If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See "Configuration File Server Settings" on page 108 for more details.

2. Place the configuration files to download on the computer hosting the HTTP or TFTP server.

   These files must be in a directory under the root path.

3. If not already done, set the configuration file path as described in "Setting up the Configuration File Download" on page 109.

4. In the *configFileFetchingMIB,* set the *configFileTransferProtocol* variable to either **http** or **tftp**.

   If you are using the HTTP protocol to download the configuration, be aware that your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.

5. If you are using the HTTP protocol to download the configuration and your HTTP server requires authentication, set the following:

   - The user name in the *configFileTransferUsername* variable.
   - The password in the *configFileTransferPassword* variable.

   The Mediatrix 2102 supports basic and digest HTTP authentication, as described in RFC 2617.

6. Set the *configFileAutoUpdateOnRestartEnable* variable to **enable** (in the *configFileAutomaticUpdate* group).

7. In the *sysConfigMIB*, set the *sysConfigDownloadConfigFile* variable to **automaticInitiateFileDownload**.

   The automatic configuration update will be performed each time the Mediatrix 2102 restarts.

   The unit configuration is only updated if at least one parameter value defined in the downloaded configuration files is different from the actual unit configuration.

Automatic Update at a Specific Time Interval

You can configure the Mediatrix 2102 to download new configuration files at a specific day and/or time.

▶ **To set the automatic update at a specific time interval:**

1. Set the configuration file server host and port as defined in "Configuration File Server Settings" on page 108.

> **Caution:** When downloading via HTTP, the configuration file server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).
>
> If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See "Configuration File Server Settings" on page 108 for more details.

2. Place the configuration files to download on the computer hosting the HTTP or TFTP server.

   These files must be in a directory under the root path.

3. If not already done, set the configuration file path as described in "Setting up the Configuration File Download" on page 109.

4. In the *configFileFetchingMIB,* set the *configFileTransferProtocol* variable to either **http** or **tftp**.

   If you are using the HTTP protocol to download the configuration, be aware that your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.

5. If you are using the HTTP protocol to download the configuration and your HTTP server requires authentication, set the following:
   - The user name in the *configFileTransferUsername* variable.
   - The password in the *configFileTransferPassword* variable.

   The Mediatrix 2102 supports basic and digest HTTP authentication, as described in RFC 2617.

6. Define the time base for automatic configuration updates in the *configFileAutoUpdateTimeUnit* variable (in the *configFileAutomaticUpdate* group).

   You have the following choices:

Table 74: Time Unit Parameters

Parameter	Description
seconds	Updates the unit's configuration every *x* seconds. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7).
minutes	Updates the unit's configuration every *x* minutes. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7).
hours	Updates the unit's configuration every *x* hours. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7).
days	Updates the unit's configuration every *x* days. You can specify the *x* value in the variable *configFileAutoUpdatePeriod* (see Step 7). You can also define the time of day when to perform the update in the *configFileAutoUpdateTimeOfDay* variable (see Step 8).

7. Set the waiting period between each configuration update in the *configFileAutoUpdatePeriod* variable.

   The time unit for the period is specified by the *configFileAutoUpdateTimeUnit* variable (see Step 6). Available values are from 1 to 48.

   It may be possible that the Mediatrix 2102 skips a scheduled periodic update if the previous periodic update has not finished yet. This may happen with periods of a few seconds.

Let’s say for instance that you set the period to two seconds and the automatic update mechanism takes five seconds to complete. The following describes the behaviour:

Table 75: Scheduled Periodic Update

Time (s)	Description
0	Beginning of the automatic update mechanism.
2	Automatic update. The file transfer starts.
4	Automatic update. The Mediatrix 2102 skips this scheduled update because the previous update has not finished yet.
6	Automatic update. The Mediatrix 2102 skips this scheduled update because the previous update has not finished yet.
7	The file transfer is finished and the configuration file is applied.
8	Automatic update. The file transfer starts.

8. If you have selected **days** in Step 6, set the time of the day when to initiate a configuration update in the *configFileAutoUpdateTimeOfDay* variable.

The time of the day is based on the *sntpTimeZoneString* variable setting (see “Chapter 17 - SNTP Settings” on page 183 for more details).

You must have a time server SNTP that is accessible and properly configured, or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server’s documentation. You can also refer to “Chapter 17 - SNTP Settings” on page 183 for more details on how to configure the Mediatrix 2102 for a SNTP server.

The configuration files are downloaded at the first occurrence of this value and thereafter at the period defined by the *configFileAutoUpdatePeriod* variable. Let’s say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the automatic update is enabled after 14h00, the first update will take place the day after at 14h00, then the second download two days later at the same hour, and so on.

Available values are -1, and from 0 to 23.

Setting the variable to **-1** means that the time of the day at which the Mediatrix 2102 first downloads the configuration files is randomly selected.

9. Set the *configFileAutoUpdatePeriodicEnable* variable to **enable**.

10. In the *sysConfigMIB*, set the *sysConfigDownloadConfigFile* variable to **automaticInitiateFileDownload**.

The unit configuration is only updated if at least one parameter value defined in the downloaded configuration files is different from the actual unit configuration.

If one of the telephones/faxes is off-hook, the Mediatrix 2102 will perform the update 5 minutes after both ports are detected on-hook.

Error Handling

The following configuration file fetching service error sources are divided in three types depending on the transfer protocol: common errors (Table 35), TFTP errors (Table 36) and HTTP errors (Table 37). The error cause and the unit behaviour are also described.

Table 76: Configuration File Fetching Error Handling

Error Type	Cause	Behaviour
Common Error Handling		
Invalid file format	The file format is not valid.	Send a syslog **warning** message including the file location/name with the transfer server address: `The fetched configuration file “XXX”, from server “XXX”, has an invalid format.` No recorded settings applied.
Empty file	Committing an empty file.	Send a syslog **warning** message including the file location/name with the transfer server address: `The fetched configuration file “XXX”, from server “XXX”, is empty.`
Invalid file content	The file contains invalid characters. Allowed characters are ASCII codes 10 (LF), 13(CR), 32 to 126 and 191 to 255.	Send a syslog **warning** message including the file location/name, the transfer server address and the invalid character (ASCII code): `The fetched configuration file “XXX”, from server “XXX”, has an invalid character “ASCII code XXX”.` No recorded settings applied.
Invalid transfer server address	The server address is not valid.	Send a syslog **warning** message including the transfer server address: `No configuration file is fetched because the server host “XXX” is invalid.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
File size too big	Downloading a file with a size exceeding 512000 bytes.	Send a syslog **warning** message including the file location/name, the transfer server address, the file size and the maximum allowed size: `The fetched configuration file “XXX”, from server “XXX”, has a size “XXX bytes” that exceeds the maximum allowed size “XXX bytes”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Invalid encryption	The configuration file cannot be decrypted. A badly encrypted file is detected if the header or the padding is invalid.	Send a syslog **warning** message including the file location/name and the transfer server address: `The fetched configuration file \”%s\”, from server \”%s\”, can not be decrypted.`

Table 76: Configuration File Fetching Error Handling (Continued)

Error Type	Cause	Behaviour
TFTP-Specific Error Handling		
File not found	Received error code 1 (file not found) from the TFTP server.	Send a syslog **warning** message including the file name and location with the TFTP server address: `The configuration file “XXX” was not found on the TFTP server “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Access violation	Received error code 2 (access violation) from the TFTP server.	Send a syslog **warning** message including the file name and location with the TFTP server address: `The configuration file “XXX” was not fetched. There was a TFTP access violation with server “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Connection timeout	No answer from the TFTP server. The time elapsed since the TFTP request was sent exceeds 32 seconds.	Send a syslog **warning** message including the file name and location with the TFTP server address: `The configuration file “XXX” was not fetched. The TFTP connection with server “XXX” timed out.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Transfer error	Received a TFTP error (other than error code 1 and 2) from the TFTP server.	Send a syslog **warning** message including the file name and location with the TFTP server address: `Error in the TFTP transfer of the configuration file “XXX” from host “XXX” and port number XXX.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
File size too big	Downloading a file with a size exceeding 512000 bytes.	Abort the transfer by sending error code 3 (disk full or allocation exceeded) to the TFTP client.
HTTP-Specific Error Handling		
Access unauthorized	Received a 401 Unauthorized from the HTTP server.	Send a syslog **warning** message including the file location/name with the HTTP server address: `The access to configuration file “XXX” is unauthorized on HTTP server “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
File not found	Received a 404 Not Found from the HTTP server.	Send a syslog **warning** message including the file location/name with the HTTP server address: `The configuration file “XXX” was not found on the HTTP server “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.

Table 76: Configuration File Fetching Error Handling (Continued)

Error Type	Cause	Behaviour
Session timeout	No answer from the HTTP server. The time elapsed since the HTTP request was sent exceeds 15 seconds.	Send a syslog **warning** message including the file location/name with the HTTP server address: `The configuration file “XXX” was not fetched. The HTTP session with server “XXX” timed out.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Session closed by peer	The HTTP server closed the session.	Send a syslog **warning** message including the file location/name with the HTTP server address: `The configuration file “XXX” HTTP transfer session was closed by peer: host “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail*.
Transfer error	Received an HTTP error (other than 401 and 404) from the HTTP server.	Send a syslog **warning** message including the file location/name with the HTTP server address and port: `Error in the HTTP transfer of the configuration file “XXX” from host “XXX” and port number XXX.` Set *sysAdminDownloadConfigFileStatus* to *fail*.

Management Server

You can set the Mediatrix 2102 so that it asks the management server to send it a configuration file.

> **Note:** Downloading a configuration file from the management server can only be performed through the TFTP protocol.

Management Server Configuration

To download a configuration file from the management server, you must setup the management server information as per “Chapter 23 - Management Server Configuration” on page 225.

Downloading from the Management Server

Once the management server has been properly set up, you can define the configuration file download.

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

▶ **To download the configuration file from the management server:**

1. Place the configuration file on the computer hosting the management server.
2. In the *sysConfigMIB*, request a configuration file download by setting the *sysConfigDownloadConfigFile* variable to **requestFileDownload**.
3. Set the *sysConfigDownloadConfigMode* variable to **request**.

   The Mediatrix 2102 sends a notification, *msTrapConfigInformation,* to the management server, via SNMP traps, to request the configuration file.

   The management server then initiates the TFTP session and pushes the file into the unit.

   If the management server is the Unit Manager Network from Mediatrix, the following steps are automatically performed. If you are using another management server, you may have to perform them manually.

   a. The Unit Manager Network sets the *sysConfigDownloadConfigMode* variable to **record**.

   b. The Unit Manager Network sends the configuration file to the Mediatrix 2102.

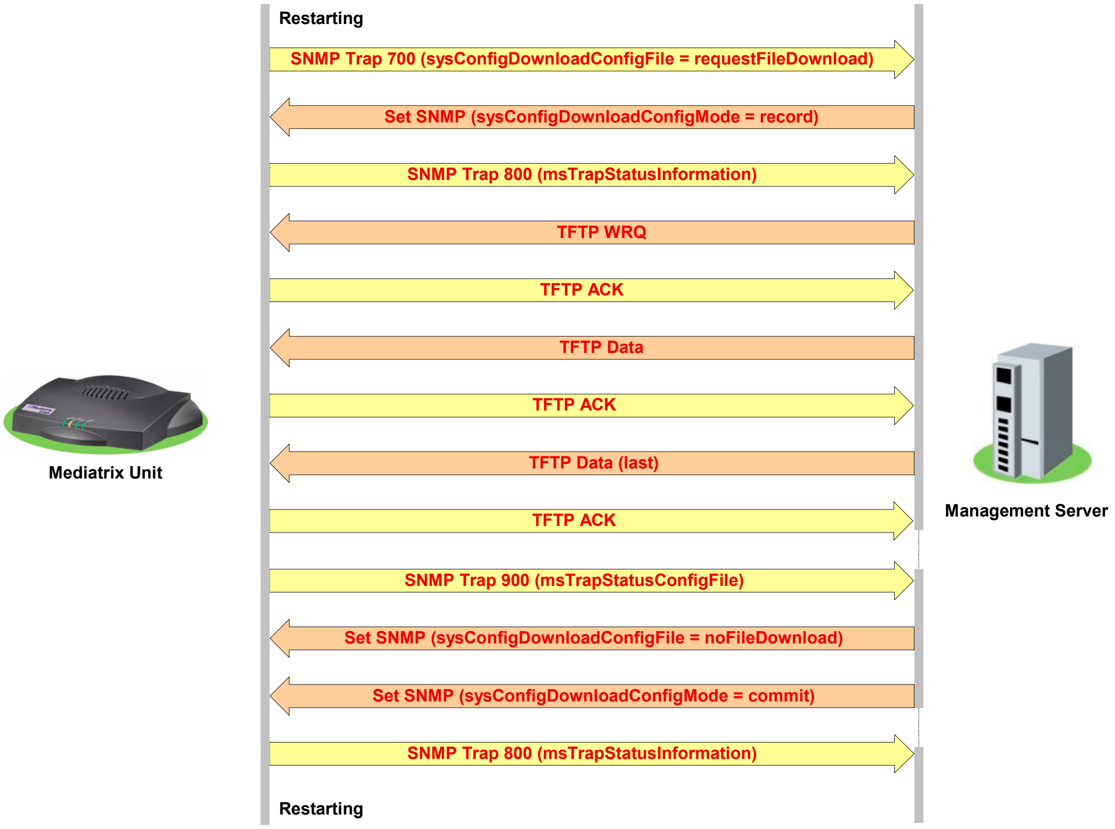
   c. Once the configuration file has been sent, the Unit Manager Network sets the *sysConfigDownloadConfigFile* variable to **noFileDownload**.

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

   If a valid configuration file is successfully downloaded, then the Mediatrix 2102 automatically restarts to apply all the new settings. If the Mediatrix 2102 does not restart, this could mean the download failed. In this case, you can query the status of the last configuration file download in the *sysAdminDownloadConfigFileStatus* variable:

   - idle: No configuration file download has been performed yet.
   - fail: The last configuration file download failed.
   - success: The last configuration file download succeeded.
   - inProgress: A configuration file download is in progress.
   - listening: The unit is listening and waiting for a configuration file to be sent by the management server.

Figure 34: Configuration Sequence Update Using the Management Server


Restarting
SNMP Trap 700 (sysConfigDownloadConfigFile = requestFileDownload)
Set SNMP (sysConfigDownloadConfigMode = record)
SNMP Trap 800 (msTrapStatusInformation)
TFTP WRQ
TFTP ACK
TFTP Data
TFTP ACK
TFTP Data (last)
TFTP ACK
SNMP Trap 900 (msTrapStatusConfigFile)
Set SNMP (sysConfigDownloadConfigFile = noFileDownload)
Set SNMP (sysConfigDownloadConfigMode = commit)
SNMP Trap 800 (msTrapStatusInformation)
Restarting
Mediatrix Unit
Management Server

Error Handling

The following are possible error sources when updating the unit configuration using the management server. The error cause and the unit behaviour are also described.

Table 77: Configuration File Error Handling with the Management Server

Error Type	Cause	Behaviour
Empty file	Committing an empty file.	Send a syslog **warning** message including the file name and the TFTP client address: `The configuration file "XXX" pushed to the unit by the TFTP client "XXX" is empty.`
Invalid file content	Committing a file that contains invalid characters. Allowed characters are ASCII codes 10 (LF), 13(CR), 32 to 126 and 191 to 255.	Send a syslog **warning** message including the file name, the TFTP client address and the invalid character (ASCII code): `The configuration file "XXX" pushed to the unit by the TFTP client "XXX" has an invalid character "ASCII code XXX".` No recorded settings applied.
Invalid file format	Committing a file with an invalid format.	Send a syslog **warning** message including the file name and the TFTP client address: `The configuration file "XXX" pushed to the unit by the TFTP client "XXX" has an invalid format.` No recorded settings applied.

Table 77: Configuration File Error Handling with the Management Server (Continued)

Error Type	Cause	Behaviour
File size too big	Downloading a file with a size exceeding 512000 bytes.	Send a syslog **warning** message including the file name, the TFTP client address, the file size and the maximum allowed size: `The configuration file “XXX” from the TFTP client “XXX” is not downloaded because its size “XXX bytes” exceeds the maximum allowed size “XXX bytes”.` Send error code 3 (disk full or allocation exceeded) to the TFTP client. Set *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
TFTP transfer error	Received a TFTP error from the TFTP client.	Send a syslog **warning** message including the file name and the TFTP client address: `Error in the TFTP transfer of the configuration file “XXX” from the TFTP client “XXX”.` Set *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
TFTP transfer aborted	The transfer was aborted while in progress by changing the value of *sysConfigDownload ConfigMode* or *sysConfigDownloadConfigFile*.	Send a syslog warning message including the file name and the TFTP client address: `The TFTP transfer of the configuration file “XXX” from the TFTP client “XXX” was aborted.` Set *sysAdminDownloadConfigFileStatus* to *fail* and send *msTrapStatusConfigFile*.
File pulling not allowed	A TFTP client is trying to read a file from the unit.	Send a syslog informational message including the file name and the TFTP client address: `The TFTP client “XXX” is trying to pull the file “XXX” from the unit. This is not allowed.` Send error code 2 (access violation) to the TFTP client.

Syslog Messages

A syslog message is sent whenever it is impossible for the management server to download a configuration file or when it is impossible to apply the new settings to the unit.

Table 78: Syslog Messages Using the Management Server

Level	Message	Event
Warning	`The notification “XXX” could not be sent to msHost “XXX” and msTrapPort XXX.`	A SNMP trap could not be sent to the management server. The syslog warning message includes the SNMP trap number, the management server address and port.
Informational	`Parameter values defined in the configuration file were successfuly committed. Restarting the unit...`	A downloaded configuration file was successfully committed.
Warning	`None of the parameter values defined in the configuration file was successfully committed.`	No parameter value from the downloaded configuration file was successfully applied (e.g., because of bad OIDs).

Configuration File Example

The configuration file format uses XML (eXtensible Markup Language). The following is the accepted format:

```
<MX_Config_File FileId="MX_MIBFILE" MIBVersionNumber="" VersionNumber="1.0">
   <Object Prefix="" Suffix="" Value=""/>
   <Object Prefix="" Suffix="" Value=""/>
</MX_Config_File>
```

The following is an example of a configuration file:

```
<MX_Config_File FileId="MX_MIBFILE" MIBVersionNumber="1.0" VersionNumber="1.0">
   <Object Prefix="1.3.6.1.4.1.4935.15.1.8.1" Suffix="0" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.1.10.1" Suffix="0" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.1.10.10.1" Suffix="0" Value="192.168.0.10"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.1.20.1" Suffix="0" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.3.1.30.1" Suffix="0" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.3.1.30.3" Suffix="0" Value="ConfigFile.xml"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.15.1.5" Suffix="0" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.35.1.20.1.1" Suffix="3" Value="0"/>
   <Object Prefix="1.3.6.1.4.1.4935.15.35.1.20.1.1" Suffix="4" Value="0"/>
</MX_Config_File>
```

Note: When creating and/or editing a configuration file, the following ASCII codes are supported:

- 10 (LF)
- 13(CR)
- 32 to 126

All other ASCII codes will result in an invalid configuration file.

CHAPTER
10

Software Download

This chapter describes how to download a software version available on the designated software server into the Mediatrix 2102.

You have the choice to perform the software download by using the TFTP protocol or the HTTP protocol. You can also configure the Mediatrix 2102 to automatically update its software version.

Note: You can only perform a software download from the WAN interface of the Mediatrix 2102. Software downloads from the LAN side are not supported.

Before Downloading

To download a software, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- MIB browser (with the current Mediatrix 2102 MIB tree)

  You can use the MIB browser built in the Mediatrix's Unit Manager Network. See "Unit Manager Network – Element Management System" on page xxv for more details.
- Software upgrade zip file
- SNTP server properly configured
- HTTP server with proper root path
- Syslog daemon (optional)

Configuring the TFTP Server

If you are to perform a software download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server. This PC must not have a firewall running. Mediatrix also recommends to place the PC and the Mediatrix 2102 in the same subnet.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

If you are to use the automatic software update feature (see "Automatic Software Update" on page 134 for more details), you must have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to "Chapter 17 - SNTP Settings" on page 183 for more details on how to configure the Mediatrix 2102 for a SNTP server.

Configuring the HTTP Server

If you are to perform a software download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. This PC must not have a firewall running. Mediatrix also recommends to place the PC and the Mediatrix 2102 in the same subnet.

It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Software Servers Configuration

The Mediatrix 2102 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 2102 through a DHCP server or manually enter them yourself in static variables.

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

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.

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

1. In the *ipAddressConfig* folder, locate the *imageSelectConfigSource* variable (under the *ipAddressConfigImage* group).

This variable defines whether the Mediatrix 2102 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 79: Primary Image Server DHCP Information

To use a...	Set...
vendor specific code	The *imageDhcpPrimarySiteSpecificCode* variable to **0**. Set the Primary image server IP address in the DHCP server inside the vendor specific sub-option 117 (hexadecimal 0x75).
site specific code	The *imageDhcpPrimarySiteSpecificCode* variable to any value between 128 and 254. Set the Primary image server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *imageDhcpPrimarySiteSpecificCode* variable in the unit’s configuration).

See “Vendor and Site Specific DHCP Options” on page 64 for more details.

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

Table 80: Secondary Image Server DHCP Information

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

Table 80: Secondary Image Server DHCP Information (Continued)

To use a...	Set...
site specific code	The *imageDhcpSecondarySiteSpecificCode* variable to any value between 128 and 254. Set the Secondary image server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *imageDhcpPrimarySiteSpecificCode* variable in the unit's configuration).

See "Vendor and Site Specific DHCP Options" on page 64 for more details.

Static Configuration

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

▶ **To use static information:**

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

This variable defines whether the Mediatrix 2102 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 81: Image Static Information

Variable	Description
imageStaticPrimaryHost	Static primary image server IP address or domain name. This is the current address of the PC that hosts the files required for the download (extracted from the zip file). **Default Value**: 192.168.0.10
imageStaticPrimaryPort	Static primary image server IP port number. **Default Value**: 69
imageStaticSecondary Host	Static secondary image server IP address or domain name. This is the current address of the PC that hosts the files required for the download (extracted from the zip file). **Default Value**: 192.168.0.10
imageStaticSecondaryPort	Static secondary image server IP port number. **Default Value**: 69

The default port value complies to RFC 1340 on the well-known ports (assigned numbers). This value (69) applies to a TFTP server. It may be different for other servers. If you are using an HTTP server, you must change the port value to 80.

Download Procedure

The following describes how to download a software version into the Mediatrix 2102.

Note: Configuration settings are not lost when upgrading the software to a newer version. However, configuration settings may be lost if you upload an older firmware to the device. See "Software Downgrade" on page 137 for more details.

You have the choice to perform the software download by using the TFTP protocol or the HTTP protocol. You can also configure the Mediatrix 2102 to automatically update its software version.

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

Note: You can only perform a software download from the WAN interface of the Mediatrix 2102. Software downloads from the LAN side are not supported.

Extracting the Zip File

The zip file contains the software information required for the download.

Extract the contents of the zip file on the PC designated as the software file server. Be sure to use the defined folder name. This creates a directory that contains the files required for the Mediatrix 2102 to properly update its software.

The directory name must be the same as the name defined in the *imageLocation* or *imageSelectionFileLocation* variable of the *imageMIB*. See "Setting up the Image Path" on page 128 for more details.

Mediatrix suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

This directory must be located under the root path as defined in the TFTP/HTTP server or the software download will not proceed.

Setting up the Image Path

When performing a software download, you must configure the path, on the remote image server, of the directory where you extracted the files required for the download. This applies to both the manual or automatic download procedure, using the HTTP or TFTP protocol.

The directory must be located under the root path, as defined in the TFTP or HTTP server, or the software download will not proceed. See "Before Downloading" on page 125 for more details.

The Mediatrix 2102 first downloads a file called "setup.inf". This file contains the list of all the other files to download, depending on the product. The "setup.inf" file and all the other files must be in the same directory. If any of the files is missing, the procedure will not work properly.

▶ **To setup the Image path:**

1. In the *imageMIB*, select where to get the image location in the *imageLocationProvisionSource* variable.

   You have the following choices:

Table 82: Image Location Parameters

Parameter	Description
static	Uses the directory specified in the *imageLocation* variable (see Step 2).
remoteFile	The image location is defined in a file called "mediatrix2102targetimage.inf". The location of this file is defined in the *imageSelectionFileLocation* variable. This is useful if you are using automatic updates with multiple units (see Step 3).

2. If you have set the *imageLocationProvisionSource* variable to **static** (see Step 1), configure the path in the *imageLocation* variable.

   This is the location of the "setup.inf" file that contains the list of the files to download into the Mediatrix 2102. The "setup.inf" file and all the other files must be in the same directory. In other words, this is the path from the root TFTP/HTTP folder down to the files extracted from the zip file.

3. If you have set the *imageLocationProvisionSource* variable to **remoteFile** (see Step 1):

   a. Create a text file and write the path and/or name of the directory that contains the files required for download. Save this file as "mediatrix2102targetimage.inf" under the server root path.

Note: If you leave the file empty, the Mediatrix 2102 will look for the software download information in the root directory of the image server.

   b. Configure the path of the "mediatrix2102targetimage.inf" file in the *imageSelectionFileLocation* variable.

   Note that the selection file name is in lower case. Some web servers are case sensitive.

   This is useful if you are using automatic updates with multiple units. If you want the units to download a new version, you only have to change the path once in the "mediatrix2102targetimage.inf" file. If you were to use the *imageLocation* variable, you would have to change the path in every unit.

Let's consider the following example:

- The directory that contains the files required for download is called: **SIP_v5.0.1.1_MX-S5001-01**.
- This directory is under **C:/Root/Download**.

Table 83: Path Configurations Example

TFTP/HTTP Root Path	Corresponding Path Name
c:/root/download	SIP_v5.0.1.1_MX-S5001-01
c:/	root/download/SIP_v5.0.1.1_MX-S5001-01
c:/root	download/SIP_v5.0.1.1_MX-S5001-01

The following are some tips to help your download process:

- If available, use the *Browse* button (or equivalent) of the TFTP/HTTP server to select the directory, eliminating typographical errors.
- Use the "/" character when defining the path to indicate sub-directories. For instance, *root/download*.

  If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the "/" character and produce an error. In this case, use the "\" character.
- Use basic directory names, without spaces or special characters such as "~", "@", etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the image path of the Mediatrix 2102 (you may have to convert "\" into "/") to eliminate typographical errors.

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

Software Download Status

You can validate the status of the software download in various ways.

Syslog Messages

If you are using a Syslog daemon, you will receive messages that inform you of the software update status. The following are the syslog messages the Mediatrix 2102 sends:

Table 84: Software Update Syslog Messages

Level	Message	Event
General Messages		
Informational	`The software update succeeded.`	The software update has been successful.
Error	`The software update failed.`	The software update experienced an error and has not been completed.
Warning	`Primary image server not specified, cannot download file: xxx`	This error occurs when an image download is initiated and no domain name or address is specified for the primary image server.
Warning	`Secondary image server not specified, cannot download file: xxx.`	When a request involving the primary server fails, the secondary server is tried. This error occurs when there is no address or domain name specified for the secondary image server.
Error	`Cannot resolve address of image server: xxx.`	A DNS request failed to resolve the domain name of the image server (primary or secondary).
Error	`Target image at location: xxx from host: xxx is invalid or corrupted.`	For periodic and automatic updates, the target image to download is first compared with the installed image. This error occurs when this comparison failed because of corruption in the target image files.
Informational	`Image download transfer initiated.`	When manual, periodic or “at restart” image download is initiated.
Warning	`The file: xxx from host: xxx exceeds the size limit.`	The selection file or “setup.inf” file received exceeds 10000 bytes.
Informational	`Target image at location: xxx from host xxx is identical to currently installed image. Transfer aborted.`	For periodic and automatic updates, the target image to download is first compared with the installed image. This message occurs when this comparison determined that the target image is identical to the installed image.
HTTP-Specific Messages		
Warning	`HTTP image transfer of file: xxx from host: xxx was closed by peer.`	The HTTP transfer was closed by the peer.

Table 84: Software Update Syslog Messages (Continued)

Level	Message	Event
Warning	`HTTP image transfer of file: xxx from host: xxx was closed due to unsupported or malformed response from the host.`	In the HTTP response, one of the following error occurred: • The protocol version is not 1.0 or 1.1. • Some field or line is not properly formatted. • The trailing <crlf> is not present at the end of the header. • Unsupported kind of response.
Warning	`HTTP image transfer of file: xxx from host: xxx was refused because of a malformed or incompatible request.`	When receiving HTTP response #400 or #403.
Warning	`HTTP image transfer of file: xxx from host: xxx was refused because of a server error.`	When receiving HTTP response #500 or #501.
Warning	`HTTP image transfer of file: xxx from host: xxx was refused because service is unavailable.`	When receiving HTTP response #503.
TFTP-Specific Messages		
Warning	`Image transfer of file: xxx from host: xxx and port: xxx was closed due to unexpected error`	Unexpected error, either internal or on a TFTP or HTTP connection.
Warning	`Image transfer of file: xxx from host: xxx port: xxx was closed after timeout`	When not receiving TFTP packets for 32 seconds or not receiving a HTTP packet for 15 seconds.
Warning	`Image transfer. File: xxx not found on host: xxx`	When receiving TFTP error “NOT FOUND” or HTTP response #404.
Warning	`Image transfer. Access to file: xxx on host: xxx is unauthorized`	When receiving TFTP error “ACCESS” or HTTP response #401.

If the local syslog messages are enabled (see “Local Syslog” on page 236 for more details), you can view these messages on the web interface.

LED States

When the Mediatrix 2102 initiates a software download, the LEDs located on the front panel indicate the status of the process.

Table 85: LED States in Software Download

Event	LED State
Image downloading and writing	Each LED blinks alternately at 1 Hz with 1/4 ON duty cycle. **Warning**: Do not turn the Mediatrix 2102 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.

See “LED Indicators” on page 15 for a detailed description of the LED patterns related to the software download process.

MIB Variable

You can validate the result of the last software update by checking the state of the *sysAdminLastDownloadSoftware* MIB variable.

Download via TFTP

The following steps explain how to download a software by using the TFTP protocol.

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

▶ **To download a software via TFTP:**

1. If not already done, setup the Image server used to download the software (see “Before Downloading” on page 125).

2. Be sure that UDP ports 60000 to 60512 inclusively are opened in your firewall.

3. If not already done, configure the Image path as described in “Setting up the Image Path” on page 128.

4. If not already done, configure the image hosts and ports as defined in “Software Servers Configuration” on page 126.

5. Set the TFTP root path in your TFTP server.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server’s documentation.

6. Set the *imageTransferProtocol* variable to **tftp**.

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

All activities in progress on the Mediatrix 2102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is “locked”). The software upgrade may take place.

The Mediatrix 2102 lines will be unlocked after successfully downloading the software and restarting. If, for any reason, the software download is not successful, you must manually unlock the lines as per “Lines Administrative State” on page 139.

8. Initiate the download by setting the *sysAdminCommand* variable (in the *sysAdminMIB*) to **downloadSoftware**.

This starts the download process.

Caution: Never shutdown the Mediatrix 2102 manually while in the download process, because the image may be partially written and the Mediatrix 2102 is unable to restart.

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

If Transparent Address Sharing is enabled during the software download, the PC connected to the Mediatrix 2102 may experience momentary loss of Internet connectivity.

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

Download via HTTP

The following steps explain how to download a software by using the HTTP protocol.

▶ **To download a software via HTTP:**

1. If not already done, setup the Image server used to download the software (see "Before Downloading" on page 125).

2. If not already done, configure the Image path as described in "Setting up the Image Path" on page 128.

3. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 126.

> **Caution:** When downloading via HTTP, the image server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).
>
> If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See "Software Servers Configuration" on page 126 for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to **http**.

Your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.

5. If your HTTP server requires authentication, set the following:

- The user name in the *imageTransferUsername* variable.
- The password in the *imageTransferPassword* variable.

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

All activities in progress on the Mediatrix 2102 are terminated immediately and the unit enters the maintenance mode (the value of the *groupAdminState* variable is "locked"). The software upgrade may take place.

The Mediatrix 2102 lines will be unlocked after successfully downloading the software and restarting.

If, for any reason, the software download is not successful, you must manually unlock the lines as per "Lines Administrative State" on page 139.

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

This starts the download process.

> **Caution:** Never shutdown the Mediatrix 2102 manually while in the download process, because the image may be partially written and the Mediatrix 2102 is unable to restart.

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

If Transparent Address Sharing is enabled during the software download, the PC connected to the Mediatrix 2102 may experience momentary loss of Internet connectivity.

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

Automatic Software Update

You can configure the Mediatrix 2102 to automatically update its software version. This update can be done:

- Every time the Mediatrix 2102 restarts.
- At a specific time interval you can define.

Automatic Update on Restart

The Mediatrix 2102 may download a new software version each time it restarts.

▶ **To set the automatic update every time the Mediatrix 2102 restarts:**

1. If not already done, setup the Image server used to download the software (see “Before Downloading” on page 125).
2. If not already done, configure the Image path as described in “Setting up the Image Path” on page 128.
3. If not already done, configure the image hosts and ports as defined in “Software Servers Configuration” on page 126.

> ⚠ **Caution:** When downloading via HTTP, the image server’s port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).
>
> If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See “Software Servers Configuration” on page 126 for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to either **http** or **tftp**.

   If you are using the HTTP protocol to download the software, be aware that your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.
5. If you are using the HTTP protocol and your HTTP server requires authentication, set the following:
   - The user name in the *imageTransferUsername* variable.
   - The password in the *imageTransferPassword* variable.
6. Set the *imageAutoUpdateOnRestartEnable* variable to **enable**.
7. Set the *imageAutoUpdateEnable* variable to **enable**.

   The automatic software update will be performed each time the Mediatrix 2102 restarts.

Automatic Update at a Specific Time Interval

You can configure the Mediatrix 2102 to download a software version at a specific day and/or time.

▶ **To set the automatic update at a specific time interval:**

1. If not already done, setup the Image server used to download the software (see "Before Downloading" on page 125).
2. If not already done, configure the Image path as described in "Setting up the Image Path" on page 128.
3. If not already done, configure the image hosts and ports as defined in "Software Servers Configuration" on page 126.

> **Caution:** When downloading via HTTP, the image server's port must be 80. You can query the actual port assigned in the *imagePrimaryPort* and *imageSecondaryPort* read-only variables (in the *ipAddressStatus* folder).
>
> If you are using a DHCP server and it did not provide the proper port, reconfigure it with the proper port or use a static configuration. See "Software Servers Configuration" on page 126 for more details.

4. In the *imageMIB*, set the *imageTransferProtocol* variable to either **http** or **tftp**.

   If you are using the HTTP protocol to download the software, be aware that your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.

5. If you are using the HTTP protocol and your HTTP server requires authentication, set the following:
   - The user name in the *imageTransferUsername* variable.
   - The password in the *imageTransferPassword* variable.

6. Define the time base for automatic software updates in the *imageAutoUpdateTimeUnit* variable (in the *imageAutomaticUpdate* group).

   You have the following choices:

Table 86: Time Unit Parameters

Parameter	Description
seconds	Updates the software every *x* seconds. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7).
minutes	Updates the software every *x* minutes. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7).
hours	Updates the software every *x* hours. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7).
days	Updates the software every *x* days. You can specify the *x* value in the variable *imageAutoUpdatePeriod* (see Step 7). You can also define the time of day when to perform the update in the *imageAutoUpdateTimeOfDay* variable (see Step 8).

7. Set the waiting period between each software update in the *imageAutoUpdatePeriod* variable.

   The time unit for the period is specified by the *imageAutoUpdateTimeUnit* variable (see Step 6). Available values are from 1 to 48.

   It may be possible that the Mediatrix 2102 skips a scheduled periodic update if the previous periodic update has not finished yet. This may happen with periods of a few seconds.

Let’s say for instance that you set the period to two seconds and the automatic update mechanism takes five seconds to complete. The following describes the behaviour:

Table 87: Scheduled Periodic Update

Time (s)	Description
0	Beginning of the automatic update mechanism.
2	Automatic update. The software download starts.
4	Automatic update. The Mediatrix 2102 skips this scheduled update because the previous update has not finished yet.
6	Automatic update. The Mediatrix 2102 skips this scheduled update because the previous update has not finished yet.
7	The software download is finished and the new software is applied.
8	Automatic update. The software download starts.

8. If you have selected **days** in Step 6, set the time of the day when to initiate a software update in the *imageAutoUpdateTimeOfDay* variable.

The time of the day is based on the *sntpTimeZoneString* variable setting (see “Chapter 17 - SNTP Settings” on page 183 for more details).

You must have a time server SNTP that is accessible and properly configured, or the automatic software update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server’s documentation. You can also refer to “Chapter 17 - SNTP Settings” on page 183 for more details on how to configure the Mediatrix 2102 for a SNTP server.

The software is downloaded at the first occurrence of this value and thereafter at the period defined by the *imageAutoUpdatePeriod* variable. Let’s say for instance the automatic software download is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic download is enabled before 14h00, the first download will take place the same day at 14h00, then the second download two days later at the same hour, and so on.
- If the automatic download is enabled after 14h00, the first download will take place the day after at 14h00, then the second download two days later at the same hour, and so on.

Available values are -1, and from 0 to 23. Setting the variable to **-1** means that the time of the day at which the Mediatrix 2102 first initiates a software download is randomly selected.

9. Set the *imageAutoUpdateEnable* variable to **enable**.

If one of the telephones/faxes is off-hook, the Mediatrix 2102 will perform the download five minutes after both ports are detected on-hook.

Spanning Tree Protocol (STP)

Many network switches use the Spanning Tree Protocol (STP) to manage Ethernet ports activity. When a software download occurs, the *Computer* and *Network* connectors of the Mediatrix 2102 may switch off. This shutdown may trigger these network switches to shutdown the matching Ethernet port for at least one minute. This shutdown on the switch side can prevent software download.

To prevent this, the Mediatrix 2102 supports the STP. However, this management has a potential time cost. It may appear from time to time that software downloads take more time. This is normal.

The following is an example where the STP management impacts the download duration.

- The software download procedure does not use any DHCP and DNS services.
- The primary image server is down (or not properly configured).
- The secondary image server is up and running well.

In this case, the Mediatrix 2102 tries to contact the primary image server. As it is not available, the Mediatrix 2102 retries for two minutes. It contacts the secondary server after that period and starts the software download.

> **Note:** When using the Mediatrix 2102, Mediatrix recommends to disable the Spanning Tree Protocol on the network to which the unit is connected.

Software Downgrade

It is possible to downgrade a Mediatrix 2102 from the current version (for instance, v5.0rx.x) to an older version (for instance, v4.4rx.x).

> **Note:** If you perform a default reset on the Mediatrix 2102, you must download the current version into the unit before performing the software downgrade procedure.

▶ **To perform a software downgrade:**

1. Create, in a common folder under the TFTP root path, the current (for instance, v5.0) and older (for instance, v4.4) applications folders.
2. Re-update the Mediatrix 2102 with the current application.

   The Mediatrix 2102 runs the current software version (v5.0rx.x).
3. Perform the software downgrade to the older application (v4.4rx.x) as described in "Download Procedure" on page 128.

Emergency Software Procedure

If the software download is suddenly interrupted, it may not be complete. Without any protection against this situation, the Mediatrix 2102 is not functional.

A transfer may be interrupted for the following reasons:

- An electrical shortage.
- The user of the Mediatrix 2102 can accidentally power off the unit.

Depending on the moment when the software download has been interrupted, the emergency software procedure (also called rescue application) can automatically start a new software download to repair the software if it has been corrupted by the interruption. However, there is a small but critical time frame during which unrecoverable errors could happen. This is why it is very important that the unit is not turned off during software downloads.

Using the Emergency Software

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

1. The Mediatrix 2102 tries to initiate the software download with the primary software server.
2. If the software download fails with the primary software server, the Mediatrix 2102 tries to initiate the software download with the secondary software server.
3. If the primary and the secondary servers cannot be reached, the Mediatrix 2102 tries two default servers: 192.168.0.10 and then 192.168.0.2.

   If, for some reason, it is impossible to rescue the unit by using the primary and secondary servers, setting up a server at one of these addresses within the correct subnet will provide an ultimate way to rescue the unit. However, if these addresses cannot be reached from the unit's subnet, the default gateway must provide appropriate routing to them.
4. If the software download also fails with the two default servers, the Mediatrix 2102 idles for one minute.
5. After this one minute, the Mediatrix 2102 tries to initiate the software download again.
6. If the software download fails again with the primary, secondary, and default software servers, the Mediatrix 2102 idles for two minutes before attempting to initiate the software download.
7. If the emergency software download still fails, the Mediatrix 2102 tries to initiate the software download again by doubling the delay between each attempt up to a maximum of 16 minutes:
   - first attempt: 1 minute delay
   - second attempt: 2 minutes delay
   - third attempt: 4 minutes delay
   - fourth attempt: 8 minutes delay
   - fifth attempt: 16 minutes delay
   - sixth attempt: 16 minutes delay
   - etc.

   This procedure continues until the software download completes successfully. The software download can fail if the software server cannot be reached or if the software directory is not found on the software server.

CHAPTER 11

Line Configuration

This chapter describes the features available on the lines connected to the Mediatrix 2102.

For information on voice codecs, see “Chapter 12 - Voice Transmissions” on page 145.

For information on data codecs, see “Chapter 13 - Fax Transmission” on page 157.

Lines Administrative State

You can independently set the administrative state of each analog line of your Mediatrix 2102. This state determines how the Mediatrix 2102 processes calls.

For instance, you must properly unlock the two analog lines of the Mediatrix 2102 to properly make and receive calls on all of them.

The administrative states may be applied in two ways:

- Temporary: The administrative state is applied immediately, but it is not kept after the Mediatrix 2102 restarts.
- Permanent: When the Mediatrix 2102 restarts, it reads a MIB variable to determine the administrative state defined for each analog line.

Temporary Administrative State

You can set the administrative state of a line that will be kept until the Mediatrix 2102 restarts. Once the unit restarts, it uses the permanent state defined for each line. See “Permanent Administrative State” on page 140 for more details.

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

▶ **To set a temporary administrative state:**

1. In the *ifAdminMIB*, locate the *ifAdminSetAdmin* variable.

   This variable temporary locks/unlocks the selected line of the Mediatrix 2102. This state is kept until the unit restarts. It offers the following settings:

Table 88: Temporary Lock Settings

Setting	Description
unlock	Registers the line to the SIP server.
lock	Cancels the line registration to the SIP server. Active calls in progress remain established until normal call termination. No new calls may be initiated.
forcelock	Cancels the line registration to the SIP server. All active calls in progress are terminated immediately. No new calls may be initiated.

Permanent Administrative State

The permanent administrative state is applied every time the Mediatrix 2102 restarts.

▶ **To set a permanent administrative state:**

1. In the *ifAdminMIB*, locate the *ifAdminInitialAdminState* variable.

   This variable indicates the administrative state the current analog line will have after the Mediatrix 2102 restarts. It offers the following settings:

Table 89: Permanent Lock Settings

Setting	Description
unlocked	Registers the line to the SIP server.
locked	The analog line is unavailable for normal operation. It cannot be used to make and/or receive calls.

Line Grouping

A group is a collection of analog lines that, when called from the IP network, behave as if they were only one line. It’s the same principle as calling a call centre, where there is only one telephone number, but there are several telephones on the call centre side. An algorithm allows to choose the telephone that will ring upon a new incoming call.

Currently, the Mediatrix 2102 does not use groups and the FXS lines are not part of any group. Future versions of the Mediatrix 2102 will allow you to define additional groups.

Unregistered Line Behaviour

You can specify whether a line should remain enabled or not when not registered. This is useful if you want your users to be able to make calls even if the line is not registered with the SIP server.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

▶ **To specify unregistered line behaviour:**

1. In the *sipExperimentalMIB*, locate the *sipUnregisteredPortBehavior* variable.

   The following values are available:

Table 90: Unregistered Line Behaviour

Value	Description
disablePort	When the line is not registered, it is disabled. The user cannot make or receive calls. Picking up the handset yields a fast busy tone, and incoming INVITEs receive a “403 Forbidden” response.
enablePort	When the line is not registered, it is still enabled. The user can receive and initiate outgoing calls. Note that because the line is not registered to a registrar, its public address is not available to the outside world; the line will most likely be unreachable except through direct IP calling.

Flash Hook Detection

The flash hook can be described as quickly depressing and releasing the plunger in or the actual handset-cradle to create a signal indicating a change in the current telephone session. Services such as picking up a call waiting, second call, call on hold, and conference are triggered by the use of the flash hook.

A flash hook is detected when the hook switch is pressed for a shorter time than would be required to be interpreted as a hang-up.

Using the “flash” button that is present on many standard telephone handsets can also trigger a flash hook.

The Mediatrix 2102 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 91: Flash Hook Parameters

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

2. Restart the Mediatrix 2102 so that the changes may take effect.

Source Line Selection

The source line selection feature defines a list of callers that have the right to use a specific FXS line to make a call. This feature can be used to map an FXS line to a specific FXO line of a gateway such as the Mediatrix 1204. See “Examples of Source Line Selection Use” on page 142 for more details.

▶ **To set the line selection:**

1. In the *lineSelectionMIB*, define the list of telephone numbers that can use this line to make calls in the *lineSelectionDigitMap* variable.

   Call sources that match this digit map can use this line. This string must follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). This digit map will not have any effect unless the feature’s status is “enabled”.

   Because this variable is located in a table, you can define different digit maps for each line of the Mediatrix 2102.

2. Enable the line selection feature by setting the *lineSelectionEnable* variable to **enable**.

   The source of the call is compared to all the source line selection digit maps defined in the previous step. The result of this comparison is a list of lines that can take the call, but are not necessarily available to do so.

   Once the match list has been created, there are two possibilities:

   - The list contains one or more lines. The line selection algorithm selects a line. If none of the lines in the list are available, the call is rejected. See “Line Selection Algorithm” on page 143 for details.
   - The list is empty. The line selection algorithm cycles through all lines that do not use source line selection. If no available lines can be found, the call is rejected. See “Line Selection Algorithm” on page 143 for details.

   Because this variable is located in a table, you can enable/disable the feature on a per-line basis.

Examples of Source Line Selection Use

FXS to FXO Line Mapping

You can map an FXS line to a specific FXO line of a gateway such as the Mediatrix 1204. In this case, a call made from this FXS line will always use the same FXO line. To achieve that, the Mediatrix 2102 and Mediatrix 1204 configurations would be something similar to the following:

```
Mediatrix 2102: IP address 192.168.0.1
sipUAMainUsername = 6661111 (FXS line #1)
sipUAMainUsername = 6662222 (FXS line #2)


Mediatrix 1204: IP address 192.168.0.2
lineSelectionDigitMap (FXO line #1) = 6661111
telephonyAttributesAutomaticCallEnable = enable
telephonyAttributesAutomaticCallTargetAddress = 6661111
lineSelectionDigitMap (FXO line #2) = 6662222
telephonyAttributesAutomaticCallEnable = enable
telephonyAttributesAutomaticCallTargetAddress = 6662222
lineSelectionDigitMap (FXO line #3) = 6663333
telephonyAttributesAutomaticCallEnable = enable
telephonyAttributesAutomaticCallTargetAddress = 6662222
lineSelectionDigitMap (FXO line #4) = 6664444
telephonyAttributesAutomaticCallEnable = enable
telephonyAttributesAutomaticCallTargetAddress = 6662222
```

With such a configuration, a call made from line #2 of a Mediatrix 2102 is processed on line #2 of the Mediatrix 1204. On the other hand, if a caller from the SCN calls line #3 of the Mediatrix 1204, the call is automatically redirected to line #3 of the Mediatrix 2102.

Reserving an FXS Line

You can reserve an FXS line for specific individuals. For instance, these individuals could be the management team members of a company.

If the telephone numbers of the management team are 221 and 222 and you want to reserve an FXS line for their exclusive use, configure the Mediatrix 2102 as follows:

```
lineSelectionDigitMap (FXS line #1) = (221|222)
lineSelectionDigitMap (FXS line #2) = xxx
```

The management team can thus use all FXS lines, while others can only use lines 2,3 and 4.

Line Selection Algorithm

Upon receiving a call, you can define in which way the Mediatrix 2102 selects a line to distribute the call load across all lines. Before accepting to use a line, the Mediatrix 2102 must check the following:

- The line's administrative status is idle.
- The line is configured to allow IP to line calls.

If the above three criteria are met, the line can be used to place a call, otherwise the IP to line call is rejected.

To define how to use lines:

1. In the *lineGroupingMIB*, locate the *lineGroupingGroupConfigTable* group.

2. Set the algorithm to select a line on an incoming IP to line call in the *lineGrpConfLineSelectionAlgorithm* variable.

Table 92: Line Selection Algorithm

Algorithm	Description
roundRobin	The unit starts from the line that follows the line used for the last IP to line call. For instance, if line #1 was used in the last call, the unit starts with line #2. Going toward the highest line, the unit selects the first line available. If the highest line is unavailable, the search continues from the lowest line number of the group to the line used for the last IP to line call.
lowToHigh	Starting from the lowest line number and going toward the highest line number, the unit selects the first line available.
highToLow	Starting from the highest line number and going toward the lowest line number, the unit selects the first line available.

3. If applicable, enable the call forward on no resource mechanism by setting the *lineGrpConfCallForwardNoRessourceEnable* to **enable**.

   This mechanism reroutes an incoming IP to line call in the event that all the lines are unavailable.

   The call is rerouted to the destination specified in the *lineGrpConfCallForwardNoRessourceAddress* variable.

4. Set the number to call when all lines are unavailable in the *lineGrpConfCallForwardNoRessourceAddress* variable.

   Accepted formats are:

   - telephone numbers (5551111)
   - SIP URLs such as "scheme:user@host". For instance, "sip:user@foo.com".

   This string is used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

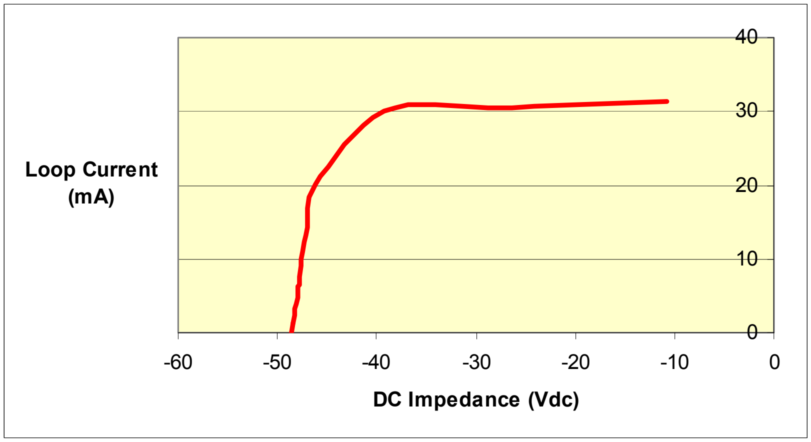
5. Restart the Mediatrix 2102 so that the changes may take effect.

Loop Current

When one of its analog lines goes off-hook, the Mediatrix 2102 controls the line in a fixed loop current mode. The value of the loop current can be modified through the MIB.

Note that the actual measured current may be different than the value you set, because it varies depending on the DC impedance. This is illustrated in Figure 35 for a loop current of 32 mA.

Figure 35: Loop Current vs Impedance – 32 mA



To set the loop current:

1. In the *fxsMIB,* set the *fxsLoopCurrent* variable to the value you want to use.

   The loop current is in mA. The range of available values is from 20 mA to 32 mA.

2. Restart the Mediatrix 2102 so that the changes may take effect.

When a remote end-user goes on-hook, the Mediatrix 2102 signals the far end disconnect by performing a current loop drop (< 1 mA) on the analog line. This current loop drop, also referred to as “Power Denial” mode, is typically used for disconnect supervision on analog lines. The Mediatrix 2102 maintains a current drop for one second (this value cannot be configured), then a busy tone is generated to indicate the user to hang up.

CHAPTER 12

Voice Transmissions

This chapter describes the various codecs the Mediatrix 2102 supports for transmitting audio signals.

Codec Descriptions

The two lines of the Mediatrix 2102 can simultaneously use the same codec (for instance, G.711 PCMA), or a mix of any of the supported codecs. Set and enable these codecs for **each** line.

Table 93: Codecs Comparison

	Compression	Voice Quality
G.711	None	Excellent
G.723.1	Highest	Good
G.729a/ab	High	Fair/Good

G.711 PCMA and PCMU

Specified in ITU-T Recommendation G.711. The audio data is encoded as 8 bits per sample, after logarithmic scaling. PCMU denotes µ-law scaling, PCMA A-law scaling.

Table 94: G.711 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 1 ms. See “Packetization Time” on page 148 for more details.
Voice Activity Detection (VAD)	Can be enabled or disabled. When enabled, two levels of detection are available: transparent or conservative. See “G.711 VAD” on page 153 for more details.
Comfort noise	Supports white and custom comfort noise as defined in *draft-ietf-avt-rtp-cn-05.txt*. See “G.711 Comfort Noise” on page 155 for more details.

Analog Modem

The Mediatrix 2102 can send modem transmissions in clear channel (G.711). It 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.

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 to compress the speech signal component of multi-media services at a very low bit rate. The audio is encoded in 30 ms frames.

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

Table 95: G.723.1 Features

Feature	Description
Packetization time	Range of 30 ms to 120 ms with increment of 30 ms. See "Packetization Time" on page 148 for more details.
Voice Activity Detection (VAD)	The Mediatrix 2102 supports the annex A. Annex A is the built-in support of VAD in G.723.1.

G.729

Specified in ITU-T Recommendation G.729, coding of speech at 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP). For all data rates, the sampling frequency (and RTP timestamp clock rate) is 8000 Hz.

A voice activity detector (VAD) and comfort noise generator (CNG) algorithm in Annex B of G.729 is recommended for digital simultaneous voice and data applications; they can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B comfort noise frame occupies 2 octets.

The Mediatrix 2102 supports G.729A and G.729AB for encoding and G.729, G.729A and G.729AB for decoding.

Table 96: G.729 Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increment of 10 ms. See "Packetization Time" on page 148 for more details.
Voice Activity Detection (VAD)	The Mediatrix 2102 supports the annex B. Annex B is the built-in support of VAD in G.729. See "G.729 VAD" on page 154 for more details.

Preferred Codec

The preferred codec is the codec you want to favour during negotiation.

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

▶ **To set a preferred codec:**

1. In the *voiceIfMIB,* locate the *voiceIfCodecPreferred* variable (*voiceIfCodecTable*).

This variable sets the preferred codec for this line.

2. Choose the codec you want to use from one of the available configurations:

- pcmu
- pcma
- g723
- g729

The default value is **pcmu**.

Enabling Individual Codecs

Enabling individual codecs allows you to define codecs that can be considered during negotiation. If codecs are disabled, they are not considered.

▶ **To enable voice codecs:**

1. In the *voiceIfMIB,* choose the codec you want to use (*voiceIfCodecTable*).

You have the choice between the following codecs:

Table 97: Enabling Voice Codecs

Codec	Variable	Set to...
PCMU (G.711 u-Law)	voiceIfCodecPcmuEnable	enable
PCMA (G.711 a-Law)	voiceIfCodecPcmaEnable	enable
G.723.1	voiceIfCodecG723Enable	g723-53kbs g723-63kbs
G.729.A	voiceIfCodecG729Enable	enable

Packetization Time

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet.

▶ **To set the packetization time:**

1. In the *voiceIfMIB,* set the packetization time of the codec(s) as required (*voiceIfCodecTable*). Available values vary from one codec to another.

Table 98: Packetization Time Settings

Variable	Definition	Values (ms)
PCMU (G.711 u-Law)		
voiceIfCodecPcmuMinPTime	Lower boundary for the packetization period. **Default Value**: 10	10-100, with increments of 1
voiceIfCodecPcmuMaxPTime	Upper boundary for the packetization period. **Default Value**: 100	10-100, with increments of 1
PCMA (G.711 a-Law)		
voiceIfCodecPcmaMinPTime	Lower boundary for the packetization period. **Default Value**: 10	10-100, with increments of 1
voiceIfCodecPcmaMaxPTime	Upper boundary for the packetization period. **Default Value**: 100	10-100, with increments of 1
G.723		
voiceIfCodecG723MinPTime	Lower boundary for the packetization period. **Default Value**: 30	30, 60, 90, 120
voiceIfCodecG723MaxPTime	Upper boundary for the packetization period. **Default Value**: 120	30, 60, 90, 120
G.729		
voiceIfCodecG729MinPTime	Lower boundary for the packetization period. **Default Value**: 10	10-100, with increments of 10
voiceIfCodecG729MaxPTime	Upper boundary for the packetization period. **Default Value**: 100	10-100, 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 is the default RTP value (20 ms for G.711 and G.729.AB, 30 ms for G.723) if it is included in the range delimited by the minimum and maximum. Otherwise, it is the minimum.

DTMF Transport Type

Standards Supported	- draft-choudhuri-sip-info-digit-00.txt - RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

You can define how to transport the DTMFs.

▶ **To set the DTMF transport type:**

1. In the *voiceIfMIB,* set the DTMF transport type in the *voiceIfDtmfTransport* variable (*voiceIfDtmfTransportTable* group).

The following choices are available:

Table 99: DTMF Transport Type Parameters

Transport Parameter	Description
inBand	The DTMFs are transmitted like the voice in the RTP stream.
outOfBandUsingRtp	The DTMFs are transmitted as per RFC 2833 (see "DTMF Payload Type" on page 150 for additional information).
outOfBandUsingSignalingProtocol	The DTMFs are transmitted as per *draft-choudhuri-sip-info-digit-00.txt* (see "DTMF Transport Using SIP INFO" on page 150 and "DTMF Transport over the SIP Protocol" on page 151 for more details).
signalingProtocolDependent	The signalling protocol has the control to select the DTMF transport mode. The SDP body includes both RFC 2833 and *draft-choudhuri-sip-info-digit-00.txt* in that order of preference.

DTMF out-of-band

Certain compression codecs such as G.723.1 and G.729 effectively distort voice because they lose information from the incoming voice stream during the compression and decompression phases. For normal speech this is insignificant and becomes unimportant. In the case of pure tones (such as DTMF) this distortion means the receiver may no longer recognize the tones. The solution is to send this information as a separate packet to the other endpoint, which then plays the DTMF sequence back by re-generating the true tones. Such a mechanism is known as out-of-band DTMF. The Mediatrix 2102 receives and sends out-of-band DTMFs as per RFC 2833 using RTP. DTMFs supported are 0-9, A-D, *, #.

DTMF Transport Using SIP INFO

Standards Supported	• RFC 2976: The SIP INFO Method • draft-choudhuri-sip-info-digit-00.txt

You can use the SIP INFO method to collect and transport DTMFs. The collection process is regarded as being an unsolicited one-character timer-less digit collection.

When the feature is enabled:

- The Mediatrix 2102 sends a separate SIP INFO method every time a digit is entered during the call.
- The Mediatrix 2102 plays each DTMF sent in a separate message upon receiving a valid SIP INFO message.

To enable the DTMF transport using the SIP INFO feature:

1. In the *voiceIfMIB*, set the DTMF transport type in the *voiceIfDtmfTransport* variable (*voiceIfDtmfTransportTable* group) according to the transport type you want to use.

   There are three methods to transport DTMF events:

   - in-band
   - out-of-band using RTP (RFC 2833)
   - out-of-band using SIP INFO

Table 100: Transport Type Setting

To	Set the variable to:
Transport DTMF events in-band.	inBand
Transport DTMF events out-of-band by exclusively using RTP (RFC 2833).	outOfBandUsingRtp
Transport DTMF events out-of-band by exclusively using the SIP INFO method.	outOfBandUsingSignalingProtocol
Offer the choice to transport DTMF events out-of-band by using either RTP or the SIP INFO method.	signalingProtocolDependent

If you set the *voiceIfDtmfTransport* variable to **signalingProtocolDependent**, the remote party must select one of the two transport types. Transporting DTMF by using RTP has priority over the SIP INFO method.

DTMF Payload Type

Standards Supported	RFC 1890 – RTP Profile for Audio and Video Conferences with Minimal Control

When selecting the *outOfBandUsingRtp* DTMF transport mode (see “DTMF Transport Type” on page 149 for more details), you can determine the actual RTP dynamic payload type used for the “telephone-event” in an initial offer. The payload types available are as per RFC 1890.

To define the DTMF payload type:

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

   Available values range from 96 to 127.

DTMF Transport over the SIP Protocol

Standards Supported	draft-choudhuri-sip-info-digit-00.txt

You can select the method used to transport DTMFs out-of-band over the SIP protocol.

This feature is effective only if the *voiceIfDtmfTransport* variable is set to **outOfBandUsingSignalingProtocol** (see “DTMF Transport Type” on page 149 for more details).

▶ **To select the DTMF transport method over the SIP protocol:**

1. In the *voiceIfMIB*, set the DTMF transport type in the *voiceIfDtmfTransport* variable to **outOfBandUsingSignalingProtocol**.
2. In the *sipInteropMIB*, set the DTMF transport type in the *sipInteropDtmfTransportMethod* variable (*sipInteropDtmfTransportBySipProtocol* group).

   The following methods are available:

   Table 101: DTMF Out-of-Band Transport Methods

Method	Description
draftChoudhuriSipInfoDigit00	Transmits DTMFs by using the method defined in *draft-choudhuri-sip-info-digit-00*. Only the unsolicited-digit part is supported.

infoDtmfRelay	Transmits DTMFs by using a custom method. This custom method requires no SDP negotiation and assumes that the other peer uses the same method.
	It uses a SIP INFO message with a content of type *application/dtmf-relay*. The body of the message contains the DTMF transmitted and the duration of the DTMF:
	`Signal= 1`
	`Duration= 160`
	When transmitting, the duration is the one set in the *sipInteropDtmfTransportDuration* variable (see Step 3 below).
	When receiving, the duration of the DTMF received is not used. The value is the one set in the *analogScnGwDtmfDuration* variable (see Step 4 below).
	DTMFs are transmitted one at a time. It is thus not compatible with the PIN dialing feature (see “PIN Dialing” on page 219 for more details).
	Available digits are “0123456789ABCD*#”. The Mediatrix 2102 also supports the “,;p” characters when receiving DTMFs.

3. Set the DTMF duration sent in the INFO message when using the **infoDtmfRelay** method to transmit DTMFs in the *sipInteropDtmfTransportDuration* variable.

   This value is expressed in milliseconds (ms). The default value is **100** ms.
4. In the *analogScnGwMIB*, set the DTMF duration when using the **infoDtmfRelay** method to receive DTMFs in the *analogScnGwDtmfDuration* variable.

   This is the duration, in milliseconds (ms), a DTMF is played when dialing the destination phone number.
5. Set an inter-digit dial delay in the *analogScnGwInterDigitDial Delay* variable.

   This is the delay, in milliseconds (ms), between two DTMFs when dialing the destination phone number. This is useful when the Mediatrix 2102 receives DTMFs out-of-band faster than it can signal them.
6. Restart the Mediatrix 2102 so that the changes may take effect.

Adaptative Jitter Buffer

The jitter buffer allows better protection against packet loss, but increases the voice delay. If the network to which the Mediatrix 2102 is connected suffers from a high level of congestion, the jitter buffer protection level should be higher. If the network to which the Mediatrix 2102 is connected suffers from a low level of congestion, the jitter buffer protection level should be lower.

> **Note:** You cannot disable the adaptative jitter buffer on the Mediatrix 2102. However, if you set the *voiceIfTargetJitterBufferLength* and *voiceIfMaxJitterBufferLength* variables to the same value, you will have a non-adaptative jitter buffer.

▶ **To set Jitter Buffer variables:**

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

2. Define the jitter buffer length in the *voiceIfTargetJitterBufferLength* variable.

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

Values range from 0 ms to 125 ms. The default value is 30 ms. You can change values by increments of 1 ms, but Mediatrix recommends to use multiple of 5 ms.

It is best not to set target jitter values below the default value. Setting a target jitter buffer below 5 ms could cause an error. Jitter buffer adaptation behaviour varies from one codec to another. See “About Changing Jitter Buffer Values” on page 152 for more details.

3. Define the maximum jitter buffer length in the *voiceIfMaxJitterBufferLength* variable.

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

Values range from 0 ms to 125 ms. The default value is 125 ms. You can change values by increments of 1 ms, but Mediatrix recommends to use multiple of 5 ms.

See “About Changing Jitter Buffer Values” on page 152 for more details.

4. Enable the jitter buffer protection by setting the *voiceIfAdaptativeJitterBufferEnable* variable to **enable**.

5. Restart the Mediatrix 2102 so that the changes may take effect.

About Changing Jitter Buffer Values

Mediatrix recommends to avoid changing the target and maximum jitter buffer values unless experiencing or strongly expecting one of the following symptoms:

- If the voice is scattered and a lot of jitter buffer events are received when the syslog is enabled, try to increase the maximum jitter buffer value.
- If the delay in the voice path (end to end) is too long, you can lower the target jitter value, but ONLY if the end-to-end delay measured matches the target jitter value.

  For instance, if the target jitter value is 50 ms, the maximum jitter is 300 ms and the delay measured is 260 ms, it would serve nothing to reduce the target jitter. However, if the target jitter value is 100 ms and the measured delay is between 100 ms and 110 ms, then you can lower the target jitter from 50 ms to 30 ms.

Voice Activity Detection

The Voice Activity Detection (VAD) defines how the Mediatrix 2102 sends information pertaining to silence. This allows the unit to detect when the user talks, thus avoiding to send silent RTP packets. This saves on network resources. However, the VAD may affect packets that are not really silent (for instance, cut sounds that are too low). The VAD can thus slightly affect the voice quality.

Note: You cannot disable the G.723 VAD.

G.711 VAD

The G.711 VAD is generic – when enabling VAD, G.711 sends speech frames only during periods of audio activity. During silence periods, G.711 does not send speech frames, but it may send Comfort Noise (CN) packets (payload 13) containing information about background noise.

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

▶ **To enable G.711 VAD:**

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

2. Define the sensitivity of the VAD algorithm to silence periods in the *voiceIfG711VoiceActivityDetectionEnable* variable.

The following settings are available:

Table 102: G.711 VAD Settings

Setting	Description
Disable	VAD is not used.
Transparent	VAD is enabled. It has low sensitivity to silence periods.
Conservative	VAD is enabled. It has normal sensitivity to silence periods.

The difference between transparent and conservative is how “aggressive” the algorithm considers something as an inactive voice and how “fast” it stops the voice stream. A setting of conservative is a little bit more aggressive to react to silence compared to a setting of transparent.

The default value is **conservative**.

3. Restart the Mediatrix 2102 so that the changes may take effect.

G.729 VAD

G.729 has a built-in VAD in its Annex B version. It is recommended for digital simultaneous voice and data applications and can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B frame occupies 2 octets. The CN packets are sent in accordance with annex B of G.729.

▶ **To enable G.729 VAD:**

1. In the *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the *voiceIfG729VoiceActivityDetectionEnable* variable.

   The following settings are available:

Table 103: G.729 VAD Settings

Setting	Description
disable	G.729 uses annex A only. The Mediatrix 2102 does not send G.729 Annex B comfort noise frames.
enable	G.729 annex A is used with annex B. The Mediatrix 2102 sends G.729 Annex B comfort noise frames during silence periods.

See “Enabling Individual Codecs” on page 147 for more details.

Echo Cancellation

Echo cancellation eliminates the echo effect caused by signal reflections. An echo is a signal that has been reflected or otherwise returned with enough magnitude and delay to be perceived. The echo cancellation is usually an active process in which echo signals are measured and cancelled or eliminated by combining an inverted signal with the echo signal.

You cannot disable echo cancellation on the Mediatrix 2102.

G.711 Comfort Noise

Standards Supported	draft-ietf-avt-rtp-cn-05.txt

Comfort Noise (CN) defines how the Mediatrix 2102 processes silence periods information it receives.

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

During silence periods, the Mediatrix 2102 may receive CN packets containing information about background noise. When enabling Comfort Noise Generation (CNG), those packets are used to generate local comfort noise.

▶ **To enable Comfort Noise:**

1. In the *voiceIfMIB*, locate the *voiceIfTable* group.
2. Define the type of comfort noise in the *voiceIfG711ComfortNoiseGenerationEnable* variable.

   The following settings are available:

   Table 104: Comfort Noise Settings

Setting	Description
disable	CNG disabled.
whiteNoise	CNG enabled – white noise.
customNoise	CNG enabled – custom noise. More elaborated background noise that sounds better than white comfort noise.

3. Restart the Mediatrix 2102 so that the changes may take effect.

User Gain

The user gain allows you to modify the input and output sound level of the Mediatrix 2102.

Caution: Use these settings with great care. Mediatrix recommends not to modify the user gain variables unless absolutely necessary because default calibrations may not be valid anymore.

Modifying user gains may cause problems with DTMF detection and voice quality – using a high user gain may cause sound saturation (the sound is distorted). Furthermore, some fax or modem tones may not be recognized anymore. The user gains directly affect the fax communication quality and may even prevent a fax to be sent.

You can compensate with the user gain if there is no available configuration for the country in which the Mediatrix 2102 is located. Because the user gain is in dB, you can easily adjust the loss plan (e.g., if you need an additional 1 dB for analog to digital, simply put 1 for user gain input).

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

▶ **To set user gain variables:**

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

2. Define the following variables:

- *voiceIfUserInputGainOffset*: User input gain offset in dB (from analog to digital).
- *voiceIfUserOutputGainOffset*: User output gain offset in dB (from digital to analog).

Values range from -30 dB to +20 dB. However, going above +6 dB may introduce clipping/distortion depending on the country selected. Under -24 dB, you will not have much signal either.

3. Restart the Mediatrix 2102 so that the changes may take effect.

CHAPTER
13

Fax Transmission

This chapter describes how to perform fax transmissions in clear channel and T.38 with the Mediatrix 2102.

Introduction

The Mediatrix 2102 handles G3 and Super G3 fax transmissions at speeds up to 14.4 kbps. Automatic fax mode detection is standard on all lines. Real-Time Fax Over UDP with the T.38 protocol stack is also available.

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

A fax call works much like a regular voice call, with the following differences:

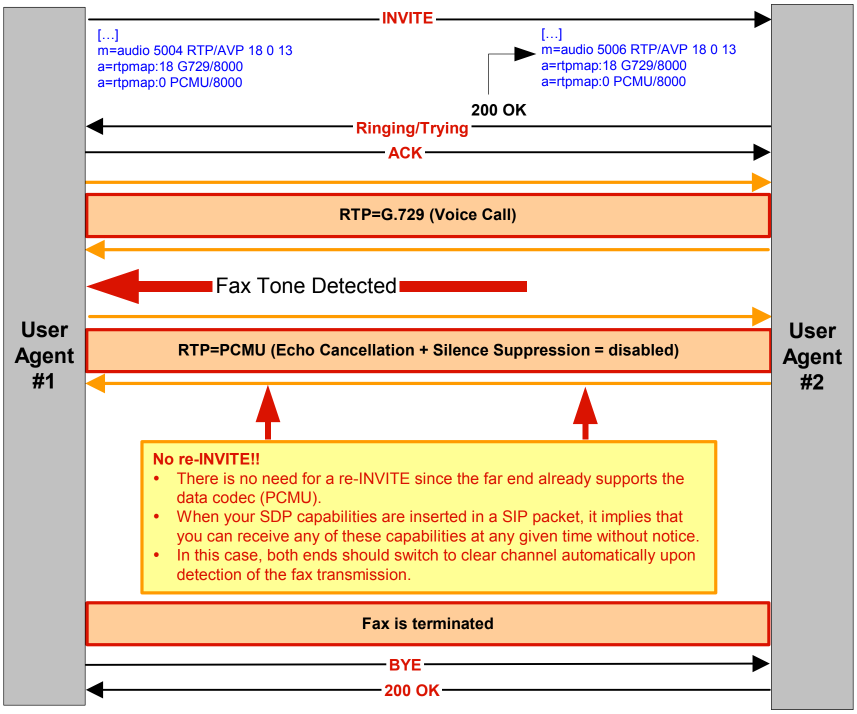
1. The fax codec may be re-negotiated by using a re-INVITE.
2. The goal of the re-INVITE is to allow both user agents to agree on a fax codec, which is either:
    - *a.* Clear channel (PCMU/PCMA) without Echo Cancellation nor Silence Suppression (automatically disabled).
    - *b.* T.38.
3. Upon fax termination, if the call is not BYE, the previous voice codec is recovered with another re-INVITE.

All lines of the Mediatrix 2102 can simultaneously use the same codec (for instance, T.38), or a mix of any of the supported codecs. Set and enable these codecs for **each** line.

Clear Channel Fax

The Mediatrix 2102 can send faxes in clear channel. The following is a clear channel fax call flow:

Figure 36: Clear Channel Fax Call Flow


INVITE
[...]
m=audio 5004 RTP/AVP 18 0 13
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
[...]
m=audio 5006 RTP/AVP 18 0 13
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
200 OK
Ringing/Trying
ACK
RTP=G.729 (Voice Call)
Fax Tone Detected
User Agent #1
User Agent #2
RTP=PCMU (Echo Cancellation + Silence Suppression = disabled)
No re-INVITE!!
• There is no need for a re-INVITE since the far end already supports the data codec (PCMU).
• When your SDP capabilities are inserted in a SIP packet, it implies that you can receive any of these capabilities at any given time without notice.
• In this case, both ends should switch to clear channel automatically upon detection of the fax transmission.
Fax is terminated
BYE
200 OK

▶ To set a preferred clear channel fax transmission codec:

1. Set the clear channel codec to use upon detecting a fax tone in the *dataIfClearChannelCodecPreferred* variable.

   This variable is used to decide which of PCMU or PCMA is preferred, even for voice transmissions. It has an impact only if a codec other than PCMU or PCMA is chosen in the *voiceIfCodecPreferred* variable (see "Preferred Codec" on page 147). For instance, if G.723 is the preferred voice codec, then PCMU and PCMA are ordered following the *dataIfCleaChannelCodecPreferred* setting.

   Clear channel faxes use the negotiated codec, regardless of the setting applied to *dataIfCleaChannelCodecPreferred*.

   Mediatrix suggests to use *pcma* if you are located in Europe and *pcmu* anywhere else. However, you should check first which codec is supported in your telephone network.

T.38 Fax

Standards Supported	• Based on *draft-ietf-sipping-realtimefax-01.txt* • Recommendation ITU T.38 version 0

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

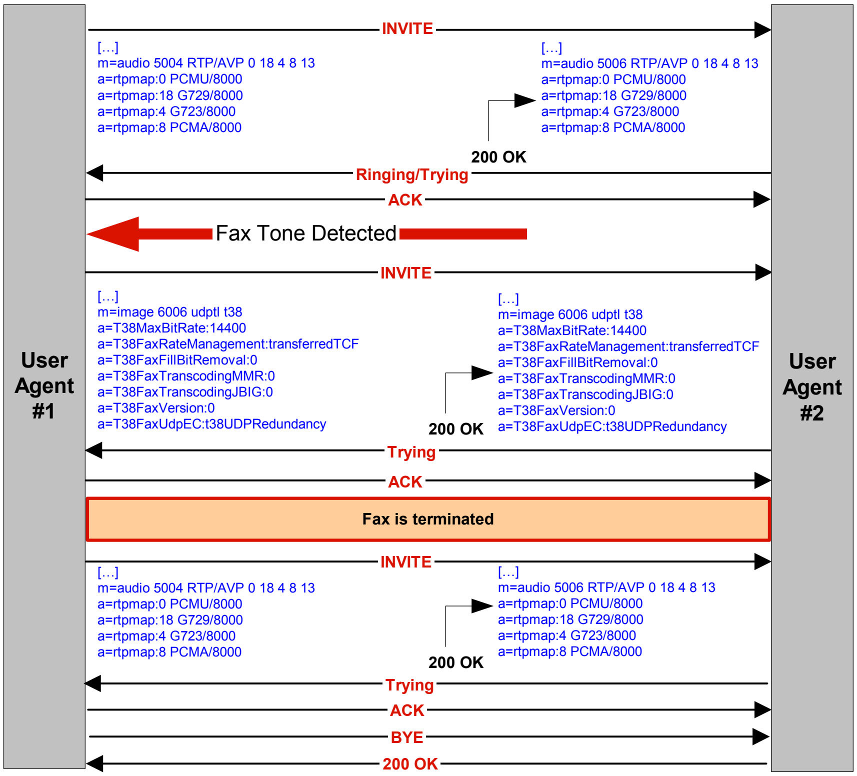
The Mediatrix 2102 can send faxes in T.38 mode over UDP or TCP. T.38 is used for fax if both units are T.38 capable; otherwise, transmission in clear channel over G.711 as defined is used (if *G.711 µ-law* and/or *G.711 A-law* are enabled). If no clear channel codecs are enabled and the other endpoint is not T.38 capable, the fax transmission fails.

Caution: The Mediatrix 2102 opens the T.38 channel only after receiving the “200 OK” message from the peer. This means that the Mediatrix 2102 cannot receive T.38 packets before receiving the “200 OK”. Based on RFC 3264, the T.38 channel should be opened as soon as the unit sends the “INVITE” message. See “Fax Issues” on page 247 for more details.

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

The following is a T.38 fax call flow:

Figure 37: T.38 Fax Call Flow



```
[…]
m=audio 5004 RTP/AVP 0 18 4 8 13
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
```

```
[…]
m=audio 5006 RTP/AVP 0 18 4 8 13
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
```

```
[…]
m=image 6006 udptl t38
a=T38MaxBitRate:14400
a=T38FaxRateManagement:transferredTCF
a=T38FaxFillBitRemoval:0
a=T38FaxTranscodingMMR:0
a=T38FaxTranscodingJBIG:0
a=T38FaxVersion:0
a=T38FaxUdpEC:t38UDPRedundancy
```

```
[…]
m=image 6006 udptl t38
a=T38MaxBitRate:14400
a=T38FaxRateManagement:transferredTCF
a=T38FaxFillBitRemoval:0
a=T38FaxTranscodingMMR:0
a=T38FaxTranscodingJBIG:0
a=T38FaxVersion:0
a=T38FaxUdpEC:t38UDPRedundancy
```

```
[…]
m=audio 5004 RTP/AVP 0 18 4 8 13
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
```

```
[…]
m=audio 5006 RTP/AVP 0 18 4 8 13
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
```

▶ **To set T.38 fax transmission:**

1. Enable T.38 by setting the *dataIfCodecT38Enable* variable to **enable**.
2. Set the number of redundancy packets sent with the current packet in the *dataIfCodecT38ProtectionLevel* variable.

   This is the standard redundancy offered by T.38. Please see step ***3*** for additional reliability options for T.38.

   Available values range from 1 to 5, 3 being the default value.
3. For additional reliability, define the number of times T.38 packets are retransmitted in the *dataIfT38FinalFramesRedundancy* variable.

   This only applies to the T.38 packets where the PrimaryUDPTL contains the following T.38 data type:

   - HDLC_SIG_END,
   - HDLC_FCS_OK_SIG_END,
   - HDLC_FCS_BAD_SIG_END and
   - T4_NON_ECM_SIG_END
4. Restart the Mediatrix 2102 so that the changes may take effect.

CHAPTER

14

Bypass Configuration

The Mediatrix 2102 may have an optional RJ-11 connector used to connect to a standard SCN line, called *Bypass*. It allows its users to make emergency calls and maintain telephone services in the event of a power outage or network failure.

Bypass Connector Settings

During normal operation, the SCN line connected to the *Bypass* connector is switched out of the circuit through commuting relays.

The *Bypass* connector can be activated by three different conditions:

- When power is removed from the Mediatrix 2102.
- When the IP network is down.
- When the user dials a pre-configured digits sequence (e.g., “911”), which indicates to the Mediatrix 2102 that the user wants to make an emergency call.

If one of these conditions is met, a phone/fax used on FXS connector 1 is directly connected to the SCN Bypass line. Connector 1 stays in Bypass connection until:

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

Emergency Number Bypass

If the Bypass connection has been triggered because of an emergency call, the user automatically bypasses the VoIP connection of the Mediatrix 2102. Connector 1 of the unit is thus directly connected to the SCN and the unit dials the emergency number on the SCN side.

Once the call is finished and the telephone is on-hook, the Mediatrix 2102 stays connected to the SCN for a period of time you can define. During this period of time, the emergency operator can reach the caller through the SCN bypass connector. When this period of time elapses, the Mediatrix 2102 goes back to its normal operational mode if the telephone is on-hook. If the telephone is off-hook, the unit stays in bypass mode until the telephone is put on-hook and the period of time you defined has elapsed.

Note: The Emergency number bypass feature has priority over all other dial maps of the Mediatrix 2102, including the Emergency call service (“Emergency Call” on page 201). As soon as the user dials the emergency number, the *Bypass* connector activates and the call is sent on the PSTN. No INVITE SIP is sent even if the Emergency call service dial map is set with the same value.

▶ **To enable the emergency number bypass feature:**

1. In the *fxsMIB*, define the emergency number that must be connected to the SCN in the *fxsEmergencyBypassDialMap* variable.

   For instance, you could decide to put “911” as the emergency number. This number must follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187).

2. Define the period of time for which the Mediatrix 2102 stays connected to the SCN once the telephone is on-hook in the *fxsEmergencyBypassTimeout* variable.

   During this period of time, the emergency operator can reach the caller through the SCN bypass connector.

3. Define how long, in seconds, the Mediatrix 2102 will wait before playing emergency digits on the SCN side once in bypass mode in the *fxsEmergencyBypassDialDelay* variable.

   The default Value is **3** seconds.

4. Enable the emergency bypass feature by setting the *fxsEmergencyBypassEnable* variable to **enable**.

Standard Bypass

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

▶ To enable the standard Bypass feature:

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

   This option enables/disables the bypass service.

Table 105: Bypass Values

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

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

The default value is **enable**.

CHAPTER

15

SIP Protocol Features

This chapter defines the SIP-specific feature to set up to properly use the SIP signalling programs and information defined in Mediatrix' SIP stack.

User Agents

A user agent is a logical entity that can act as both client and server for the duration of a dialog. Each line (also known as endpoint) of the Mediatrix 2102 is a user agent.

You can set information for each user agent such as its telephone number and friendly name. This information is used to dynamically create the *To*, *From* and *Contact* headers used in the request the user agent sends. These headers make up the caller ID information that is displayed on telephones/faxes equipped with a proper LCD display. See "Caller ID Information" on page 83 for more details.

Most of the variables related to the user agents are located in tables. You can display and define the information for all lines. You can also use these tables to create/edit five user names and passwords per line. This means that:

- Rows 1-5 of the table are reserved for line 1.
- Rows 6-10 of the table are reserved for line 2.
- etc.

If you want to enter a user name for the second line, you must do so in the sixth row of the table. If you want to enter a user name for the third line, you must do so in the eleventh row of the table, and so on.

Before changing a parameter value, 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.

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

▶ **To set basic user agent information:**

1. In the *sipMIB*, set the user agent port number in the *sipPort* variable.

   The default value is 0. If *sipPort* is set to 0, the default SIP port is used.

2. In the *sipUAIfTable* group, set a main user name in the *sipUAMainUsername* variable.

   The main user name uniquely identifies this endpoint in the domain, such as a telephone number. It is used to create the *Contact* and *From* headers. The *From* header carries the permanent location (IP address, home domain) where the endpoint is located. The *Contact* header carries the current location (IP address) where the endpoint can be reached. Contact headers are used in two ways:

   - First, contacts are registered to the registrar. This enables callers to be redirected to the endpoint's current location.
   - Second, a contact header is sent along with any request the user agent sends (e.g., INVITE), and is used by the target user agent as a return address for later requests to this endpoint.

3. Set a display name in the *sipUADisplayName* variable.

   This is a friendly name for the user agent. It contains a descriptive version of the URI and is intended to be displayed to a user interface.

4. Define a list of other accepted user names in the *sipUAOtherAcceptedUsernames* variable.

   This is a list of user names that the endpoint recognizes as its own, but does not register in contacts sent to the registrar. The endpoint only registers the user name in *sipUAMainUsername*.

You can use this variable 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.

To include more than one user name, separate them with a “,” character, such as: user1, user2, 5552222, 18195552222.

You can now define the session timers parameters. See “Session Timers” on page 164 for more details.

SIP User Agent Header

Standards Supported	RFC 3261 – SIP: Session Initiation Protocol, section 20.41 (User-Agent)

The *User-Agent* header field contains information about the user agent client originating the request. For instance, the information of the *User-Agent* header could be something like the following:

```
User-Agent: Softphone Beta1.5
```

You can specify if the Mediatrix 2102 sends this information or not when establishing a communication.

▶ **To enable sending the SIP User Agent header:**

1. In the *sipInteropMIB*, set the *sipInteropSendUAHeaderEnable* variable to **enable**.

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 at every *n* seconds.

A successful response (200 OK) to this INVITE indicates that the peer is still alive and reachable. A timeout to this INVITE may mean that there are problems in the signalling path or that the peer is not available anymore. In that case, the call is shut down by 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. It must be equal to or greater than the minimum value. This value is reflected in the *Session-Expires* header.

2. Set the session timer minimum expiration delay in the *sipUAMinimumSessionExpirationDelay* variable.

This is the minimum value, in seconds, for the periodical session refreshes. It must be equal to or smaller than the maximum value. This value is reflected in the *Min-SE* header.

The *Min-SE* value is a threshold under which proxies and user agents on the signalling path are not allowed to go.

▶ **To disable the Session Timer service:**

1. Set the *sipUAMaximumSessionExpirationDelay* variable to **0**.

Increasing the maximum helps to reduce network traffic, but also makes “dead” calls longer to detect.

Session Timer Version

Standards Supported	- draft-ietf-sip-session-timer-08.txt - draft-ietf-sip-session-timer-04.txt (expired)

You can select the version of the session timer draft that the Mediatrix 2102 uses. Session timer versions other than those provisioned may not work because of backward compatibility issues between the versions.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See "MIB Structure" on page 43 for more details.

The Mediatrix 2102 supports the following session timer versions:

Table 106: Session Timer Versions Supported

Version	Description
sessionTimer04	The Mediatrix 2102 uses 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 use this setting for backward compatibility issues only.
sessionTimer08	The Mediatrix 2102 uses 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. Use this setting if you do not need to interoperate with session timer v4-enabled parties.

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

1. In the *sipInteropMIB*, set the *sipInteropSessionTimersVersion* variable with the proper version.
   - sessionTimer04
   - sessionTimer08

Background Information

The following explains how the session timers are used.

SDP in Session Timer reINVITEs

The reINVITE is sent with the last SDP that was negotiated. Receiving 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 replies a "422 Timer too low" to the INVITE and terminates the call. The phone does not ring.

It is up to the caller to decide what to do when it receives a 422 to its INVITE. 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 the Session?

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 always let the user agent client (caller) perform the refreshes if the caller supports session timers. In the case where the caller does not support session timers, the Mediatrix unit assumes the role of the refresher.

Authentication

Standards Supported	Basic and Digest authentication as per RFC 3261

Authentication information allows you to add some level of security to the Mediatrix 2102 lines by setting user names and passwords. You can add two types of authentication information:

- line-specific authentication
- unit authentication

When a realm requests authentication, the line-specific authentication is tried first, and then the unit authentication if required.

Line-Specific Authentication

You can define up to five user names and five passwords for each line of the Mediatrix 2102. A line can thus register with five different realms. Keep in mind that:

- Rows 1-5 of the table where you define the user names and passwords are reserved for line 1.
- Rows 6-10 of the table where you define the user names and passwords are reserved for line 2.
- etc.

For instance, to enter a user name for the second line, you must do so in the sixth row of the table. To enter a user name for the third line, you must do so in the eleventh row of the table, and so on.

To set line-specific authentication:

1. In the *sipUAIfAuthenticationTable* group, set the following information:

Table 107: Line-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 up to five user names and five passwords for the Mediatrix 2102. These user names and passwords apply to all lines of the unit.

In the *Unit Manager Network Administration Manual*, refer to chapter *Signalling Protocols Parameters*, section *SIP Authentication*.

To set unit authentication:

1. In the *sipUnitAuthenticationTable* group, set the following information:

Table 108: 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.

Table 108: Unit-Specific Authentication (Continued)

Variable	Description
sipUnitAuthPassword	User password.

Authentication Request Protection

When the Mediatrix 2102 sends an authentication request, you can configure it so that it tries to apply the authentication with integrity protection when this feature is supported by the SIP server. However, you can disable this behaviour to only apply the authentication.

▶ **To set the quality of protection:**

1. In the *sipInteropMIB*, specify the quality of protection the SIP User Agent should apply to its authentication request in the *sipInteropAuthenticationQop* variable.

The following values are supported:

Table 109: Quality of Protection

Parameter	Description
auth	The SIP User Agent applies authentication only. This is the default value.
auth-int	The SIP User Agent applies authentication with integrity protection (see RFC 2617).

2. Restart the Mediatrix 2102 so that the changes may take effect.

NAT Traversal

The Mediatrix 2102 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.

Currently only one Mediatrix unit can be deployed behind a standard NAT.

You can configure the Mediatrix 2102 with the public IP address of the NAT system, which allows to reach the unit. SIP packets sent by the Mediatrix 2102 contain the NAT address configured as SIP contact. If the NAT service is not activated, the real IP address of the Mediatrix 2102 is used.

This method is recommended when the public IP address of the NAT system is static or does not change regularly since it would cause downtime until it is changed manually.

Mediatrix 2102 Configuration

This section describes how to activate the NAT service of the Mediatrix 2102.

▶ **To activate the NAT service:**

1. In the *ipAddressConfig* folder, set the *localHostWanAddressSelectConfigSource* variable to **static**.

Note: If you want to do NAT traversal, you cannot use a PPPoE connection.

2. Enter the public IP address of the NAT system in the *localHostStaticWanAddress* variable.

   This is the public IP address used as Contact address by outgoing SIP packets crossing a NAT system.

NAT System Configuration

You must configure the NAT system to some degree. The configuration required depends on the type of NAT system you are using, but this usually involves port forwarding configuration.

Network Address Translation

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

NAT automatically provides firewall-style protection without any special set-up because it only allows connections originating on the inside network. This means, for instance, that an internal client can connect to an outside FTP server, but an outside client cannot connect to an internal FTP server because it would have to originate the connection, and NAT does not allow that.

Call Transfer Capacity

The following are parameters you can set to define how the Mediatrix 2102 handles call transfers.

Call Transfer Version

Standards Supported	- draft-ietf-sip-cc-transfer-05.txt - draft-ietf-sip-cc-transfer-02.txt (expired) - draft-ietf-sip-refer-02.txt

You can select the version of the transfer draft that the Mediatrix 2102 uses. The provisioned version is used for initiating transfers and receiving them. Transfer versions other than those provisioned do not work.

Table 110: Call Transfer Versions Supported

Version	Description
transfer02	The Mediatrix 2102 executes transfers by using the methods described in the now expired *draft-ietf-sip-cc-transfer-02.txt*. This draft was obsoleted. Its use is deprecated and you should use this setting for backward compatibility issues only.
transfer05UsingRefer02	The Mediatrix 2102 executes transfers by 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*. Use this setting if you do not need to interop with transfer02-enabled parties. See “Replaces Configuration Setting” on page 169 for more details.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

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

1. In the *sipInteropMIB*, set the *sipInteropTransferVersion* variable with the proper version.
   - transfer02
   - transfer05UsingRefer02

Replaces Configuration Setting

You can configure how to use 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. This allows you to control how the Mediatrix 2102 interoperates with other vendor’s products and older Mediatrix units.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

▶ **To set Replaces configuration:**

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

   You have the following choices:

Table 111: Replaces Configuration

Configuration	Description
doNotUseReplaces	The *Replaces* header is not used.

Table 111: Replaces Configuration (Continued)

Configuration	Description
useReplacesWithRequire	The *Replaces* header is used. It can be seen in the *Refer-To* header of the REFER request sent by the transferor. It can also be seen in the INVITE sent by the transferee. The target that supports *Replaces* uses its informations to merge the new INVITE with an existing call specified in the *Replaces* header. The transferee requires to use the replaces extension for proper completion of the transfer. If the target of the transfer does not support the replaces extension, the Mediatrix 2102 retries 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 is carried out without using the replaces extension.
useReplacesNoRequire	The *Replaces* header is used. It can be seen in the *Refer-To* header of the REFER request sent by the transferor. It can also be seen in the INVITE sent by the transferee. The target that supports Replaces uses its information to merge the new INVITE with an existing call specified in the *Replaces* header. This disables the transfer fallback. The replaces information is still present, but no check is made that it is effectively used to complete the transfer.

Replaces Version

Standards Supported	• sip-replaces-01 draft • sip-replaces-03 draft

You can select the version of the *ietf-sip-replaces* draft to which the Mediatrix 2102 must conform. The provisioned version affects the way blind transfers are executed.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

The Mediatrix 2102 supports the following versions:

Table 112: Replaces Versions Supported

Version	Description
replaces01	When following the *sip-replaces-01* draft, the Transferor can use a REFER with Replaces when proceeding to initiate a blind transfer. This results in the Transferee including a Replaces header in its INVITE to the Transfer Target.
replaces03	When initiating a blind transfer, the Transferor first CANCELs its call with the Target and then issues a REFER without Replaces to the Transferee. **Note**: A side effect of using *replaces03* is that the phone will stop ringing and start again.

▶ **To set the version of Replaces supported:**

1. In the *sipInteropMIB*, set the *sipInteropReplacesVersion* variable with the proper version.
   - replaces01
   - replaces03

Transmission Timeout

Standards Supported	• RFC 2543bis – SIP: Session Initiation Protocol • RFC 3261 – SIP: Session Initiation Protocol

If a DNS SRV answer contains more than one entry, the Mediatrix 2102 will try these entries if the entry initially selected does not work. You can configure the maximum time, in seconds, to spend waiting for answers to messages, from a single source. Retransmissions still follow the algorithm proposed in *RFC 2543bis*, but the total wait time can be overridden by using this feature.

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

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See "MIB Structure" on page 43 for more details.

▶ **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.

SIP Transport Type

Standards Supported	RFC 3261 – SIP: Session Initiation Protocol

You can globally set the transport type for all the lines of the Mediatrix 2102 to either UDP (User Datagram Protocol) or TCP (Transmission Control Protocol). The Mediatrix 2102 will include its supported transports in its registrations.

▶ **To set the transport type:**

1. In the *groupAdminMIB*, set the *groupAdminState* variable to **locked**.

   When in administrative state, all lines are unregistered. This solves the possible problems of registration synchronization and of an active call that uses a transport that was just disabled.
2. In the *sipMIB*, set the priority order of the transport in the *sipTransportQValue* variable.

   A qvalue parameter is added to each contact. This only applies if the transport-specific registration is enabled.

   The qvalue gives each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference.

   The format of the qvalue string must follow the RFC 3261 ABNF (a floating point value between 0.000 and 1.000). If you specify an empty string, no qvalue is set in the contacts.

   Because this variable is located in a table, you can have a different value for each line.
3. Enable the transport by setting the *sipTransportEnable* variable to **enable**.

   The UDP and TCP transport types are located in a table with two rows – one for each type. You can enable/disable a type for the unit.

   If the TCP transport type is not used, Mediatrix strongly suggests to disable it.
4. Enable the transport registration by setting the *sipTransportRegistrationEnable* variable to **enable**.

   The Mediatrix 2102 includes its supported transports in its registrations. It registers with one contact for each transport that is currently enabled. Each of these contacts contains a "transport" parameter.

This is especially useful for a system where there are no SRV records configured to use a predefined transport order for receiving requests. When sending a request, the unit either follows the SRV configuration, or, if not available, any transport parameter received from a redirection or from a configured SIP URL. See “Chapter 6 - DNS SRV Configuration” on page 79 for more details.

Note: If the Mediatrix 2102 has the following configuration:

- the *sipTransportRegistrationEnable* variable is set to **disable**
- the UDP transport type is disabled
- the TCP transport type is enabled

The Mediatrix 2102 will not work properly unless the SIP server uses the TCP transport type by default.

This is also true if the Mediatrix 2102 has the TCP transport disabled and the UDP transport enabled. In this case, the Mediatrix 2102 will not work properly unless the SIP server uses the UDP transport protocol by default.

Transport Parameter

You can define whether the Mediatrix 2102 must include its supported transport in all SIP messages that have the *Contact* header, except for the REGISTER message. See “SIP Transport Type” on page 171 for details on how to include transport parameters in the REGISTER message.

If enabled, then the Mediatrix 2102 will send SIP messages with the “transport” parameter in the *Contact* header set to the currently supported transport type.

▶ **To include the supported transport in the contact header:**

1. In the *sipMIB*, indicate if the unit must include its suported transport in the *Contact* header in the *sipTransportContactEnable* variable.

   Availables values are *enable* and *disable*. If you set the variable to enable, the transport parameter is either set to:

   - *transport=tcp* when TCP is enabled and UDP is disabled
   - *transport=udp* when UDP is enabled and TCP disabled
   - no transport parameter when both TCP and UDP are enabled

UDP Source Port Behaviour

You can configure if the Mediatrix 2102 always uses the same local port (the port on which it is listening for incoming packets) when sending SIP traffic over UDP. This is called symmetric UDP source port. Symmetric UDP ports are sometimes needed to traverse NAT/Firewall devices.

When changing this setting, all destinations are automatically sent out of the penalty box, when applicable.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

▶ **To set the UDP source port behaviour:**

1. In the *groupAdminMIB*, set the *groupAdminState* variable to **locked**.

   You can only change the UDP source port behaviour while the Mediatrix 2102 is in this maintenance mode.

2. In the *sipInteropMIB*, set the *sipInteropSymmetricUdpSourcePortEnable* variable to **enable**.

   The SIP signalling sent over UDP originates from the same port as the port on which the user agent is listening (see “User Agents” on page 163 for details). ICMP messages are not processed, which means that unreachable targets will take longer to detect.

   If you set the variable to **disable**, the SIP signalling over UDP uses a randomly-generated originating port. ICMP errors are processed correctly.

SIP Penalty Box

The penalty box feature is used to "quarantine" a given host which address times out. During that time, the address is considered as "non-responding" for all requests.

This feature is most useful when using multiple servers and some of them are down. It ensures that users wait a minimal period of time before trying a secondary host.

Penalty Box vs Transport Types

Mediatrix recommends to use this feature with care when supporting multiple transports (see "SIP Transport Type" on page 171 for more details) or you may experience unwanted behaviours.

When the Mediatrix 2102 must send a packet, it retrieves the destination from the packet. If the destination address does not specify a transport to use and does not have a DNS SRV entry that configures which transport to use, then the Mediatrix 2102 tries all transports it supports, starting with UDP. If this fails, it tries with TCP. The unit begins with UDP because all SIP implementations must support this transport, while the mandatory support of TCP was only introduced in RFC 3261.

An important fact is that it is not the destination itself that is placed in the penalty box, but the combination of address, port and transport. When a host is in the penalty box, it is never used to try to connect to a remote host unless it is the last choice for the Mediatrix 2102 and there are no more options to try after this host.

Let's say for instance that the Mediatrix 2102 supports both the UDP and TCP transports. It tries to reach endpoint "B" for which the destination address does not specify a transport and there is no DNS SRV entry to specify which transports to use in which order. It turns out that this endpoint "B" is also down. In this case, the Mediatrix 2102 first tries to contact endpoint "B" via UDP. After a timeout period, UDP is placed in the penalty box and the unit then tries to contact endpoint "B" via TCP. This fails as well and TCP is also placed in the penalty box.

Now, let's assume endpoint "B" comes back to life and the Mediatrix 2102 tries again to contact it before UDP and TCP are released from the penalty box. First, the unit tries UDP, but it is currently in the penalty box and there is another transport left to try. The Mediatrix 2102 skips over UDP and tries the next target, which is TCP. Again, TCP is still in the penalty box, but this time, it is the last target the Mediatrix 2102 can try, so penalty box or not, TCP is used all the same to try to contact endpoint "B".

There is a problem if endpoint "B" only supports UDP (RFC 2543-based implementation). Endpoint "B" is up, but the Mediatrix 2102 still cannot contact it: with UDP and TCP in the penalty box, the unit only tries to contact endpoint "B" via its last choice, which is TCP.

The same scenario would not have any problems if the penalty box feature was disabled. Another option is to disable TCP in the Mediatrix 2102, which makes UDP the only possible choice for the unit and forces to use UDP even if it is in the penalty box.

You must fully understand the above problem before configuring this feature. Mixing endpoints that do not support the same set of transports with this feature enabled can lead to the above problems, so it is suggested to either properly configure SRV records for the hosts that can be reached or be sure that all hosts on the network support the same transport set before enabling this feature.

Penalty Box Configuration

The following steps describe how to configure the penalty box feature.

▶ **To set the penalty box feature:**

1. In the *sipMIB*, locate the *sipPenaltyBox* group.
2. Set the amount of time, in seconds, that a host spends in the penalty box in the *sipPenaltyBoxTime* variable.

   Changing the value does not affect IP addresses that are already in the penalty box. The *sipPenaltyBoxTime* only affects new entries in the penalty box.

3. Enable the SIP penalty box feature by setting the *sipPenaltyBoxEnable* variable to **enable**.

   The penalty box is always “active”. This means that even if the feature is disabled, IP addresses are marked as invalid, but they are still tried. This has the advantage that when the feature is enabled, IP addresses that were already marked as invalid are instantly put into the penalty box.

Max-Forwards Header

Standards Supported	RFC 3261 – SIP: Session Initiation Protocol

You can configure whether the Mediatrix 2102 inserts the *Max-Forwards* header into sent requests, as per RFC 3261. Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop. If the Max-Forwards value reaches 0 before the request reaches its destination, it will be rejected with a “483 (Too Many Hops)” error response.

This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

▶ **To insert the Max-Forwards header into SIP requests:**

1. In the *groupAdminMIB*, set the *groupAdminState* variable to **locked**.

   You can only change the *Max-Forwards* header while the Mediatrix 2102 is in this maintenance mode.

2. In the *sipInteropMIB*, set the *sipInteropMaxForwardsValue* variable to the value you want.

   Any positive value means that the *Max-Forwards* header is inserted into sent requests. The default value is **70**.

▶ **To disable inclusion of this header in SIP requests:**

1. In the *groupAdmin* MIB, set the *groupAdminState* variable to **locked**.
2. In the *sipInteropMIB*, set the *sipInteropMaxForwardsValue* variable to **-1**.

Referred-By Field

The SIP REFER method allows the referrer to provide information about the reference to the refer target by using the referee as an intermediary. The mechanism for carrying the referrer's identity, expressed as a SIP URI, is the *Referred-By* header.

You can configure the *Referred-By* field used in a SIP REFER request to decide whether it contains the permanent URL provided by the SIP stack or the address of record used when the unit registered.

▶ **To configure the *Referred-By* field:**

1. In the *sipInteropMIB*, set the *sipInteropReferredByConfig* variable to the value you want.

Table 113: Referred-By Field Parameters

Parameter	Description
useSipStackDefault	The SIP stack populates the *Referred-By* header field.
useLocalUrl	Uses the local URL to populate the *Referred-By* header field.

Direction Attributes in a Media Stream

The Mediatrix 2102 allows you to define various direction attributes pertaining to the media stream.

When Putting a Call on Hold

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

The Mediatrix 2102 can provide the direction attribute and the meaning of the connection address “0.0.0.0” sent in the SDP when an endpoint is put on hold.

See “Call Hold” on page 203 for more details on holding calls.

▶ **To define the direction attribute when putting a call on hold:**

1. In the *sipInteropMIB*, set the *sipInteropOnHoldSdpStreamDirection* variable to the proper value.

Table 114: Direction Attributes

Parameter	Description
inactive	The stream is put on hold by marking it as *inactive*. This is the default value. This setting should be used for backward compatibility issues.
sendonly	The stream is put on hold by marking it as *sendonly*. This method allows the Mediatrix 2102 to be in conformance with RFC 3264.

Direction Attribute

Standards Supported	• RFC 2543 – SIP: Session Initiation Protocol • RFC 3264 – An Offer/Answer Model with Session Description Protocol (SDP)

You can define if the SDP direction attribute is present in the initial INVITE sent by the Mediatrix 2102 and if the direction attribute present in the SDP received from the peer is ignored or not.

▶ **To define if the direction attribute is present:**

1. In the *sipInteropMIB*, set the *sipInteropSdpDirectionAttributeEnable* variable to the proper value.

Table 115: SDP Direction Attribute

Parameter	Description
disable	No direction attribute is present in the SDP sent by the Mediatrix 2102. The Mediatrix 2102 ignores any direction attribute found in the SDP received from the peer. To put an endpoint on hold, a SDP containing a connection address of “0.0.0.0” is sent. The method to put a session on hold is in conformance with RFC 2543.

Table 115: SDP Direction Attribute (Continued)

Parameter	Description
enable	The Mediatrix 2102 always sends the direction attribute in the SDP of the initial INVITE. The initial handshake determines if the peer supports the direction attribute or not. • If the direction attribute is present in the SDP received from the peer, the Mediatrix 2102 sends the direction attribute in the SDP for the remainder of the session. • If the direction attribute is not present in the SDP received from the peer, the Mediatrix 2102 does not send the direction attribute in the SDP for the remainder of the session. If present in the SDP, the direction attribute is preferred over the connection address to transmit session modification information. This method is in conformance with RFC 3264.

Registration Parameters

The following describes registration parameters and behaviours you can configure.

Refreshing Registration

You can refresh the registration, i.e., commit the changes you have done to the registration. When refreshing the registration, all enabled endpoints unregister themselves from the previous registrar and send a new registration to the current registrar with the current parameters.

Variables whose modification require a registration refresh are:

- sipRegistrarStaticHost
- sipRegistrarStaticPort
- sipUAMainUsername
- sipUADisplayName
- sipServerSelectConfigSource
- sipTransportRegistrationEnable
- sipTransportEnable (if sipTransportRegistrationEnable is enabled)
- sipTransportQValue (if sipTransportRegistrationEnable is enabled)

To refresh the registrations:

1. In the *sipMIB*, locate the *sipRegistrationCmdRefresh* variable.

   The following values are available:

   - noOp: No operation.
   - refresh: Refresh registrations.

2. Define the time, in seconds, at which a registered unit begins updating its registration before the registration expiration in the *sipReRegistrationTime* variable.

For instance, if the variable is set to 43 and the registration lasts one hour, the unit will send new REGISTER requests 59 minutes and 17 seconds after receiving the registration acknowledgement (43 seconds before the unit becomes unregistered).

> **Note:** Normally, the Mediatrix 2102 cannot make or receive calls until the REGISTER has completed successfully. Because the timeout for a SIP transaction in UDP is 32 seconds, it is possible to have an ongoing re-REGISTER transaction at the same moment that the registration itself expires. This could happen if *sipReRegistrationTime* is set to a value lower than 32.
>
> In that case, the user agent becomes unregistered, and will become registered again only when the re-REGISTER request is answered with a positive response from the server. See “Unregistered Line Behaviour” on page 140 for a workaround if the unit cannot make calls during that period.

Registration Expiration

The SIP protocol allows an entity to specify the “expires” parameter of a contact in a REGISTER request. The server can return this “expires” parameter in the 200 OK response or select another “expires”. In the REGISTER request, the “expires” is a suggestion the entity makes.

The “expires” parameter indicates how long, in seconds, the user agent would like the binding to be valid.

You can configure the “expires” parameter the Mediatrix 2102 sends.

▶ **To configure the registration expiration:**

1. In the *sipMIB*, set the *sipRegistrationProposedExpirationValue* variable with the suggested expiration delay, in seconds, of a contact in the REGISTER request.

   Available values are from 1 s to 86,400 s (one day).

   This value does not modify the time before a re-REGISTER.

   - The time is the “expires” of the contact in the 200 OK response to the REGISTER request minus the value set in the *sipReRegistrationTime* variable.
   - If the “expires” of the contact in the 200 OK response to the REGISTER is not present or not properly formatted, then the time is the default registration expires minus the value set in the *sipReRegistrationTime* variable.

   See “Refreshing Registration” on page 176 for more details.

   Setting the variable to **0** disables the expiration suggestion.

Default Registration Expiration

Standards Supported	RFC 3261 – SIP: Session Initiation Protocol, section 20.41 (User-Agent)

RFC 3261 specifies that, when the “expires” parameter or the “Expires” header are missing or not properly formatted for a contact of the 200 OK in response to a REGISTER request, the unit must use a default registration expiration value of 3600 s.

You can configure the value of the default registration expiration.

▶ **To configure the default registration expiration:**

1. In the *sipInteropMIB*, set the *sipInteropDefaultRegistrationExpiration* variable with the default registration expiration.

   The delay before a re-REGISTER is the value set in the *sipInteropDefaultRegistrationExpiration* variable minus the value set in the *sipReRegistrationTime* variable. See “Refreshing Registration” on page 176 for more details.

   The recommended value in RFC 3261 (section 10.2) is 3600 seconds.

2. Restart the Mediatrix 2102 so that the changes may take effect.

Local Ring Behaviour on Provisional Response

You can set the Mediatrix 2102 so that it starts or not the local ring upon receiving a “18x Provisional” response without SDP.

This setting does not affect the behaviour when the “18x Provisional” response contains SDP, which allows to establish an early media session before the call is answered.

▶ **To define the local ring behaviour on provisional response:**

1. In the *sipInteropMIB*, set the *sipInteropLocalRingOnProvisionalResponse* variable to the proper value.

Figure 38: Local Ring Behaviour

Parameter	Description
disable	The local ring is not started on a “18x Provisional” response without SDP, except for a “180 Ringing” message. This is the default value. **Note**: Using this default value means you are implementing a behaviour that is different from previous versions of the Mediatrix 2102 application. The 180 Ringing message is a provisional or informational response used to indicate that the INVITE message has been received by the user agent and that alerting is taking place.
enable	The local ring is started on any “18x Provisional” response without SDP.

SIP Credential

You can configure how the Mediatrix 2102 reuses the credential in different transactions of the same call or registration. For instance, it may be required that a new SIP request does not reuse the credential negotiated in the previous transaction of the same call or registration. For example, a re-INVITE will not reuse the credential of the INVITE but will be challenged.

▶ **To enable the Mediatrix 2102 not to reuse the SIP credential:**

1. In the *sipInteropMIB*, set the *sipInteropReuseCredentialEnable* variable to **disable**.

   If you set this variable to **enable** (which is the default value), the Mediatrix 2102 reuses the credential negotiated in previous transactions.

Branch Parameter Settings

The following are settings related to the Branch parameter.

Branch Matching Method

Standards Supported	• RFC 2543 – SIP: Session Initiation Protocol, section 10.1.2 • RFC 3261 – SIP: Session Initiation Protocol, section 8.1.1.7

You can configure the method used to match incoming SIP packets with a branch. A branch could be described as a link that allows to match a response to a request.

▶ **To configure the branch matching method:**

1. In the *sipInteropMIB*, set the *sipInteropBranchMatchingMethod* variable with the proper method to use.

Table 116: Branch Matching Method

Method	Description
rfc2543	Follows the method described in RFC 2543 (section 10.1.2). Responses are mapped to requests by the matching *To*, *From*, *Call-ID*, and *CSeq* headers and the branch parameter of the first *Via* header.
rfc3261	Follows the method described in RFC 3261 (section 8.1.1.7). A *Via* is inserted into the request and the *Via* header field value must contain a branch parameter. This parameter is used to identify the transaction created by that request. It is used by both the client and the server. The branch ID is used to facilitate its use as a transaction ID. It must always begin with the characters "z9hG4bK". If this is not the case, the Mediatrix 2102 uses the branching method as described in RFC 3261, section 17.2.3.

Transaction Matching Procedure

You can configure the use of the *Via* branch behaviour for incoming CANCEL requests. You can specify whether the SIP stack's transaction matching procedure ignores the branch parameter of the *Via* header field in CANCEL requests with no *To* tag.

▶ **To configure the use of the *Via* branch behaviour for CANCEL requests:**

1. In the *sipInteropMIB*, set the *sipInteropIgnoreViaBranchIdInCancelEnable* variable with the proper behaviour.

Table 117: Via Branch Behaviour

Method	Description
disable	The transaction matching procedure behaves according to section 17.2.3 of RFC 3261. This is the default value.
enable	The branch parameter is not used as a transaction matching criterion for CANCEL requests with no *To* tag.

Ringing Response Code

You can configure the response code sent back when the line starts ringing.

▶ **To configure the response code sent back:**

1. In the *sipInteropMIB*, set the *sipInteropRingingResponseCode* variable with the proper code to send back.

Table 118: Ringing Response Code

Method	Description
send180Ringing	The Mediatrix 2102 sends out a “180 Ringing” response without a body. In this case, the ringback the caller hears is generated by his own unit upon receiving the message. This is the default value.
send183WithSdp	The Mediatrix 2102 returns a “183 Session Progress” packet with SDP (needed if the endpoint is required to generate ringback on connection). In this case, the RTP channel is opened earlier to allow the callee’s unit to generate the ringback and send it to the caller.

CHAPTER

16

STUN Configuration

This chapter describes how to configure the STUN client of the Mediatrix 2102.

What is STUN?

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

STUN (Simple Traversal of UDP through NATs) is a simple client / server protocol that uses UDP packets to discover the configuration information of NATs and firewalls between a device and the public Internet:

- NAT type
- NAT binding public address
- NAT binding time to live

NAT (Network Address Translator) is a device that translates the IP address used within a “private” network to a different IP address known in another “public” network. See “NAT Traversal” on page 168 for more details.

STUN supports a variety of existing NAT devices and does not require any additional hardware or software upgrades on the NAT device.

The Mediatrix 2102 uses the STUN protocol to discover its NAT binding for the following three IP addresses/ports (sockets):

- Signalling protocol (SIP) IP address/port
- RTP IP address/port
- T.38 IP address/port

SIP Outbound Proxy

For a unit to work properly behind a firewall, it must keep a pinhole opened by sending keepalive packets through the firewall.

The Mediatrix 2102 only sends keepalive packets to the last destination for a specific socket. When a unit is not configured with an outbound proxy, it can send, through its SIP socket, messages to various destinations, such as a SIP redirect server, another SIP unit, or a MWI server. If, for instance, the last SIP message was sent to the MWI server, the Mediatrix 2102 will keep the pinhole opened for the MWI server only (sending keepalive message to the MWI server) and won't be reacheable by other units outside the firewall.

To avoid those issues, all SIP message should come and go from the same source/destination on the public side of the firewall, i.e., a SIP outbound proxy. Mediatrix thus recommends that you use a SIP outbound proxy. See “Outbound Proxy Server” on page 75 for more details.

Restrictions on the Mediatrix STUN Implementation

- The Mediatrix 2102 does not currently support NAT type discovery.
- The Mediatrix 2102 does not currently support STUN NAT binding time to live discovery.
- The Mediatrix 2102 does not currently support the TLS security mechanism.
- Due to a limitation of most routers, an RTP portal might be required in order for two units behind the same NAT/firewall to be able to communicate with each other.

STUN Client Configuration

The following describes how to configure the Mediatrix 2102 STUN client via SNMP. You can also use the web interface to configure the STUN parameters. See “STUN Page” on page 36 for more details.

▶ **To configure the STUN client:**

1. In the *ipAddressConfig* folder, locate the *ipAddressConfigStunStatic* group.

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

2. Set the static STUN server IP address or Fully Qualified Domain Name (FQDN) in the *stunStaticHost* variable.

The default value is **192.168.0.10**.

3. Set the static STUN server IP port number in the *stunStaticPort* variable.

The default value is **3478**.

4. Set the amount of time, in seconds, the Mediatrix 2102 should keep a STUN query result in its internal cache in the *stunQueryCacheDuration* variable.

Keeping a query in a cache helps to reduce the amount of unnecessary STUN queries when an RTP or T.38 socket is re-used within a short period of time. Available values range from 0 s to 3600 s.

When set to **0**, the cache is disabled and the unit performs a STUN query each time a socket needs to be used.

5. Set the maximum amount of time, in milliseconds, the Mediatrix 2102 should wait for an answer to a STUN query sent to a STUN server in the *stunQueryTimeout* variable.

Available values range from 500 ms to 10000 ms. The default value is 1000 ms.

Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure.

6. Define the interval, in seconds, at which the Mediatrix 2102 sends blank keepalive messages to keep a firewall hole opened in the *stunKeepAliveInterval* variable.

Keepalive messages are used by both the signalling protocol socket and the RTP socket to keep those connections opened through a firewall. Available values range from 0 s to 120 s. The default value is 30 s.

When set to **0**, no keepalive packet is sent.

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

7. Enable the STUN client by setting the *stunEnable* variable to **enable**.

This enables the STUN client for all sockets (VoIP signalling, RTP and T.38) altogether.

The following behaviour also applies:

- If a unit is unable to re-register and there are no ongoing calls, it tries to rediscover its NAT binding for the signalling protocol socket.
- If a STUN server is unresponsive, it is put in a “penalty box” for 60 seconds. See “SIP Penalty Box” on page 173 for more details.

8. Restart the Mediatrix 2102 so that the changes may take effect.

CHAPTER 17

SNTP Settings

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix 2102. It updates the internal clock of the unit, which is the client of a SNTP server. It is required when dealing with features such as the caller ID.

SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport.

Enabling the SNTP Client

Standards Supported	RFC 1769 – Simple Network Time Protocol (SNTP)

You must enable the SNTP client of the Mediatrix 2102 to properly connect to a a SNTP or NTP server.

▶ **To enable the SNTP feature:**

1. In the *sntpMIB*, set the *sntpEnable* variable to **enable**.
2. Set the following synchronization information:

Table 119: SNTP Synchronization Information

Variable	Description
sntpSynchronizationPeriod	Time interval (in minutes) between requests made to the SNTP server. The result is used to synchronize the unit with the time server. The maximum value is set to 1440 minutes (24 hours). **Default Value**: 1440
sntpSynchronizationPeriodOnError	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1440 (24 hours). **Default Value**: 60

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the SNTP server. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

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

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.

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

1. In the *ipAddressConfig* folder, locate the *sntpSelectConfig Source* variable (under the *ipAddressConfigSntp* group).

   This variable defines whether the Mediatrix 2102 must ask for its SNTP server settings through a DHCP server or not.

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

   You can query the SNTP server’s IP address and port number assigned by the DHCP server in the *sntpHost* and *sntpPort* read-only variables (under the *ipAddressStatusSntp* group).

3. Set the DHCP Vendor Specific code of the SNTP feature in your DHCP server.

   See “SNTP” on page 62 for more details.

Static Configuration

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

▶ **To use static information:**

1. In the *ipAddressConfig* folder, locate the *sntpSelectConfig Source* variable (under the *ipAddressConfigSntp* group).

   This variable defines whether the Mediatrix 2102 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 120: SNTP Static Address

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

Defining a Custom Time Zone

Standards Supported	bootp-dhcp-option-88.txt Internet draft

When starting, the Mediatrix 2102 queries a NTP or SNTP server to receive time information. It receives the information in Greenwich Mean Time (GMT) format (also known as Universal Time Coordinated - UTC), so it needs to convert this GMT time into the proper time zone. To do this, the Mediatrix 2102 offers time zone configuration with daylight saving settings.

▶ **To define a custom time zone:**

1. In the *sntpMIB*, enter a valid POSIX (Portable Operating System Interface) string in the *sntpTimeZoneString* variable as defined in the <bootp-dhcp-option-88.txt> Internet draft.

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

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

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

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

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

STD / DST

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

OFFSET

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

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

START / END

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

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

  ```
  M10.4.0
  ```

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

  ```
  M10.5.0
  ```

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

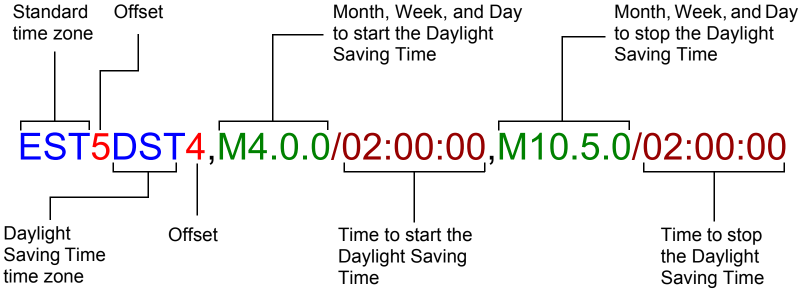
```
M10.1.6
```

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

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

Example

The following is an example of a proper POSIX string:


Standard time zone
Offset
Month, Week, and Day to start the Daylight Saving Time
Month, Week, and Day to stop the Daylight Saving Time
EST5DST4,M4.0.0/02:00:00,M10.5.0/02:00:00
Daylight Saving Time time zone
Offset
Time to start the Daylight Saving Time
Time to stop the Daylight Saving Time

The following are some valid POSIX strings:

Table 121: 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
Central Australia Standard Time	CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
Australia Eastern Standard Time	AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
UTC (Coordinated Universal Time)	UTC0

CHAPTER

18 Digit Maps

This chapter describes how to use a digit map.

Standards Supported	RFC 2705 – Media Gateway Control Protocol (MGCP) Version 1.0, section 3.4 (Formal syntax description of the protocol).

In the *Unit Manager Network Administration Manual*, refer to chapter *Dial Map Parameters*.

What is a Digit Map?

A digit map allows you to compare the number users just dialed to a string of arguments. If they match, users can make the call. If not, users cannot make the call and get an error signal. It is thus essential to define very precisely a digit map before actually implementing it, or your users may encounter calling problems.

Because the Mediatrix 2102 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 enough digits entered from the user to place a call.

Syntax

The permitted digit map syntax is taken from the core MGCP specification, RFC 2705, section 3.4:

```
DigitMap = DigitString  / '(' DigitStringList ')'
DigitStringList = DigitString 0*( '|' DigitString )
DigitString = 1*(DigitStringElement)
DigitStringElement = DigitPosition ['.']
DigitPosition = DigitMapLetter / DigitMapRange
DigitMapLetter = DIGIT / '#' / '*' / 'A' / 'B' / 'C' / 'D' / 'T'
DigitMapRange =  'x' / '[' 1*DigitLetter ']'
DigitLetter ::= *((DIGIT '-' DIGIT ) / DigitMapLetter)
```

Where “x” means “any digit” and “.” means “any number of”.

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

Table 122: 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 2102 with a digit map that corresponds to the dial plan.

A Mediatrix 2102 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 123: 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 the time defined, it is likely that they have finished dialing and the SIP Server can make the call.
x	Matches any digit, excluding “#” and “*”.
|	Indicates a choice of matching expressions (OR).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
[	Indicates the start of a range of characters.
]	Indicates the end of a range of characters.

How to Use a 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
```

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
```

If the number you dial begins with anything other than 2, 3, or 4, the call is not placed and you get a busy signal.

Combining Several Expressions

You can combine two or more expressions in the same digit map by using the “|” operator, which is equal 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]xxxxxx)
```

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: Enclose the digit map in parenthesis when using the “|” option.

Using the # and * Characters

It may sometimes be required that users dial the “#” or “*” to make calls. This can be easily incorporated in a 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. You can specify to remove the “#” or “*” found at the end of a dialed number. See “Setting up Digit Maps” on page 190.

Using the Timer

You can configure the Timer. See “Digit Maps Timeouts” on page 191 for more details. It indicates that if users have not dialed a digit for the time defined, it is likely that they have finished dialing and the Mediatrix 2102 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 2102 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.

Calls Outside the Country

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

```
001x.T
```

In this example, the digit map looks for a number that begins with 001, and then any number of digits after that (x.).

Example

Table 122 on page 187 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

The Mediatrix 2102 validates the digit map as you are entering it and it forbids any invalid value.

Setting up Digit Maps

The variables related to the digit maps are located in tables. You can create/edit ten digit maps for each Mediatrix 2102. Before changing a parameter value, 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 telephone number potentially matches two of the rules, the first rule encountered is applied.

Each of these digit map rules has six specific variables to define for the digit map to work properly.

▶ **To set up digit maps:**

1. In the *digitMapMIB*, define the digit map string that is considered valid when dialed in the *digitMapAllowedDigitMap* variable.

   The string must use the syntax described in "Digit Maps" on page 187. The string format is validated upon entry. Invalid entries are refused. The default value is **x.T**.

2. Define the amount of digits to remove from the beginning of the dialed number, after dialing, but before initiating the call, in the *digitMapPrefixedDigitRemovalCount* variable.

   For instance, when dialing "1-819-xxx-xxxx", specifying a value of "4" means that the call is started by using the number "xxx-xxxx". The default value is **0**.

   This rule is applied BEFORE applying both *digitMapSuffixStringToRemove* (Step 3) and *digitMapPrependedString* (Step 4).

3. Define the string to look for and remove, from the end of the dialed number, in the *digitMapSuffixStringToRemove* variable.

   This is helpful if one of the digit maps contains a terminating character that must not be dialed.

   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 "#", specify "#" in this variable and the resulting number is "25".

   This rule is applied AFTER applying *digitMapPrefixedDigitRemovalCount* (Step 2) but BEFORE applying *digitMapPrependedString* (Step 4).

4. Define the string to insert at the beginning of the dialed number before initiating the call in the *digitMapPrependedString* variable.

   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.

   This rule is applied AFTER applying both *digitMapPrefixedDigitRemovalCount* (Step 2) and *digitMapSuffixStringToRemove* (Step 3).

5. Enable the digit map by setting the *digitMapAllowedEnable* variable to **enable**.

   When enabled, this digit map is recognised and accepted only if it is also valid.

Refused Digit Maps

A refused digit map forbids your users to call specific numbers; for instance, you want to accept all 1-8xx numbers except 1-801. You can create/edit ten refused digit maps for each Mediatrix 2102.

▶ **To set up refused digit maps:**

1. In the *digitMapMIB*, define the digit map string that is considered invalid when dialed in the *digitMapRefusedDigitMap* variable.

   The string must use the syntax described in “Digit Maps” on page 187. The string format is validated upon entry. Invalid entries are refused.

2. Enable the refused digit map by setting the *digitMapRefusedEnable* variable to **enable**.

   When enabled, this digit map is recognised and refused only if it is also valid.

Digit Maps Timeouts

You can define timeouts that apply to the whole unit when dialing a digit map.

▶ **To configure digit map timeouts:**

1. In the *digitMapMIB* (*digitMapTimeouts* group), define the total time the user has to dial the DTMF sequence in the *digitMapTimeoutCompletion* variable.

   The timer starts when the dial tone is played. When the timer expires, the receiver off-hook tone is played.

   This value is expressed in milliseconds (ms). Values range from 1000 ms to 180000 ms. The default value is **60000** ms.

2. Define the time between the start of the dial tone and the receiver off-hook tone, if no DTMF is detected, in the *digitMapTimeoutFirstDigit* variable.

   This value is expressed in milliseconds (ms). Values range from 1000 ms to 180000 ms. The default value is **20000** ms.

3. Define the value of the “T” digit in the *digitMapTimeoutInterDigit* variable.

   The “T” digit is used to express a time lapse between the detection of two DTMFs.

   This value is expressed in milliseconds (ms). Values range from 500 ms to 10000 ms. The default value is **4000** ms.

Digit Map Examples

Digit Map 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 124: Digit Map Rules #1 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	(011x.#|001x.T)
digitMapPrefixedDigitRemovalCount	3 A valid telephone number must contain a country code, an area code, and a number – the “011” part is not required.

Digit Map Rule #2

This digit map rule checks for long distance calls outside your area code.

Table 125: Digit Map Rules #2 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	1xxxxxxxxxx
digitMapPrefixedDigitRemovalCount	1 The first digit “1” in the digit map indicates a user wants to call outside his or her own area code. It must 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 as the code used when the user wants to indicate a communication outside of his or her own area code. It is still good practice to have this number removed and to add the country code, even 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 126: Digit Map Rules #3 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	425xxxxxxx
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 127: Digit Map Rules #4 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	([235-9]xxxxxx|45[1-9]xxxx|4[0-469]xxxxx)
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.

Digit Map Example 2 – PBX Emulation

Let’s say you are located in the 819 area code. You are in an office where you 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 128: 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 129: 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 – the “9011” part is not required.

Digit Map Rule #3

This digit map rule checks for long distance calls outside your area code.

Table 130: 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 or 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 130: Digit Map Rules #3 Settings (Continued)

Variable	Setting
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 as the code used when the user wants to indicate a communication outside of his or her own area code. It is still good practice to have this number removed and to add the country code, even if these two numbers are the same.

Digit Map Rule #4

This digit map rule checks for local calls in the same area code.

Table 131: Digit Map Rules #4 Settings

Variable	Setting
digitMapAllowedEnable	Enable
digitMapAllowedDigitMap	9[2-8]xxxxxx
digitMapPrefixedDigit RemovalCount	1 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).
digitMapPrependedString	1819 (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.

CHAPTER

19

Telephony Features

This chapter explains how to set the telephony variables of the Mediatrix 2102 to define the way the unit handles calls.

Call Processes

The following examples illustrate some of the various calling processes the Mediatrix 2102 supports. These processes can be adapted at will to suit your needs and requirements.

The Mediatrix 2102 can communicate with the following devices:

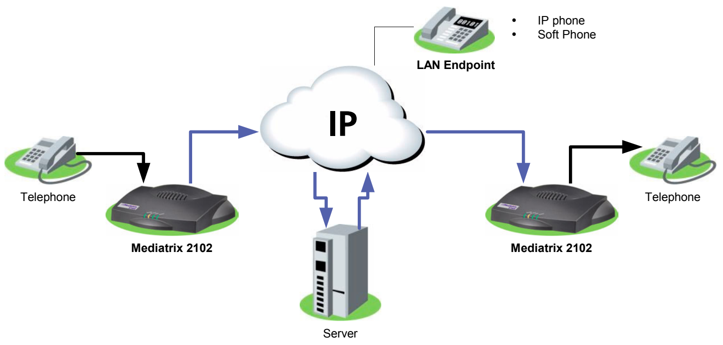
- Another telephone or fax connected to the same Mediatrix 2102.
- Another access device on the IP network such as the Mediatrix 1104 or Mediatrix 1124.
- Any LAN Endpoint on the IP network such as:
  - a Soft Phone
  - an IP phone directly connected to the IP network
- A SCN phone or fax. However, the Mediatrix 2102 would need to contact an analog gateway such as the Mediatrix 1204.

Calls Involving Another Mediatrix 2102

The following example illustrates how to reach a phone or fax on another Mediatrix 2102.

Phone/Fax -> Mediatrix 2102 A -> Mediatrix 2102 B -> Phone/Fax

A user makes a call with the phone/fax connected to a Mediatrix 2102, which in turn contacts another Mediatrix 2102, then reaches the corresponding phone/fax.

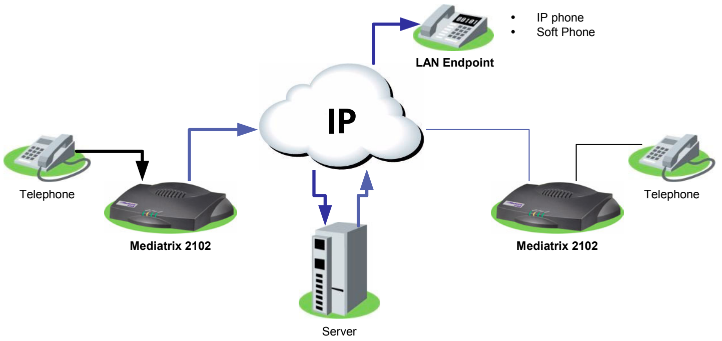


Calls Involving a Mediatrix 2102 and a LAN Endpoint

The following examples illustrate how a phone/fax connected to a Mediatrix 2102 can communicate with a LAN Endpoint on the IP network.

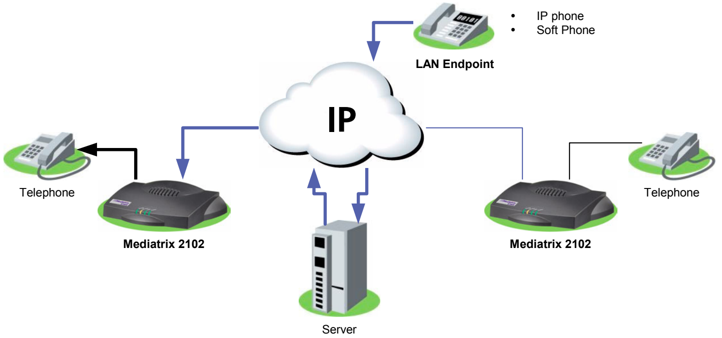
▶ Phone/Fax -> Mediatrix 2102 -> LAN Endpoint

A user makes a call with the phone/fax connected to a Mediatrix 2102, which reaches the corresponding LAN Endpoint on the IP network.



▶ LAN Endpoint -> Mediatrix 2102 -> Phone/Fax

A LAN Endpoint contacts the Mediatrix 2102, which reaches the corresponding phone/fax connected to the Mediatrix 2102.



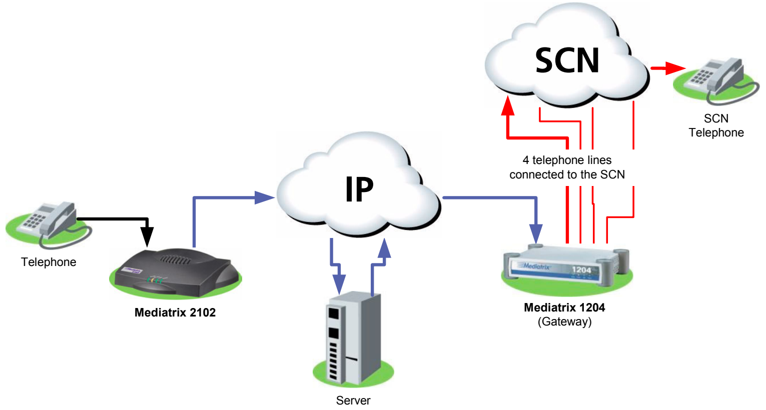
Calls Involving an Analog Gateway

The following example illustrates how a telephone/fax connected to a Mediatrix 2102 and a SCN phone can communicate via an analog gateway.

▶ Phone/Fax -> Mediatrix 2102 -> Mediatrix 1204 (Gateway) -> SCN

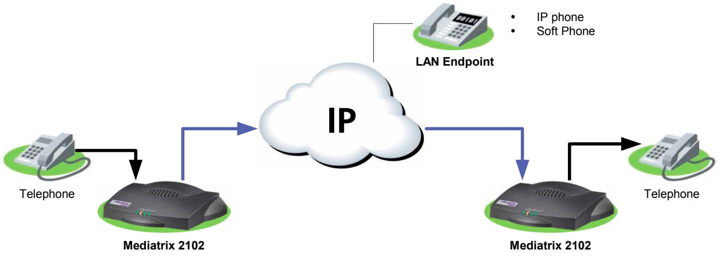
A user makes a call with the phone/fax connected to a Mediatrix 2102, which in turn contacts a Mediatrix 1204 gateway, then reaches the corresponding SCN phone.

A SCN user can also contact the Mediatrix 1204 gateway, which in turn contacts the Mediatrix 2102, then reaches the corresponding phone/fax.



Calls Without a SIP Server

You can dial another unit (gateway or access device) without the help of a SIP Server by entering its IP address.



☞ **Note:** This type of dialing is only possible when the Mediatrix 2102 is configured to allow it. See “IP Address Call Service” on page 218 for more details.

Making Calls

Users with telephones or faxes connected to a Mediatrix 2102 dial as if they were on a standard telephony system.

Complete Dialing Sequence

There are three ways to indicate the dialed number sequence is complete and the Mediatrix 2102 can dial the number:

- The administrator has set up the dialing process so that you must end the telephone number with a particular character to indicate it is complete, e.g., a “#”.
- The administrator has set up the dialing process with a timer. This timer checks the dialing process and, when no further digits have been dialed for the time set by the administrator, it assumes the number is complete and dials it.
- The administrator has set up the Mediatrix 2102 so it knows exactly how many digits it must collect before it places the call. It finds the number of digits to collect by looking at the first few numbers dialed. For example: a telephone number beginning by 1 should be followed by 10 more digits in North America.

Dialing a Telephone Number or Numerical Alias

This section assumes that the Mediatrix 2102 is configured to do SCN emulation. The Mediatrix 2102 could be configured to do any other kind of emulation, thus its users would simply have to dial as if they were using their old system.

▶ **To dial a Standard Call:**

1. Dial the telephone number as if you were using a standard telephone, with country code and area code when required.

   Examples:

   ```
   223
   8298749
   15145701234
   ```

   A Standard Call uses the server to contact the remote dialed user. The server takes the decision about redirecting the call on the SCN or keeping it on the network. Keeping the call on the network takes precedence over redirecting it on the SCN. If the call needs to go on the SCN, the server redirects it to a proper analog gateway (such as the Mediatrix 1204) that will place the call to the SCN network.

☞ **Note:** You can dial one star numbers *xx (such as *69). These numbers are automatically inserted in the Request-URL of the SIP INVITE request.

▶ **To dial a Forced SCN call:**

1. Dial “**”.
2. Dial the telephone number as if you were using a standard telephone, with country code and area code when required.

   Examples:

   ```
   **8298749
   **15145701234
   ```

   A Forced SCN Call allows you to specify that the user you want to reach is located on the SCN network. This leaves no decision to the server; it must find a proper gateway and place the call on the SCN. This option can be useful only when a SCN number is shadowed by a network number.

☞ **Note:** A forced SCN call is only be possible if an analog gateway such as the Mediatrix 1204 is available on the IP network.

Emergency Call

The Emergency Call service (also called urgent gateway) allows a “911”-style service. It allows a user to dial a special digit map resulting in a message being sent to a specified urgent gateway, bypassing any other intermediaries.

If enabled, whenever the user dials the specified digit map, a message is sent to the target address.

▶ **To enable the emergency call service:**

1. In the *emergencyCallMIB*, locate the *emergencyCallUrgentGatewayEnable* variable (under the *emergencyCallUrgentGatewayCustomization* 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 must dial to start the urgent gateway call feature in the *emergencyCallUrgentGatewayDigitMap* 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 follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service's status is “enabled”.

   The activating sequence is set for all the lines of the Mediatrix 2102. You cannot have different sequences for each line.

3. Set the number to reach for an urgent call in the *emergencyCallUrgentGatewayTargetAddress* variable.

   Accepted formats are:

   - telephone numbers (5551111)
   - SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

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

CHAPTER

20

Subscriber Services

The Mediatrix 2102 offers subscriber services users can directly access on their telephone. However, you must set these services before they can be used.

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

In the *Unit Manager Network Administration Manual*, refer to chapter *Subscriber Services Parameters*, section *SIP Configuration Window*.

Call Hold

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

You must enable this service for the following services to work properly:

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

Enabling Call Hold

You must enable this service before your users can use it.

To enable the call hold service:

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Set the *subscriberServicesHoldEnable* variable to **enable**.

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

   You can find the current status of the service in the *subscriberServicesHoldStatus* read-only variable (under the *subscriberServicesIfStatusTable*).

Using Call Hold

The following is the procedure to use this service on the user's telephone.

To put the current call on hold:

1. Perform a Flash-Hook by pressing the "Flash" button on your analog telephone.

   This puts the call on hold. You can resume the call in the same way.

Second Call

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

The call hold service must be enabled for this service to work. See “Call Hold” on page 203.

Enabling Second Call

You must enable this service before your users can use it.

▶ **To enable the second call service:**

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Set the *subscriberServicesSecondCallEnable* variable to **enable**.

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

   You can find the current status of the service in the *subscriberServicesSecondCallStatus* read-only variable (under the *subscriberServicesIfStatusTable*).

Using Second Call

The following is the procedure to use this service on the user’s telephone.

▶ **To use the second call service:**

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold and the second line is automatically connected to your line.
2. Initiate the second call.

Call Forward

The Call Forward service offers various ways to forward calls:

- Unconditional
- On Busy
- On No Answer

Unconditional

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

Setting up Call Forward Unconditional

You must condigure and enable this service before your users can use it.

▶ **To set the Call Forward Unconditional feature:**

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfCallForwardActivationTable* group.

2. Set the status of the service in the *subscriberServicesCallForwardUnconditionalActivation* variable to **inactive** or **active**.

To let the user activate or deactivate this service with his or her handset, proceed to steps 3 and 4. In that case, the variable is automatically updated to reflect the activation status.

3. Define the digits that users must dial to start the service in the *subscriberServicesCallForwardUnconditionalEnableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

For instance, you could decide to put “*70” as the sequence to activate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

The activating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.

4. Define the digits that users must dial to stop the service in the *subscriberServicesCallForwardUnconditionalDisableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

For instance, you could decide to put “*71” as the sequence to deactivate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

The deactivating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.

5. Define the address to which forward incoming calls in the *subscriberServicesCallForwardUnconditionalForwardingAddress* variable.

Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

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

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

6. Enable the Call Forward Unconditional by setting the *subscriberServicesCallForwardUnconditionalEnable* variable to **enable** (under the *subscriberServicesIfEnablingTable* group).

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

Using Call Forward Unconditional

When forwarding calls outside the system, a brief ring is heard on the telephone to remind the user that the call forward service is active. The user can still make calls from the telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to activate the call forward unconditional service.

   This sequence could be something like *70.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.
5. Dial the number to which you want to forward your calls. Dial any access code if required.
6. Wait for three “beeps” followed by a silent pause.

   The call forward is established.
7. Hang up your telephone.

   The calls are checked against the digit maps set up by the system administrator.

▶ **To check if the call forward has been properly established:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial your extension or telephone number.

   The call is forwarded to the desired telephone number.
4. Hang up your telephone.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to deactivate the call forward – unconditional service.

   This sequence could be something like *71.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

   The call forward is cancelled.
5. Hang up your telephone.

On Busy

You can automatically forward the incoming calls of your users to a pre-determined target if they are already on the line. The user does not have any feedback that a call was forwarded.

Setting up Call Forward On Busy

You must configure and enable this service before your users can use it.

▶ **To set the Call Forward On Busy feature:**

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfCallForwardActivationTable* group.
2. Set the status of the service in the *subscriberServicesCallForwardOnBusyActivation* variable to **inactive** or **active**.

   To let the user activate or deactivate this service with his or her handset, proceed to steps 3 and 4. In that case, the variable is automatically updated to reflect the activation status.
3. Define the digits that users must dial to start the service in the *subscriberServicesCallForwardOnBusyEnableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

   For instance, you could decide to put “*72” as the sequence to activate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

   The activating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.
4. Define the digits that users must dial to stop the service in the *subscriberServicesCallForwardOnBusyDisableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

   For instance, you could decide to put “*73” as the sequence to deactivate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

   The deactivating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.
5. Define the address to which forward incoming calls in the *subscriberServicesCallForwardOnBusyForwardingAddress* variable.

   Accepted formats are:

   - telephone numbers (5551111)
   - SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

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

   Because this variable is located in a table, you can have a different string for each line.
6. Enable the Call Forward On Busy by setting the *subscriberServicesCallForwardOnBusyEnable* variable to **enable** (under the *subscriberServicesIfEnablingTable* group).

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

Using Call Forward on Busy

The following is the procedure to use this service on the user’s telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to activate the call forward on busy service.

   This sequence could be something like *72.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.
5. Dial the number to which you want to forward your calls. Dial any access code if required.
6. Wait for three “beeps” followed by a silent pause.

   The call forward is established.
7. Hang up your telephone.

   The calls are checked against the digit maps set up by the system administrator.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to deactivate the call forward on busy service.

   This sequence could be something like *73.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

   The call forward is cancelled.
5. Hang up your telephone.

On No Answer

You can forward the incoming calls of your users to a pre-determined target if they do not answer their telephone before a specific amount of time. The user does not have any feedback that a call was forwarded.

Setting up Call Forward On No Answer

You must configure and enable this service before your users can use it.

▶ **To set the Call Forward On No Answer feature:**

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfCallForwardActivationTable* group.
2. Set the status of the service in the *subscriberServicesCallForwardOnNoAnswerActivation* variable to **inactive** or **active**.

   To let the user activate or deactivate this service with his or her handset, proceed to steps 3 and 4. In that case, the variable is automatically updated to reflect the activation status.
3. Define the digits that users must dial to start the service in the *subscriberServicesCallForwardOnNoAnswerEnableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

   For instance, you could decide to put “*74” as the sequence to activate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

   The activating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.
4. Define the digits that users must dial to stop the service in the *subscriberServicesCallForwardOnNoAnswerDisableDigitMap* variable (under the *subscriberServicesActivationDigitmaps* group).

   For instance, you could decide to put “*75” as the sequence to deactivate the service. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

   The deactivating sequence is set for all the lines of the Mediatrix 2102. You cannot have different sequences for each line.
5. Define the address to which forward incoming calls in the *subscriberServicesCallForwardOnNoAnswerForwardingAddress* variable.

   Accepted formats are:

   - telephone numbers (5551111)
   - SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

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

   Because this variable is located in a table, you can have a different string for each line.
6. Define the time, in milliseconds, the telephone keeps ringing before the call forwarding activates in the *subscriberServicesCallForwardOnNoAnswerTimeout* variable.

   The default value is 5000.
7. Enable the Call Forward On No Answer by setting the *subscriberServicesCallForwardOnNoAnswerEnable* variable to **enable** (under the *subscriberServicesIfEnablingTable* group).

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

Using Call Forward on No Answer

The following is the procedure to use this service on the user’s telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to activate the call forward on no answer service.

   This sequence could be something like *74.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.
5. Dial the number to which you want to forward your calls. Dial any access code if required.
6. Wait for three “beeps” followed by a silent pause.

   The call forward is established.
7. Hang up your telephone.

   The calls are checked against the digit maps set up by the system administrator.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to deactivate the call forward on no answer service.

   This sequence could be something like *75.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

   The call forward is cancelled.
5. Hang up your telephone.

Call Waiting

The call waiting tone indicates to an already active call that a new call is waiting on the second line.

Your users can activate/deactivate the call waiting tone for their current call. This is especially useful when transmitting faxes. The user that is about to send a fax can thus deactivate the call waiting tone to ensure that the fax transmission will not be disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone is automatically reactivated.

Setting up Call Waiting

You must configure and enable this service before your users can use it.

▶ **To set the Call Waiting service:**

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Enable the Call Waiting feature by setting the *subscriberServicesCallWaitingEnable* variable to **enable**.

   This permanently activates the call waiting tone. When receiving new calls during an already active call, a special tone is heard to indicate that a call is waiting on the second line. The user can then answer that call by using the “flash” button. The user can switch between the two active calls by using the “flash” button.

   The call hold service must be enabled for this service to work. See “Call Hold” on page 203.

   If the user is exclusively using faxes, put the variable to **disable** to permanently disable the call waiting tone.

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

   You can find the current status of the service in the *subscriberServicesCallWaitingStatus* read-only variable (under the *subscriberServicesIfStatusTable*).
3. Define the digits that users must dial to disable the Call Waiting tone in the *subscriberServicesCallWaitingCancelDigitMap* variable.

   This allows a user who has call waiting enabled to disable that service on the next call only. If, for any reason, the user wishes to undo the cancel, simply unhook and re-hook the telephone to reset the service.

   For instance, you could decide to put “*76” as the sequence to disable the call waiting tone. This sequence must be unique and follow the syntax for digit maps (see “Chapter 18 - Digit Maps” on page 187). Dialing this digit map does not have any effect unless the service’s status is “enabled”.

   The deactivating sequence is set for all the lines of the Mediatrix 2102. You cannot have a different sequence for each line.

Using Call Waiting

The call waiting feature alerts the user if he or she is already on the telephone and a second call happens. A “beep” (the call waiting tone) is heard and repeated every ten seconds to indicate there is a second incoming call.

▶ **To put the current call on hold:**

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold and the second line is automatically connected to your line.
2. Answer the call on the second line.

▶ **To switch from one line to the other:**

1. Perform a Flash-Hook each time you want to switch between lines.

▶ **To terminate the first call before answering the second call:**

1. Hang up the telephone.
2. Wait for the telephone to ring.
3. Answer the telephone.

   The second call is on the line.

Removing the Call Waiting Tone

You can temporarily activate/deactivate the call waiting tone indicating a call is waiting. This is especially useful when transmitting faxes. If you are about to send a fax, you can thus deactivate the call waiting tone to ensure that the fax transmission is not disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone is automatically reactivated.

▶ **To deactivate the call waiting tone:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence the system administrator has implemented to deactivate the call waiting tone.

   This sequence could be something like *70.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

   The call waiting tone is disabled.

▶ **To re-enable the call waiting tone:**

1. Take the receiver off-hook.
2. Replace the receiver on-hook.

   The call waiting tone is re-enabled.

Call Transfer

The Call Transfer service offers various ways to transfer calls:

- Blind Transfer
- Attended Transfer

The SIP protocol also offers to set transfer-related parameters. See "Call Transfer Capacity" on page 169 and "Referred-By Field" on page 174 for more details.

Blind Transfer

The blind call transfer service is sometimes called Transfer without Consultation or Unattended Transfer. It allows a user to transfer a call on hold to a still ringing (unanswered) call. The individual at the other extension or telephone number does not need to answer to complete the transfer.

The call hold and second call services must be enabled for this service to work. See "Call Hold" on page 203 and "Second Call" on page 204.

Enabling Blind Call Transfer

You must enable this service before your users can use it.

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

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Set the *subscriberServicesBlindTransferEnable* variable to **enable**.

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

   You can find the current status of the service in the *subscriberServicesBlindTransferStatus* read-only variable (under the *subscriberServicesIfStatusTable*).

Using Blind Call Transfer

The following is the procedure to use this service on the user's telephone.

▶ **To transfer a current call blind:**

1. Perform a Flash-Hook by pressing the "Flash" button on your analog telephone.

   This puts the call on hold.
2. Wait for the transfer tone (three "beeps").
3. Dial the number to which you want to transfer the call.
4. Wait for the ringback tone, then hang up your telephone.

   The call is transferred. You can also wait for the third party to answer if you want. In this case, the call transfer becomes attended.

   If you want to get back to the first call (the call on hold), you must perform two Flash-Hooks.

   You are back with the first call and the third party is released.

Attended Transfer

The attended call transfer service is sometimes called Transfer with Consultation. It allows a user to transfer a call on hold to an active call. The individual at the other extension or telephone number must answer to complete the transfer.

The call hold and second call services must be enabled for this service to work. See “Call Hold” on page 203 and “Second Call” on page 204.

Enabling Attended Call Transfer

You must enable this service before your users can use it.

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

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Set the *subscriberServicesAttendedTransferEnable* variable to **enable**.

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

   You can find the current status of the service in the *subscriberServicesAttendedTransferStatus* read-only variable (under the *subscriberServicesIfStatusTable*).

Using Attended Call Transfer

The following is the procedure to use this service on the user’s telephone.

▶ **To transfer a current call attended:**

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold.
2. Wait for the transfer tone (three “beeps”).
3. Dial the number to which you want to transfer the call.

   The third party answers.
4. Hang up your telephone.

   The call is transferred.
5. If you want to get back to the first call (the call on hold), you must perform two Flash-Hooks.

   You are back with the first call and the third party is released.

Note: If the number to which you want to transfer the call is busy or does not answer, quickly perform a Flash-Hook. The busy tone or ring tone is cancelled and you are back with the first call.

Conference Call

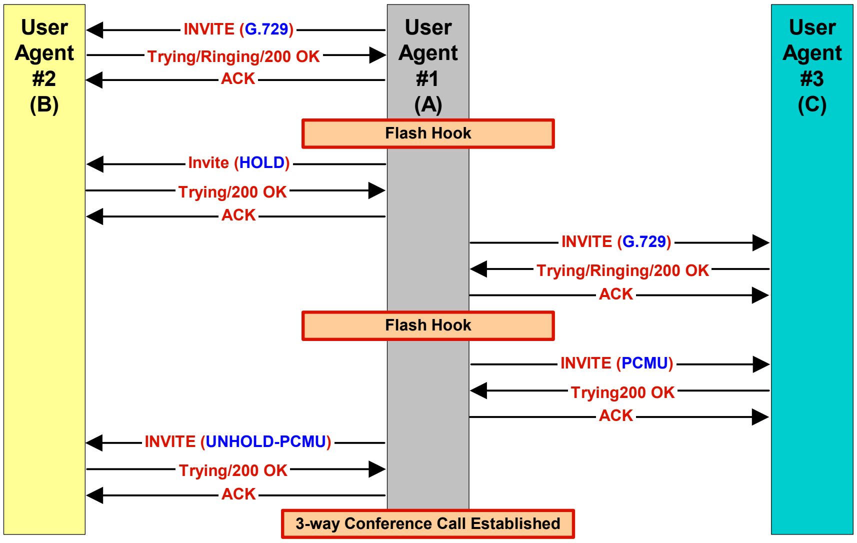
The Conference Call service allows a user to link two or more calls together to form a single conversation, called a conference.

- Only 3-way conferences are currently supported.
- A participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The participant who initiated the conference cannot put it on hold.

You must enable the call hold and second call services for this service to work. See "Call Hold" on page 203 and "Second Call" on page 204.

The following is a conference call flow example:

Figure 39: Conference Call Flow



Requirements

For the conference call to occur successfully, all parties must meet the following requirements:

- Support at least one of the PCM codecs (G.711 µ-law and G.711 A-law) enabled on the line that is having the conference. See "Enabling Individual Codecs" on page 147 for more details.
- Ability to dynamically change codec during a call.
- The packetization period (ptime) should be the same for all the participants of the conference. If this is not the case, then part of the conversation may be lost, resulting in a choppy voice. For better results, Mediatrix recommends to set the packetization period of all participants of a 3-way conference to 30 milliseconds. See "Packetization Time" on page 148 for more information on how to set the packetization period of the Mediatrix 2102.

Enabling the Conference Call Feature

You must enable this service before your users can use it.

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

1. In the *subscriberServicesMIB*, locate the *subscriberServicesIfEnablingTable* group.
2. Set the *subscriberServicesConferenceEnable* variable to **enable**.

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

   You can find the current status of the service in the *subscriberServicesConferenceStatus* read-only variable (under the *subscriberServicesIfStatusTable*).

Managing a Conference Call

If you are on the telephone with one person and want to conference with a third one, you can do so. In the following examples, let's assume that:

- "A" is the conference initiator.
- "B" is the person called on the first line.
- "C" is the person called on the second line.

▶ **To initiate a three-way conference ("A" and "B" already connected):**

1. "A" performs a Flash-Hook.

   This puts "B" on hold and the second line is automatically connected. "A" hears a dial tone.
2. "A" dials "C's" number.

   "A" and "C" are now connected.
3. "A" performs another Flash-Hook.

   The call on hold ("B") is reactivated. "A" is now conferencing with "B" and "C".

▶ **"A" wants to transfer "B" to "C" during the conference:**

1. "A" hangs up.

   The conference is terminated. "B" and "C" are now connected.

▶ **"A" wants to terminate the call with "C" and get back to the call with "B" during the conference:**

1. "A" performs a Flash-Hook.

   The conference is terminated and the call with "C" is disconnected. "A" and "B" are still connected and can go on with their conversation.

▶ **"B" (or "C") hangs up during the conference:**

1. "B" (or "C") hangs up during the conference.

   The conference is terminated, but the call between "A" and "C" (or "B") is not affected and they are still connected.

CHAPTER 21

Telephony Attributes

The telephony attributes are used to configure the characteristics of the telephony system being implemented.

Automatic Call

The automatic call feature allows you to define a telephone number that is automatically dialed when taking the handset off hook.

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

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

▶ **To set the automatic call feature:**

1. In the *telephonyAttributesMIB*, locate the *telephonyAttributesIfFeaturesTable* group.

This group contains all of the variables required to set the automatic call feature.

2. Define the number to dial when the handset is taken off hook in the *telephonyAttributesAutomaticCallTargetAddress* variable.

Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

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

Because this variable is located in a table, you can define a different number for each line of the Mediatrix 2102.

3. Enable the automatic call feature by setting the *telephonyAttributesAutomaticCallEnable* variable to **enable**.

Because this variable is located in a table, you can enable/disable the feature on a per-line basis.

Call Direction Restriction

You can define in which direction calls are allowed.

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

▶ **To set call direction restriction:**

1. In the *telephonyAttributesMIB*, locate the *telephonyAttributesIfFeaturesTable* group.
2. Define the restriction on the direction of traffic in the *telephonyAttributesCallDirectionRestriction* variable.

Table 132: Call Direction Restrictions

Restriction	Description
noRestriction	Allows incoming and outgoing calls.
scnToIpOnly	The Mediatrix 2102 allows to make calls but cannot receive calls.
ipToScnOnly	The Mediatrix 2102 allows to receive calls but does not allow to make calls.

Because this variable is located in a table, you can define a different call direction for each line of the Mediatrix 2102.

IP Address Call Service

The IP address call service allows a user to dial an IP address without the help of a SIP server. Using this method bypasses any server configuration of your unit.

The user can dial an IP address and enter an optional telephone number. Note that the optional telephone number is matched by using the same digit maps as a normal call.

Enabling IP Address Calls

▶ **To enable the IP address call service:**

1. In the *telephonyAttributesMIB*, locate the *telephonyAttributesIpAddressCallCustomization* group.
2. Enable the IP address call service by setting the *telephonyAttributesIpAddressCallEnable* variable to **enable**.

Dialing an IP Address

▶ **To make an IP address call:**

1. Dial “**” (IP address prefix).
2. Dial the numerical digits of the IP address and use the “*” for the “.” of the IP address.
3. Dial “#” to terminate the IP address.
4. Dial the telephone number of the specific line you want to reach.

   For example, let’s say you want to reach the telephone connected to Line 2 of the Mediatrix 2102 with the IP address 192.168.0.23. The phone number assigned to Line 2 of this Mediatrix 2102 is 1234. You must then dial the following digits:

   ```
   **192*168*0*23#1234
   ```

In this case, the Mediatrix 2102 sends an INVITE *1234@192.168.0.23*.

PIN Dialing

Standards Supported	draft-choudhuri-sip-info-digit-00.txt

The PIN Dialing feature allows you to configure a PIN (Personal Identification Number) that would be dialed “n” milliseconds after an outgoing call was established.

This feature could be used in the case where a user makes an automatic call to an IVR system, and after a pre-defined delay, the Mediatrix 2102 sends the DTMF tones (PIN) to indicate where the call is coming from.

The PIN is transmitted by using the DTMF out-of-band by signalling protocol transport type. Both parties involved must thus support the *draft-choudhuri-sip-info-digit-00.txt* draft. The PIN must be negotiated in the call. See “DTMF Transport Type” on page 149 for more details on the DTMF out-of-band by signalling protocol transport type.

▶ **To configure the PIN dialing feature:**

1. In the *pinDialingMIB*, define the PIN to dial in the *pinDialingPin* variable.

   The PIN contains the DTMFs to be dialed. The supported digits are “0123456789*#abcdABCD”. Pause characters “,”, “;”, and “p” are also supported and represent 1 second.

> **Note:** The *draft-choudhuri-sip-info-digit-00.txt* draft does not support the pause characters “,”, “;”, and “p”. This is a proprietary support.

2. Set the delay prior to sending the PIN in the *pinDialingDelay* variable.

   This value is expressed in milliseconds (ms). The default value is 1000 ms.

3. Enable the PIN dialing feature by setting the *pinDialingEnable* variable to **enable**.

CHAPTER 22

Message Waiting Indicator

This chapter explains how to set the Mediatrix 2102 to use the Message Waiting Indicator service.

What is Message Waiting Indicator (MWI)?

The Message Waiting Indicator (MWI) service alerts the user when new messages have been recorded on a voice mailbox.

When the user receives a call and does not answer, the notification mechanism detects this situation and starts the auto attendant. The caller can then leave a message.

After the message is recorded, the server sends a message to the Mediatrix 2102 listing how many new and old messages are available. The Mediatrix 2102 alerts the user of the new message in two different ways:

- The telephone's LED blinks (if present).
- A message waiting stutter dial tone replaces the normal dial tone when the user picks up the first line.

> **Note:** The message waiting state does not affect the Second Line feature. When in an active call, performing a flash-hook to get access to the second line plays the usual dial tone.

Standard MWI Methods

The Mediatrix 2102 supports two MWI methods.

MWI Method #1

Standards Supported	• draft-ietf-sipping-mwi-01.txt (MWI draft) • "Telecordia GR-1401-CORE (Issue 1, June 2000)" specification (visual message indication (LED blinking) • "GR-506-CORE (Issue 1, with Revision 1, November 1996)" specification (message waiting indicator tone)

The Mediatrix 2102 sends SUBSCRIBE requests to the server for each line, unless there is no subscription address defined. The Mediatrix 2102 then waits for NOTIFY requests containing the relevant message waiting information.

▶ To configure the MWI:

1. In the *mwiMIB*, set the notification mechanism server address to which the Mediatrix 2102 subscribes in the *mwiConfigUserSubscriptionAddress* variable.

   This mechanism notifies the Mediatrix 2102 when new messages are available. The address is a SIP URL such as "scheme:user@host". For instance, "sip:user@foo.com".

   Because this variable is located in a table, you can define a different address for each line of the Mediatrix 2102.

2. Define the digits that users must dial to retrieve messages in the *mwiFetchDigitMap* variable.

   Dialing these digits initiates a call to the voice messaging system. For instance, you could decide to put "*50" as the sequence a user must dial to retrieve voice messages. This sequence must be unique and follow the syntax for digit maps (see "Chapter 18 - Digit Maps" on page 187). Dialing this digit map does not have any effect unless the service's status is "enabled".

   The activating sequence is set for all the lines of the Mediatrix 2102. You cannot have different sequences for each line.

3. Set the destination to call to retrieve messages in the *mwiConfigFetchAddress* variable.

   The user typically initiates a call to the voice messaging system, and then uses an auto-attendant to get the messages. Available formats are:

   - telephone numbers (5551111)
   - SIP URLs such as "scheme:user@host". For instance, "sip:user@foo.com".

   This string is used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

   Because this variable is located in a table, you can define a different destination for each line of the Mediatrix 2102.

4. Define the duration, in seconds, of dynamic subscription to a messaging service in the *mwiExpirationTime* variable.

5. Enable the MWI by setting the *mwiConfigActivation* variable to **enable**.

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

> **Note:** The MWI subscription refresh is not supported when the caller ID is DTMF-based, so modifiying the variable *mwiConfigActivation* will have no effect.

▶ **To refresh the MWI subscription:**

1. In the *mwiMIB*, set the *mwiSubscriptionCmdRefresh* variable.

   Available values are:

   - noOp: No operation.
   - refresh: Refresh message waiting subscriptions. All enabled endpoints unsubscribe themselves from the service and re-subscribe by using the current provisioning.

MWI Method #2

Standards Supported	draft-mahy-sip-message-waiting-02.txt (expired) with proprietary modifications

This method does not require any special settings or configuration.

MWI Notify Service

The Mediatrix 2102 offers the possibility to extend some key features to remote extensions located in Branch or Home Offices across the SCN.

This service is available only when using the IP Communication Server v3.1 product as a SIP Redirect server.

For instance, a designated analog voice mail system at a main site can provide voice mail for the home or branch office. The home office user is notified of the message waiting via a message waiting LED on the telephone or a special tone when picking up the telephone.

How does the Service Work?

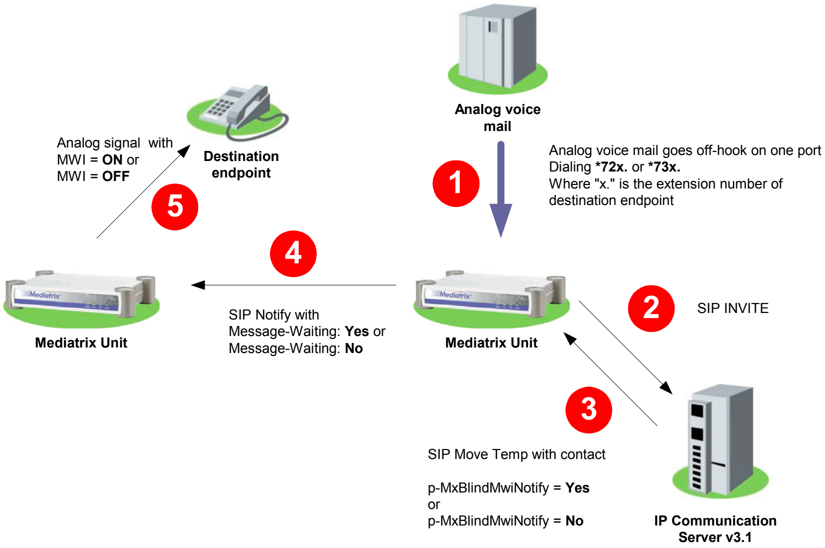
The MWI Notify service is a proprietary feature. In this solution, the analog voice mail system is configured to seize a designated outgoing line and dial a pre-defined string such as “*72xxx” to notify the server it must give a message waiting indication to extension “xxx”. Once voice messages have been retrieved, the analog voice mail system seizes the designated outgoing line and dials a pre-defined string such as “*73xxx” to notify the server to turn off the message waiting indicator for extension “xxx”.

The service uses the Route Manager currently available in the IP Communication Server v3.1 to send a special command to the Mediatrix unit.

The following is the basic sequence of operations for the MWI Notify service:

1. The analog voice mail system dials the following digits:
   `*72101`
   where `*72` is a prefix and `101` the user extension.
2. The Mediatrix unit sends a standard INVITE to the IP Communication Server v3.1 containing the complete dialed string (`*72101`).
   - *a.* The IP Communication Server looks for the registered user “*72101” in the Registrar database.
   - *b.* The IP Communication Server cannot find the user, so it asks the Route Manager to process the request.
   - *c.* Provided that the Route Manager is properly configured, it recognizes the “*72” prefix and associates it to the proper route conditions.
3. The IP Communication Server answers the request with a “Moved Temporarily”. It contains information about the target(s) in the *Contact* header plus a proprietary *p-MxBlindMWINotify=yes/no* field.
   - *a.* The Mediatrix unit retrieves the location from the IP Communication Server’s answer and the *p-MxBlindMWINotify* field.
   - *b.* The Mediatrix unit parses the answer from the IP Communication Server and recognizes *p-MxBlindMWINotify* as a special command.
4. The Mediatrix unit sends a NOTIFY to the location received from the IP Communication Server by using the proper yes or no value (*72 = yes, *73 = no) specified by the route condition.
5. The unit receiving the NOTIFY enables or disables the MWI service for the specified port/user.

Figure 40: Example of the MWI Notify Service



Configuring the IP Communication Server

In the Route Manager of the IP Communication Server, you must configure routes that would be triggered by a pre-defined prefix. The prefix could be any valid digits (DTMF). The example described above uses “*72” to enable the MWI and “*73” to disable the MWI.

For more information on how to configure the Route Manager, please refer to the *IP Communication Server Administration Manual* or the IP Communication Server contextual help.

Configuring the Mediatrix 2102

There is no special unit configuration required. The Mediatrix unit behaves as if in a standard call until it receives one of the following parameters in the *Contact* field:

- p-MxBlindMwiNotify=Yes

  or
- p-MxBlindMwiNotify=No

Upon receiving one of these parameters, the unit sends a NOTIFY to the destination endpoint instead of an INVITE. The sent NOTIFY is compliant with <draft-mahy-sip-message-waiting-02.txt>.

CHAPTER 23

Management Server Configuration

The Management Server is a generic name for a module or software that is used to remotely set up Mediatrix 2102 units. For instance, the Management Server could be the Mediatrix's Unit Manager Network product. See "Unit Manager Network – Element Management System" on page xxv for more details.

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

Using the Management Server

You have the choice of setting up Mediatrix 2102 units directly with a SNMP browser or with the Management Server. If you want to use the Management Server to setup the units, you shall tell these units how to reach the Management Server.

▶ **To use the Management Server:**

1. In the *msMIB*, locate the *msEnable* variable.

   This variable enables the Management Server to remotely manage the Mediatrix 2102.

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

3. Set the Trap retransmission period (*msTrapRetransmissionPeriod* variable) to the desired value.

   The available values range from 10 ms to 604 800 000 ms (1 week). The default value is 60 000 ms.

4. Set the Trap retransmission retry count (*msTrapRetransmissionRetryCount* variable) to the desired value.

   When the retry count is elapsed, the Mediatrix 2102 stops the provisioning sequence. The default value is 10. If this variable is set to -1, then the provisioning sequence never stops. The trap is sent until the Management Server replies.

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the Management Server. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See "Chapter 4 - IP Address and Network Configuration" on page 51 for more details.

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

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

   This variable defines whether the Mediatrix 2102 shall get its Management Server configuration through a DHCP server or not.

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

   You can query the Management Server's IP address and port number assigned by the DHCP server in the *msHost* and *msTrapPort* read-only variables (in the *ipAddressStatus* folder).

3. Set how you want to define the Management Server information in the DHCP server:

Table 133: Management Server DHCP Information

To use a...	Set...
vendor specific code	The *msDhcpSiteSpecificCode* variable to **0**. Set the management server IP address in the DHCP server inside the vendor specific sub-option 200 (hexadecimal 0xC8).
site specific code	The *msDhcpSiteSpecificCode* variable to any value between 128 and 254. Set the management server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *msDhcpSiteSpecificCode* variable in the unit's configuration).

See “Vendor and Site Specific DHCP Options” on page 64 for more details.

Static Configuration

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

▶ **To use static information:**

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

   This variable defines whether the Mediatrix 2102 shall get its Management Server configuration through a DHCP server or not.

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

3. Set the following variables:

Table 134: Management Server Static Address

Variable	Description
msStaticHost	Static management server IP address or domain name. **Default Value**: 192.168.0.10
msStaticTrapPort	Static management server IP port number. Restart the unit to update this parameter. **Default Value**: 162 **Note**: Change the port used in the management server. Not doing so will prevent you from viewing the received traps from the unit. The management server could be a product such as the Unit Manager Network.

CHAPTER

24

Quality of Service (QoS)

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. The Mediatrix 2102 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.

The Mediatrix 2102 supports the Real Time Control Protocol (RTCP), which is used to send packets to convey feedback on quality of data delivery.

The Mediatrix 2102 does not support RSVP (Resource Reservation Protocol).

Differentiated Services (DS) Field

Standards Supported	RFC 2475 – An Architecture for Differentiated Services

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

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

It is the network administrator's responsibility to provision the Mediatrix 2102 with standard and correct values.

Note: If you are using the Mediatrix 2102 in router mode, you may want to differentiate the packets sent by the PC from the packets sent by the Mediatrix 2102. In this case, you must use a substitution value, as described in "Configuring TAS" on page 93.

What are Differentiated Services?

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

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

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

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

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

▶ 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.

Note: RFC 3168 now defines the state in which to set the two least significant bits in the TOS byte. On the other hand, this RFC only applies to TCP transmissions and the bits are thus set to “0” in the Mediatrix 2102. This has the following effects:

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

2. Set the value you want to use.

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

The 802.1q standard comprises the 802.1p standard.

It is the network administrator’s responsibility to provision the Mediatrix 2102 with standard and correct values.

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

1. In the *qosIeee8021q* group of the *qosMIB*, locate the following variables:

- qosSignalingIeee8021qEnable
- qosVoiceIeee8021qEnable
- qosT38FaxIeee8021qEnable
- qosVbdIeee8021qEnable

2. Set the value of these variables to **enable**.

The corresponding user priority configuration is enabled.

3. In the *qosIeee8021q* group of the *qosMIB*, locate the following variables:

- qosSignalingIeee8021qUserPriority
- qosVoiceIeee8021qUserPriority
- qosT38FaxIeee8021qUserPriority
- qosVbdIeee8021qUserPriority

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. Restart the Mediatrix 2102 so that the changes may take effect.

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

VLANs

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

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.

The VLAN field in the Ethernet file is located after both destination and source addresses:

```
 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.

VLAN Substitution

The Mediatrix 2102 can tag the packets relayed from the *Computer* (LAN) port to the *Network* (WAN) port with a VLAN ID different from the standard value defined in "VLAN" on page 230.

> **Note:** This feature only works when TAS is disabled. See "Chapter 8 - Transparent Address Sharing" on page 87 for more details.

In this case, the packets coming from the LAN (usually a router or a PC) are tagged with a substitution VLAN ID before sending the packets to the WAN. In the opposite direction, the Mediatrix 2102 removes the VLAN tags and then send the packets to the LAN. The packets generated by the Mediatrix 2102 for VoIP/Signaling/ Management can also be tagged with a different VLAN ID.

This can be used to prioritize VoIP in a network.

▶ **To configure the VLAN substitution:**

1. In the *qosIeee8021qSubstitution* group of the *qosMIB*, define the substitution IEEE 802.1Q Virtual LAN ID in the *qosVlanIeee8021qSubstitutionVlanID* variable.

   The value 1 is the default Port VID (PVID) for bridge port. The 4095 VID (0xFFF) is reserved for implementation use and it must not be used in the tag header.

   As per the standard, some bridges may not support the full range of VID.

2. Set the substitution IEEE 802.1Q Virtual LAN default user priority in the *qosVlanIeee8021qSubstitutionUserPriority* variable.

   This value applies to all protocols for which no priority filtering is enabled (e.g. ARP, ICMP).

   - 7 = High priority
   - 0 = Low priority

3. Enable the VLAN substitution by setting the *qosVlanIeee8021qSubstitutionEnable* variable to **enable**.

   The QoS 802.1q fields of the packets sent from the PC to the WAN are assigned the value defined in the *qosVlanIeee8021qSubstitutionVlanID* variable.

4. Restart the Mediatrix 2102 so that the changes may take effect.

Ethernet Frames Issue

There is currently an issue with the CPU of the Mediatrix 2102. This issue prevents Ethernet frames, which have a 802.1q tag, to be correctly forwarded through the *Computer* (LAN) port of the Mediatrix 2102, if these frames have less than 68 bytes (including FCS).

For example, it is valid to have an Ethernet frame of 64 bytes, even if it includes a 802.1q tag. However, when the CPU switch forwards this packet through the *Computer* port, it removes the 802.1q tag, but does not add any padding byte. The Ethernet frame is output with only 60 bytes, which is invalid and dropped by most equipment.

A workaround would be to modify the behaviour of your router to generate 802.1q frames with at least 68 bytes.

CHAPTER 25

Syslog Daemon

This chapter describes how to configure and use the Syslog daemon.

Syslog Daemon Configuration

Standards Supported	RFC 3164 – The BSD Syslog Protocol

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from the Mediatrix 2102 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 2102, you can monitor each step of the software download phase. Furthermore, if the unit encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.

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

▶ **To enable the Syslog daemon:**

1. In the *syslogMIB*, locate the *syslogMsgMaxSeverity* variable.

This variable indicates which syslog message is processed. Any syslog message with a severity value greater than the selected value is ignored by the agent.

- disabled
- critical
- error
- warning
- informational
- debug

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

The following are some of the messages the unit sends:

Table 135: Syslog Messages Examples

Event	Level	Message
The configuration update with the specific configuration file has been successful (configuration file fetching)	Informational	`The specific configuration update succeeded.`
The configuration update with the specific configuration file experienced an error and has not been completed (configuration file fetching)	Error	`The specific configuration update failed.`
The software update has been successful	Informational	`The software update succeeded.`
The software update experienced an error and has not been completed	Error	`The software update failed.`

Configuration Source

The Mediatrix 2102 must know the IP address and port number of the Syslog server. You can assign these information to the Mediatrix 2102 through a DHCP server or manually enter them yourself with the static variables.

DHCP Configuration

Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. See “Chapter 4 - IP Address and Network Configuration” on page 51 for more details.

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

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

   This variable defines whether the Mediatrix 2102 shall ask for its Syslog daemon settings through a DHCP server or not.

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

   You can query the Syslog daemon’s IP address and port number assigned by the DHCP server in the *syslogHost* and *syslogPort* read-only variables (under the *ipAddressStatus Syslog* group of the *ipAddressStatus* folder).

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

Table 136: Syslog DHCP Information

To use a...	Set...
vendor specific code	The *syslogDhcpSiteSpecificCode* variable (under the *ipAddressConfigSyslogDhcp* group) to **0**. Set the Syslog server IP address in the DHCP server inside the vendor specific sub-option 110 (hexadecimal 0x6E).
site specific code	The *syslogDhcpSiteSpecificCode* variable (under the *ipAddressConfigSyslogDhcp* group) to any value between 128 and 254. Set the Syslog server IP address in the DHCP server inside the site specific option you have chosen (it must match the value of the *syslogDhcpSiteSpecific Code* variable in the unit's configuration).

See “Vendor and Site Specific DHCP Options” on page 64 for more details.

Static Configuration

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

▶ **To use static information:**

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

   This variable defines whether the Mediatrix 2102 shall ask for its Syslog daemon settings through a DHCP server or not.

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

3. Set the following variables:

Table 137: Syslog Daemon Static Address

Variable	Description
syslogStaticHost	Syslog server static IP address or domain name. **Default Value**: 192.168.0.10
syslogStaticPort	Syslog server static IP port number. **Default Value**: 514

Customizing Syslog Messages

You can display additional information in the prefix of syslog messages the Mediatrix 2102 sends. This allows you to later filter the messages. The following is the additional information you can enable:

- MAC address
- local time
- local host

> **Note:** This applies only to syslog messages sent on the network and not the local syslog messages.

▶ **To add the MAC address of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayMacAddress* variable to **enable**.

   The MAC address of the Mediatrix 2102 is part of the prefix for all syslog messages.

   If you set the variable to **disable**, the MAC address is not displayed in the prefix of the syslog messages.

▶ **To add the local time of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayTime* variable to **enable**.

   The current local time of the Mediatrix 2102 is part of the prefix for all syslog messages.

   If you set the variable to **disable**, the time is not displayed in the prefix of the syslog messages.

▶ **To add the local host of the unit in the syslog messages:**

1. In the *syslogMIB*, set the *syslogMsgDisplayLocalHost* variable to **enable**.

   The current local host of the Mediatrix 2102 is part of the prefix for all syslog messages.

   If you set the variable to **disable**, the local host is not displayed in the prefix of the syslog messages.

Configuring the Syslog Daemon Application

You shall configure the Syslog daemon to capture those messages. Refer to your Syslog daemon’s documentation to learn how to properly configure it to capture messages.

Local Syslog

The local syslog is an internal syslog server to the Mediatrix 2102. It keeps the last *n* syslog messages. These syslog messages are displayed in the *System log* page of the web interface (see “Chapter 2 - Web Interface” on page 25 for more details).

▶ **To set the local syslog:**

1. In the *syslogMIB*, locate the *syslogMsgLocalMaxSeverity* variable.

   This variable indicates which syslog message is processed by the Mediatrix 2102. Any syslog message with a severity value greater than the selected value is ignored.

   - disabled
   - critical
   - error
   - warning
   - informational
   - debug

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

   The following are some of the messages the unit sends:

   Table 138: Syslog Messages Examples

Event	Level	Message
The configuration update has been successful (configuration file fetching)	Informational	`The specific configuration update succeeded.`
The configuration update experienced an error and has not been completed (configuration file fetching)	Error	`The specific configuration update failed.`
The software update has been successful	Informational	`The software update succeeded.`
The software update experienced an error and has not been completed	Error	`The software update failed.`

2. Set the maximal number of syslog messages the Mediatrix 2102 handles in the *syslogMsgLocalMaxNbr* variable.

   Modifying this value resets the messages.

   If the Mediatrix 2102 sends a new syslog message and the maximum number of messages is reached, the oldest one is removed.

   You can view the syslog messages in the following locations:

   - In the *syslogLocalMsgTable* of the *syslogMIB.*
   - In the *System log* page of the web interface.

CHAPTER 26

Statistics

The Mediatrix 2102 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
- Minimum, maximum and average Jitter interarrival time (time, in milliseconds, between the arrival of packets)
- Minimum, maximum and average latency time

These statistics are located under the *rtpStats* group of the *rtpMIB*. See the *MIB Reference* manual for more details.

Statistics Buffers

Each statistics has three different buffers in which they are collected:

Table 139: Statistics Buffers

Statistic	Description
Last connection	These are the statistics of the last completed connection.
Current	These are the statistics of the current connection. If using the Cumulated buffer, they are added to the cumulated statistics buffer and then reset.
Cumulated	These are the cumulated statistics of all the connections. Define a period of time and maximum number of periods you want to keep. For instance, you could define to keep the statistics for the last 24 periods of 1 hour.

How are Statistics Collected?

When collecting statistics, you can do so in two ways:

- Continuous collection of statistics.

  In this case, the cumulated statistics are not used (disabled) and the current statistics are constantly updated.
- Collection of statistics for a defined period of time with a user-defined accuracy.

  For instance, you could define to keep the statistics for the last 24 periods of 1 hour.

To set statistics collection:

1. In the *sysConfigMIB*, locate the *sysConfigStats* group.
2. Set the period length you want to keep in the *sysConfigStatsPeriodLength* variable.

   The length of a period may vary from 5 minutes to 24 hours, by 5-minutes sections. At expiration, the current statistics are added to the cumulated statistics buffer and then reset. Note that modifying the value of this variable resets statistics to 0.

3. Set the maximum number of periods to cumulate in the *sysConfigStatsNumberPeriods* variable.

   The maximum number of periods cumulated is 24. If this variable is set to 0, statistics are collected indefinitely in the current variables. Note that modifying the value of this variable resets statistics to 0.

▶ **To reset statistics:**

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

   This resets all cumulated call statistics.

Statistics by Syslog

You can configure the Mediatrix 2102 to send the RTP and T.38 statistics by syslog message. You will thus be able to see them by using your syslog daemon.

- The RTP statistics are sent at the end of a call.
- The T.38 statistics are sent at the end of a fax.

The syslog message level is “informational” and uses the module name “Statistics”. Table 140 lists the different statistics fields to send.

Table 140: Statistics by Syslog

Short Name	Description	Corresponding MIB Variable
TxByte	Number of octets transmitted.	rtpStatsLastConnNumberOctetsTransmitted
RxByte	Number of octets received.	rtpStatsLastConnNumberOctetsReceived
TxPkt	Number of packets transmitted.	rtpStatsLastConnNumberPacketsTransmitted
RxPkt	Number of packets received.	rtpStatsLastConnNumberPacketsReceived
NbrPktLost	Number of packets lost.	rtpStatsLastConnNumberPacketsLost
PctPktLost	Percentage of packets lost.	rtpStatsLastConnPercentPacketsLost
JitMin	Minimum interarrival time in milliseconds.	rtpStatsLastConnInterarrivalJitterMin
JitMax	Maximum interarrival time in milliseconds.	rtpStatsLastConnInterarrivalJitterMax
JitAvg	Average interarrival time in milliseconds.	rtpStatsLastConnInterarrivalJitterAvg
LatMin	Minimum latency in milliseconds.	rtpStatsLastConnLatencyMin
LatMax	Maximum latency in milliseconds.	rtpStatsLastConnLatencyMax
LatAvg	Average latency in milliseconds.	rtpStatsLastConnLatencyAvg

The syslog message sent will have the following format:

```
RTP TxByte:<TxByte>, RxByte:<RxByte>, TxPkt:<TxPkt>, RxPkt:<RxPkt>,
NbrPktLost:<NbrPktLost>, PctPktLost:<PctPktLost>, JitMin:<JitMin>,
JitMax:<JitMax>, JitAvg:<JitAvg>, LatMin:<LatMin>, LatMax:<LatMax>,
LatAvg:<LatAvg>
```

Example with the syslog message prefix:

```
Dec 31 19:15:05 10.2.130.31 Statistics [0073] RTP TxByte:32002, RxByte:24514,
TxPkt:156, RxPkt:140, NbrPktLost:0, PctPktLost:0, JitMin:0, JitMax:6, JitAvg:3,
LatMin:8, LatMax:8, LatAvg:8
```

▶ **To enable to send statistics by syslog:**

1. In the *sysConfigMIB*, set the *sysConfigStatsBySyslogEnable* variable to **enable**.

Example

The following is an example with *sysConfigStatsNumberPeriods* = 3 and *sysConfigStatsPeriodLength* = 1 (5 minutes).

Table 141: Statistics Setting Example

Statistics	5-minutes sections					
	1	**2**	**3**	**4**	**5**	**6**
rtpStatsCurrentTotalOctetsTransmitted	50	30	60	40	100	50
rtpStatsCumulatedTotalOctetsTransmitted	0	50	80	140	130	200

1. 50 total octets transmitted in the first 5-minutes period.
2. 30 total octets transmitted in the second 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 50.
3. 60 total octets transmitted in the third 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 80.
4. 40 total octets transmitted in the fourth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable for a cumulated total octets transmitted of 140.
5. 100 total octets transmitted in the fifth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable.

   In the above example, the *rtpStatsCumulatedxx* variables always contain the statistics for the last 15 minutes (*sysConfigStatsNumberPeriods* X *sysConfigStatsPeriodLength*) accurate to 5 minutes (*sysConfigStatsPeriodLength*). This means that the statistics for the first 5-minutes period are dropped, for a cumulated total octets transmitted of 130.
6. 50 total octets transmitted in the sixth 5-minutes period. The previous statistics are transferred to the corresponding cumulated statistics variable.

   The statistics for the second 5-minutes period are dropped, for a cumulated total octets transmitted of 200.

CHAPTER 27

Maximum Transmission Unit (MTU)

This chapter describes the MTU (Maximum Transmission Unit) requirements of the Mediatrix 2102.

What is MTU?

The *Maximum Transmission Unit* (MTU) is a parameter that determines the largest packet than can be transmitted by an IP interface (without it needing to be broken down into smaller units). Each interface used by TCP/IP may have a different MTU value specified.

The MTU should be larger than or equal to the largest packet you wish to transmit unfragmented. Note that this only prevents fragmentation locally. Some other link in the path may have a smaller MTU: the packet will be fragmented at that point, although some routers may refuse packets larger than their MTU.

Mediatrix 2102 MTU

The Mediatrix 2102 MTU is 1500 bytes, which is the Ethernet typical value.

Possible Hardware Problem

The implementation of the IEEE Standard 802.1q in the Mediatrix 2102 may have a minor problem because of hardware limitations.

802.1q increases the Ethernet frame header by 4 bytes, adding a Virtual LAN ID and a user_priority. This is useful to limit broadcasts that cross bridges, and it may also prioritize frames in the queuing algorithm of switches. However, it also increases the maximum possible size of Ethernet frames from 1518 to 1522 bytes, and this might not be handled adequately by every hardware.

A workaround is available for PCs running Windows to avoid sending 1522 bytes packets (note that this happens only in special and rare cases). The workaround is to reduce the MTU of the interface (the one that sends packets with 802.1q framing) by 4 bytes.

1. Use the registry editor (regedt32) and go to the key:

   Windows 2000 and later:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
   <ethernet adapter>
   ```

   Windows NT4 and 98:

   ```
   \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<ethernet
   adapter>\Parameters\Tcpip
   ```

   where <Ethernet adapter> can be found by using the command “ipconfig /all”.

2. Add (or modify) a value named MTU of type REG_DWORD. Set it to 1496 (instead of 1500), in decimal. Restart the computer to have those changes in effect.

   In Windows 2000 and later this value is under the following key:

   - Key: *Tcpip\Parameters\Interfaces\ID* for Adapter2

- Value Type: REG_DWORD Number
- Valid Range: 68 - the MTU of the underlying network
- Default: 0xFFFFFFFF
- Description: This parameter overrides the default MTU for a network interface. The MTU is the maximum packet size in bytes that the transport will transmit over the underlying network. The size includes the transport header. Note that an IP datagram may span multiple packets. Values larger than the default for the underlying network will result in the transport using the network default MTU. Values smaller than 68 will result in the transport using an MTU of 68.

3. To validate that the changes are correct, try to ping the Mediatrix 2102 with large packets once restarted:

```
ping -l 2000
```

This will cause IP fragmentation, the first fragment being as large as the interface allows it. With the MTU reduced, you should now receive an answer. For more informations, see:

http://support.microsoft.com/default.aspx?scid=kb;en-us;120642.

CHAPTER 28

Troubleshooting

You can experience some problems when connecting the Mediatrix 2102 to the network. The following section examines some of these problems and possible solutions.

A Syslog message lists the problems the Mediatrix 2102 encounters. You can see this message with the Syslog daemon.

This chapter covers the following types of issues:

- General Operation Issues
- Calling Issues
- Fax Issues
- Configuration Issues
- Software Upgrade Issues
- SNMP Management Software Issues

General Operation Issues

The following are general operation issues you may encounter.

DESCRIPTION: Unit does not operate – All LEDs are OFF.

POSSIBLE CAUSE: Power is not fed to the unit.

SOLUTION: Check that:

- The power cord is connected to the electrical outlet.
- The power cord is fully inserted into the Mediatrix 2102 power socket.

DESCRIPTION: There is a long delay when starting the Mediatrix 2102.

POSSIBLE CAUSE: If any information is set to come from the DHCP server (for example, SNTP address), the restarting unit waits for a maximum period of two minutes if the DHCP server cannot be reached, even if most other settings are set to “static”.

This delay is caused by the Mediatrix 2102 that cannot function as configured if part of its configuration (the DHCP information) is unavailable.

The two minutes waiting period is an issue with switches that use the Spanning Tree Protocol. When this protocol is enabled, the restarting Mediatrix 2102 may be denied from the network for a certain time (about two minutes). The unit must not ignore transmission errors (i.e., timeouts) because these errors might be caused by the Spanning Tree Protocol.

SOLUTION: Mediatrix recommends to set up all information to use a static value, or have a DHCP server answer the requests. See “Static Configuration” on page 54 for more details.

DESCRIPTION: I changed the IP address of my unit, but I can’t reach the DHCP server anymore.

POSSIBLE CAUSE: A subnet mask is used to determine to which subnet an IP address belongs. An IP address has two components, the network address and the host address. For example, let’s consider the IP address 192.168.0.1. Assuming this is part of a Class B network, the first two numbers (192.168) represent the Class B network address, and the second two numbers (0.1) identify a particular host on this network.

Let’s say you have the following information:

- Mediatrix 2102 IP address: 192.168.0.1
- Subnet Mask: 255.255.0.0 (Class B)
- DHCP Server IP address: 192.168.0.20

If you happen to change the Mediatrix 2102 IP address to 192.169.0.1, for instance, the subnet mask is still valid, but cannot reach your DHCP server anymore. Refer to subnet mask documentation for more details.

DESCRIPTION: Unable to reach the Mediatrix 2102 after changing the Ethernet speed at run-time.

POSSIBLE CAUSE: Some hubs cannot adapt completely their port speed at run-time.

SOLUTION: Always restart the Mediatrix 2102 for the new setting to take effect. See “Ethernet Connection Speed” on page 69 for more details.

DESCRIPTION: In the case where my NAT/Firewall device is connected to the *Computer* port of the Mediatrix 2102 and I have a PC connected to the NAT/Firewall, the PC has limited web access in time.

POSSIBLE CAUSE: The NAT/Firewall device does not support well the small DHCP lease time of the Mediatrix 2102 (30 seconds).

SOLUTION: Modify the *ipRoutingDhcpServerLeaseTime* variable with a value greater than 30 seconds, for instance 3600 seconds (1 hour). See “Enabling TAS” on page 98 for more details.

However, note that the downtime will be greater when the ISP gives another IP address. Try several values and find out what is the smallest setting for your NAT/firewall device.

DESCRIPTION: The Bypass feature does not activate if the SIP proxy times out when a call is initiated.

POSSIBLE CAUSE: In SIP, there is no direct correlation between the user agent and the proxy. The user agent may be able to complete outgoing calls without the help of the server, and may also receive calls as well. The problem is thus normal. The SIP proxy going down is rather a network setup problem.

SOLUTION: To avoid those types of failures, the network should use redundant servers when possible.

DESCRIPTION: The PC connected to the *Computer* connector of the Mediatrix 2102 cannot register to IGMP services.

POSSIBLE CAUSE: The Mediatrix 2102 does not support the IGMP (Internet Group Management Protocol) protocol.

SOLUTION: There are no solutions.

DESCRIPTION: When I install a Mediatrix 2102 in an enterprise network and there is a PC connected to the *Computer* port, the PC will not receive the WINS Server.

- **POSSIBLE CAUSE**: The embedded DHCP server of the Mediatrix 2102 does not support the WINS Server. See “DHCP Server” on page 101 for more details.

  SOLUTION: Disable the TAS feature as described in “Enabling TAS” on page 98 because the IP address is not an issue in private networks.

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

- **POSSIBLE CAUSE**: You cannot disable the adaptative jitter buffer on the Mediatrix 2102.

  SOLUTION: If you set the *voiceIfTargetJitterBufferLength* and *voiceIfMaxJitterBufferLength* variables to the same value, you will have a non-adaptative jitter buffer. See “Adaptative Jitter Buffer” on page 152 for more details.

Calling Issues

The following are general calling issues you may encounter.

DESCRIPTION: Impossible to make a call.

If the following happens:

- Dial tone present.
- Power LED lit.
- LAN LED lit.

POSSIBLE CAUSE: Network communication is not working.

SOLUTION: Check that:

- The LAN cable is securely connected to the Mediatrix 2102 and to the network connector.
- You did not connect a crossover network cable.

POSSIBLE CAUSE: Configurable parameters of the Mediatrix 2102 are not set properly.

SOLUTION: Refer to this manual for a complete description of the configurable Mediatrix 2102 parameters.

DESCRIPTION: Cannot make or receive calls.

POSSIBLE CAUSE: There may be calls that have not been properly terminated, which causes a “leak” in the system.

SOLUTION: You can enable the SIP Context Snapshot time feature. This feature is used to find if there are improperly terminated calls. This could help to debug the system.

a. In the *syslogMIB*, set the *syslogMsgMaxSeverity* variable to **debug**.

b. Configure and enable the syslog feature.

c. In the *sipDebugMIB*, set the time, in minutes, between snapshots in the *sipDebugContextSnapshotTime* variable.

The list of contexts currently in use are periodically output as debug-level syslog messages. Note that enabling this feature will also trigger an instant snapshot.

To disable the feature, set this variable to zero (0).

Note that this feature will generate more syslog traffic, about 20 messages at each x minutes.

Note: This feature is currently located under the *mediatrixExperimental* branch of the MIB structure. See “MIB Structure” on page 43 for more details.

POSSIBLE CAUSE: It is possible that the unit is refreshing its registration and has entered a race condition between the refresh and the SIP timeouts. Normally, the Mediatrix 2102 cannot make or receive calls until the REGISTER request has completed successfully. Because the timeout for a SIP transaction in UDP is 32 seconds, it is possible to have an ongoing re-REGISTER transaction at the same moment that the registration itself expires. This could happen if the *sipReRegistrationTime* variable is set to a value lower than 32. In that case, the user agent becomes unregistered, and will become registered again only when the re-REGISTER request is answered with a positive response from the server.

SOLUTION: Set the *sipUnregisteredPortBehavior* variable to **enablePort**. This way, when an endpoint is not registered, it is still enabled. The user can receive and initiate calls. See “Unregistered Line Behaviour” on page 154 for more details. See also “Refreshing Registration” on page 176 for more details on the re-registration feature.

DESCRIPTION: When making a 3-way conference, part of the conversation is lost, resulting in a choppy voice.

- **POSSIBLE CAUSE**: The packetization period (ptime) is not the same for all the participants of the conference, which causes the choppy voice issue.

  SOLUTION: For better results, Mediatrix recommends to set the packetization period of all participants of a 3-way conference to 30 milliseconds. See "Packetization Time" on page 148 for more information on how to set the packetization period of the Mediatrix 2102.

DESCRIPTION: Unable to establish a call from the Mediatrix 2102 to a user agent such as an IP phone, a gateway or another access device.

- **POSSIBLE CAUSE**: When the Mediatrix 2102 – with its T.38 capability enabled – tries to establish a call with a 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 2102. See "T.38 Fax" on page 159 for more details.

Fax Issues

The following gives information pertaining to faxes. This includes a list of fax models tested with the Mediatrix 2102 and some specific issues the unit may encounter.

DESCRIPTION: "Poor line condition" error during a fax transmission.

- **POSSIBLE CAUSE**: The analog transmission between the fax machine and the Mediatrix 2102 is flaky, preventing the fax transmission to terminate properly. This problem is known to occur with some fax machines and it can also occur with a few fax modems.

  SOLUTION: Set the *Input sound level* to **-6 dB**. If this still does not solve the problem, try the **+6 dB** value. See "User Gain" on page 156 for more details.

DESCRIPTION: Unable to send a fax in T.38 and Clear Channel.

- **POSSIBLE CAUSE**: To properly send faxes, both units must be configured with the same settings. If you are attempting to send a fax and the transmission fails, there could be many reasons for this, but most likely the fax codec settings are at fault. The following explains the logic behind fax transmissions.

  When transmitting a fax, Unit A first verifies if Unit B supports the codec you have set in Unit A. If the codec is supported, the fax should be transmitted properly.

  If the fax codec is not supported by Unit B, Unit A tries to find a common preferred G.711 clear channel codec between the two units. If Unit A finds one, it uses this common clear channel codec and the fax should be transmitted properly. If there are no common clear channel codecs between the units, the fax transmission fails.

  SOLUTION: To avoid fax transmission problems, configure both units with the same T.38 and clear channel settings and the fax should be sent properly.

DESCRIPTION: The T.38 fax transmission fails.

POSSIBLE CAUSE: The Mediatrix 2102 opens the T.38 channel only after receiving the “200 OK” message from the peer. This means that the Mediatrix 2102 cannot receive T.38 packets before receiving the “200 OK”. Based on RFC 3264, the T.38 channel should be opened as soon as the unit sends the “INVITE” message.

Information from RFC 3264 (An Offer/Answer Model with Session Description Protocol (SDP)) - section 5.1: Once the offerer has sent the offer, it must be prepared to receive media for any recvonly streams described by that offer. It must be prepared to send and receive media for any sendrecv streams in the offer, and send media for any sendonly streams in the offer (of course, it cannot actually send until the peer provides an answer with the needed address and port information). In the case of RTP, even though it may receive media before the answer arrives, it cannot send RTCP receiver reports until the answer arrives.

SOLUTION: Be sure to reply to the “INVITE” message by a “200 OK” before sending any T.38 message to the Mediatrix 2102.

Tested Fax Models

The following table lists the fax models tested with the Mediatrix 2102 for the T.38 protocol. Each of these fax models has been emulated and tested with each other by using the FaxLab® fax/telephony testing tool.

Table 142: Tested Fax Models

Make	Models	
Brother	• 6650MC • 7150C • FAX-190 • FAX-580MC • Intellifax 600 • Intellifax 625	• Intellifax 950M • Intellifax 2500 • MFC 4550 • MFC 4600 • MFC 4650
Panasonic	• KXF-500 • KXF-580 • KXF-1600 • KXF-3000 • KX-FP270 • KX-FPC95	• PX-5 • PX-150 • PX-350 • UF-880 • UF-V60
Sharp	• FO-145 • FO-235 • FO-445 • FO-5400 • UX-104 • UX-108	• UX-117 • UX-256 • UX-460 • UX-1400 • UX-3600M
Canon	• B70 • Fax 750 • Fax B340 • L777 • MultiPass C530 • MultiPass C545 • MultiPass C555	• MultiPass C560 • MultiPass C755 • MultiPass C2500 • MultiPass C5500 • MultiPass L6000 • MultiPass TF-301
Xerox	• 3004 • 7021 • 7024 • 7033 • WorkCenter 250	• WorkCenter 470cx • WorkCenter 480cx • WorkCenter XE90fx • WorkCenter XK50cx

Table 142: Tested Fax Models (Continued)

Make	Models	
Hewlett Packard	• Fax-200 • Fax 920 • LaserJet 3200	• OfficeJet • OfficeJet 350 • OfficeJet 570

Issues Arising from Specific Combinations/Scenarios

The following are very specific issues the Mediatrix 2102 may experience with certain types of faxes.

DESCRIPTION: Fax from Brother to HP Laser Jet may fail more than 50% of the time.

ISSUE: Faxes from Brother models to Hewlett Packard LaserJet 3200 may fail half of the time when sent from a /2102 to a Mediatrix 1104 by way of two Mediatrix 1204s. The following settings were tested:

a. Pair 1 tested:
- Brother 6650MC (Originating: TX 3 Pg ECM, best encoding, V.17, 14400 bps, best resolution).
- Hewlett Packard LaserJet 3200 (Answering: RX 3 Pg, best ECM, best encoding, V.17, 9600 bps, best resolution).

b. Pair 2 tested:
- Brother Fax-580MC (Originating: TX 3 Pg ECM, best encoding, V.17, 14400 bps, best resolution).
- Hewlett Packard LaserJet 3200 (Answering: RX 3 Pg, best ECM, best encoding, V.17, 9600 bps, best resolution).

c. Pair 3 tested:
- Brother Fax-190 (Originating: TX 3 Pg, non-ECM, best encoding, V.29, 9600 bps, best resolution).
- Hewlett Packard LaserJet 3200 (Answering: RX 3 Pg, best ECM, best encoding, V.17, 9600 bps, best resolution).

DESCRIPTION: Canon B320 fax limitations.

ISSUE: The Mediatrix 2102 may not be compatible with the Canon B320 fax machine. The problem is in a T.38 transmission only and when the Canon B320 is the local fax attached to the Mediatrix 2102 and is the document receiver.

Configuration Issues

The following are issues you may encounter when changing the Mediatrix 2102 configuration.

DESCRIPTION: When the Mediatrix 2102 configuration is entirely static and I change the configuration source of any server from static to DHCP, the service related to the server is not accessible.

POSSIBLE CAUSE: If none of the *xxxConfigSource* variables (in the *ipAddressStatus* folder) are set to **dhcp**, then the Mediatrix 2102 does not send a DHCP REQUEST message. This is the case if:

- you set all *xxxSelectConfigSource* variables to something other than **dhcp** and you restart the Mediatrix 2102, or
- you select the **setConfigSourcesStatic** option of the *sysAdminCommand* variable and you restart the Mediatrix 2102.

Whenever the *xxxSelectConfigSource* variable of a specific server, e.g., syslog server, is set to **dhcp**, then no IP address can be assigned to that server (this does not trigger a DHCP request).

The service is therefore not functional, the corresponding *xxxHost* variable is set to **0.0.0.0**, and the corresponding *xxxPort* variable is not accessible (the GET request result is ERROR), in the *ipAddressStatus* folder.

Note: In the case of the SIP servers, the corresponding *xxxPort* variable is accessible.

SOLUTION: Restart the Mediatrix 2102 or set the proper *xxxSelectConfigSource* variable to **static**.

Software Upgrade Issues

The following are issues you may encounter when performing a software upgrade operation.

DESCRIPTION: An error occurs when the Mediatrix 2102 attempts to communicate with the image server.

POSSIBLE CAUSE: The directory specified in the upgrade command does not exist or does not contain the files required for the software download process.

SOLUTION:

- Check the directory name.
- Be sure that the directory contains files. If not, extract them from the zip file again. See "Download Procedure" on page 128 for more details.
- Be sure that the software server is running and properly configured.

POSSIBLE CAUSE: The IP address of the software server is not the correct one.

SOLUTION:

- Check the given IP address.
- Check the IP port.

DESCRIPTION: An error occurs when the Mediatrix 2102 attempts to transfer the software upgrade.

POSSIBLE CAUSE: The Ethernet cable has become disconnected from the Mediatrix 2102 or the PC running the file transfer.

SOLUTION: Reconnect the cable and start again.

POSSIBLE CAUSE: Power to the Mediatrix 2102 has been disrupted during the file transfer.

SOLUTION: Check the power connection to the Mediatrix 2102 and start again.

DESCRIPTION: When downgrading the Mediatrix 2102 to a previous version of the application software, the unit does not restart, the *LAN* LED is blinking and all other LEDs are off.

POSSIBLE CAUSE: The default router IP address is set to 0.0.0.0, which is not supported by the version to which you downgraded.

SOLUTION: Perform a recovery mode or a factory reset procedure after proceeding with the downgrade operation.

- If you perform a recovery mode as per "Recovery Mode" on page 21, you must manually change the default router IP address to a valid address other than 0.0.0.0, then restart the Mediatrix 2102.
- If you perform a factory reset procedure as per "Factory Reset" on page 22, everything should be working properly. However, this deletes any custom setting you may have done in other variables as it reverts the Mediatrix 2102 back to its default factory settings.

DESCRIPTION: The TFTP server does not recognize the download path and produces an error.

POSSIBLE CAUSE: You should use the “/” character when defining the path to indicate sub-directories, i.e., *c:/temp/download*. However, some TFTP servers on the Windows operating system do not recognize the “/” character and produce an error.

SOLUTION: Use the “\” character in the path definition.

DESCRIPTION: Performing a software download takes an unusually long time.

POSSIBLE CAUSE: If the following happens:

- Any information is set to come from the DHCP server (for example, the SNTP server address) and the DHCP server cannot be reached.
- The primary software server address is invalid (either set by DHCP or static).

The unit tries to reach the primary software server without realizing that the address is invalid. It keeps trying for a few minutes, even if the download procedure fails.

This delay is caused by the Mediatrix 2102 that cannot function as configured if part of its configuration (the DHCP information) is unavailable. Furthermore, there is an issue with switches that use the Spanning Tree Protocol. When this protocol is enabled, the Mediatrix 2102 may be denied from the network for a certain time, which causes the long delay.

SOLUTION: Mediatrix recommends to set up all information to use a valid static value, or have a DHCP server answer the requests. See “Static Configuration” on page 54 for more details.

SNMP Management Software Issues

The following are issues you may encounter when trying to contact the Mediatrix 2102 with a SNMP management software.

DESCRIPTION: The SNMP network management software cannot access the Mediatrix 2102.

- **POSSIBLE CAUSE**: The SNMP network management software does not have the proper Mediatrix 2102 information.

  SOLUTION: Check that:

  - The IP information for the Mediatrix 2102 is correctly configured.
  - The Mediatrix 2102 was restarted after defining the IP information.
  - The line through which you are trying to access the Mediatrix 2102 has been unlocked or is not the correct line. If it is locked, check the connections and network cabling for the connector.

  Try to locate the Mediatrix 2102 IP address. If impossible, perform a recovery reset as indicated in section "Default Settings Switch" on page 20.

DESCRIPTION: There is no response when trying to access the Mediatrix 2102.

- **POSSIBLE CAUSE**: The Mediatrix 2102 speaks the three most common SNMP protocols: SNMPv1, SNMPv2c, and SNMPv3. If you try to access it by using any other protocol, it stays silent.

DESCRIPTION: The SNMP network manager does not receive Traps.

- **POSSIBLE CAUSE**: The IP information is not correct.

  SOLUTION: Check that the IP information (IP address + IP port) of the SNMP network manager software is correctly recorded by the Mediatrix 2102.

DESCRIPTION: When trying to set a variable, the Mediatrix 2102 does no respond, nor sends an error message.

- **POSSIBLE CAUSE**: In secure management mode, the Mediatrix 2102 does not accept SNMPv1 and SNMPv2c SET requests. However, the MIB variables are viewable in any management mode (secure and not secure).

DESCRIPTION: When entering a value such as ".23" in a MIB variable (for instance, *sipTransportQValue*), the Mediatrix 2102 returns a "Wrong value" error message.

- **POSSIBLE CAUSE**: The Mediatrix 2102 does not support a value such as ".23".

  SOLUTION: Enter a value such as "0.23" instead.

DESCRIPTION: When I try to set a variable with a MIB configuration tool such as Mediatrix 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 configuration tool – the Unit Manager Network – does not support MIBs that are located under the *mediatrixExperimental* branch of the MIB structure. The Unit Manager Network does not have specific tasks to manage variables in experimental MIBs.

The *mediatrixExperimental* branch is the area where objects and events in MIBs under development can be placed without fear of conflicting with other MIBs. When the items rooted under an experimental sub-tree are ready for release, they will be under a permanent branch.

Even though the Unit Manager Network can view experimental MIBs, SNMP operations may not work properly on them.

DESCRIPTION: When viewing a table, the unit does not respond.

POSSIBLE CAUSE: It may take time to fill completely a table: from 1 to 5 seconds. This is normal, because the unit is an embedded device with limited processing power.

DESCRIPTION: Is it possible for a hacker to change the content of SNMPv3 variables once the Mediatrix 2102 is in secure mode management?

POSSIBLE CAUSE: In secure management mode, the Mediatrix 2102 works in SNMPv1 read-only, SNMPv2c read-only, and SNMPv3 read/write. SNMP requests using the first two protocols are read-only, and tables used for setting up SNMPv3 users hide the passwords they carry. Because hackers do not know what password to use in SNMPv3 requests, they cannot access the Mediatrix 2102 with read-write permission.

APPENDIX

A

Standards Compliance and Safety Information

This Appendix lists the various standards compliance of the Mediatrix 2102.

Standards Supported

The Mediatrix 2102 complies to the following standards:

Table 143: Standards Compliance

Category	Specification
Agency approvals	• UL • European Union, CE mark (Declaration of Conformity) • Anatel • NOM • A-Tick • FCC
Safety standards	• UL60950-1 • CAN/CSA-C22.2 No. 60950-00-1 • Resolution 238:2000 • IEC 60950 (1st Edition 2001 With all national deviations) • AS/NZS 60950-1 • NOM-019-SCFI-1998
Emissions	• FCC Part 15:1998 Class B • EN55022 (1994) Class B(With amendments A1 and A2) • AS/NZS CISPR 22 Class B • EN61000-3-2 (2000) Harmonic current emissions • EN61000-3-3 (1995) Voltage fluctuations and flicker (with amendment A1) • Resolution 237:2000 (Title II)
Immunity	EN55024:1998 including the following (with amendments A1 and A2): • EN61000-4-2 (1995), ESD • EN61000-4-3 (1996), Radiated RF • EN61000-4-4 (1995), Burst Transients • EN61000-4-5 (1995), Surge • EN61000-4-6 (1996), Conducted RF EN61000-4-11 (1995), Voltage Dips and Interruptions

Table 143: Standards Compliance (Continued)

Category	Specification
Telecom	• FCC Part 68:Subpart D • Industry Canada (CS-03, Issue 8, Part 1) • TBR 21: January 1998 • AS/ACIF S002 - 2001 • AS/ACIF S003 - 2001 • AS/ACIF S043 • Cofetel

Note: The standards compliance of the Mediatrix 2102 are printed on a sticker located on the bottom of the unit.

Disclaimers

The following are the disclaimers related to the Mediatrix 2102.

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 could void the user’s authority to operate the equipment.

Federal Communications Commission (FCC) Part 68

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

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

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

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

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

Connection to party lines is subject to state tariffs.

INSTALLATION

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

Industry Canada

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

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

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

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

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

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

Note: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

CE Marking

DECLARATION OF CONFORMITY

We 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 at the above address.

Translated Warning Definition

The following information provides an explanation of the symbols which appear on the Mediatrix 2102 and in the documentation for the product.

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

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

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

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

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

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

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

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

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

Varning!: Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Safety Warnings

This section lists the following safety warnings:

- Circuit Breaker (20A) Warning
- TN Power Warning
- Product Disposal Warning
- No. 26 AWG Warning
- LAN Connector Warning
- Socket Outlet Warning

Circuit Breaker (20A) Warning

> **Warning:** This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 20A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

TN Power Warning

> **Warning:** The device is designed to work with TN power systems.

Product Disposal Warning

> **Warning:** Ultimate disposal of this product should be handled according to all national laws and regulations.

No. 26 AWG Warning

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

LAN Connector Warning

> **Warning:** Do not connect the LAN connector directly to the Public Switched Telephone Network (PSTN), to an off premise application, an out of plant application, any exposed plant application, or to any equipment other than the intended application, connection may result in a safety hazard, and/or defective operation and/or equipment damage.
>
> Exposed plant means where any portion of the circuit is subject to accidental contact with electric lighting or power conductors operating at a voltage exceeding 300V between conductors or is subject to lightning strikes.

Socket Outlet Warning

> **Warning:** The socket outlet, if used, shall be located near the equipment and shall be easily accessible by the user.

Safety Recommendations

To insure general safety follow these guidelines:

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

Caution: When using this equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

APPENDIX B Standard Hardware Information

The specifications and information regarding this product are subject to change without notice. Every effort is made to ensure the accuracy of this document. Because of ongoing product improvements and revisions, Mediatrix cannot guarantee its accuracy, nor can be responsible for errors or omissions. Please contact your Mediatrix sales representative to obtain the latest version of the technical specifications.

Industry Standard Protocols

The Mediatrix 2102 has been designed to support all major industry standards used today, as well as those that will eventually be implemented at a later date. Because of this specific design characteristic, the Mediatrix 2102 can be integrated with existing telephone, fax and data equipment such as PCs and routers.

Table 144: Industry Standard Protocols

Parameter	Description
Vocoders	• G.711 (a-law, u-law) with optional VAD support • G.723.1a • G.729a • G.729ab
IP Telephony Protocols	• SIP - RFC 3261
Real-Time Transport Protocols	• RTP/RTCP - RFC 1889, RFC 1890, RFC 2833, RFC 3389
Network Management Protocols	• SNMPv3 • DHCP - RFC 2131, RFC 2132 • TFTP - RFC 1350, RFC 2347, RFC 2348, RFC 2349 • Syslog - RFC 3164 • HTTP 1.0 - RFC 1945 • Basic and digest HTTP authentication - RFC 2617
Data Features	• PPPoE client - RFC 1332, RFC 1661, RFC 1334, RFC 1994, RFC 2516, RFC 1471, RFC 1472, RFC 1473, RFC 1877. Note: some PPPoE RFCs are implemented partially. • TFTP or HTTP auto-provisioning • Transparent IP address sharing (Mediatrix patent pending technology allowing the same IP address to be shared between both Ethernet ports and distinguishing voice traffic from data traffic) • DHCP server • STUN client
QoS	• ToS • DiffServ • 802.1p • 802.1Q

Hardware Features

Display

- Power LED
- LAN activity LED
- Activity/In-Use LED indication on FXS ports
- Ready LED

Connectors

- 2 RJ-11 connectors, analog phone/fax (FXS) interface.
- 1 RJ-11 connector, PSTN bypass.
- 1 RJ-45 WAN connector, 10/100 BaseT Ethernet access with auto MDI/MDIX (cross-over Ethernet cable not required).
- 1 RJ-45 LAN connector, 10/100 BaseT Ethernet access with auto MDI/MDIX (cross-over Ethernet cable not required).

Power

- External wall plug power supply. The voltage differs depending on the hardware revision of your unit:
  - Mediatrix 2102 with hardware revision 7: 12 Vdc at 8 W.
  - Mediatrix 2102 with hardware revision 6: 24 Vdc at 13.2 W.
- Seamless switch over period if the client UPS detects a power loss and activates within 8 ms.
- Country-specific models.

Casing / Installation

- Casing: Desktop (Plastic ABS UL94 V0).
- Installation: The Mediatrix 2102 is designed for the desktop or can be wall-mountable.

Product Architecture Details

- Supports two concurrent communications using any vocoders.
- DSP-based DTMF detection and generation.
- DSP-based fax relay.
- Embedded operating system with 32-bit real-time multitasking Kernel.
- Embedded IPv4 TCP/IP stack with configurable QoS implemented by:
  - ToS byte at Network layer 3
  - 802.1p at Data Link layer 2
- Network parameters assigned via DHCP

Real Time Fax Router Technical Specifications

Automatic selection between voice and fax.

Table 145: Fax Technical Specifications

Parameter	Description
Ethernet	10/100 BaseT Ethernet
Data Link	Ethernet II
Network	IP (Internet Protocol)
Transport	TCP / UDP
Protocols	Group 3 Fax Clear channel (G.711) or T.38 Real Time Fax Over IP protocol Stack
Fax Data Compression	MH
Fax Transmission	Up to 14.4 kbps

Analog Line Interface (FXS)

- Direct connection to a fax machine or telephone
- RJ-11 connectors
- DC feeding of the access line protected for over voltage
- Loop current detection and hook flash detection capable
- Generation of Selective Ring

Table 146: Analog Line Interface

Parameter	Description
Trunk Type	Loop Start
Ring Source	45 VRMS max @ 20 up to 50 Hz (selectable) sine signal
Nominal Impedance	BellCore compliant 600/900 ohms default setting.
Ring Drive Capacity	Up to 4 ringer equivalents (4 RENs) per port (Hardware revision 7). Up to 3 ringer equivalents (3 RENs) per port (Hardware revision 6).
Loop Current Range	15 to 32 mA factory set. Default 20 mA regulated.
Ring Trip Detection Time	2 ring cycles max
On Hook Voltage	-48 VDC
Frequency Response	200 Hz to 3400 Hz ±3 dB (Tx/Rx)
Return Loss	600-3400 Hz: 30 dB

Audio Specifications

- Software input and output level adjustable within the range of -30 dB to +20 dB.
- Software-adjustable dynamic and static jitter buffer protection.
- Programmable by country: Call progress tone generation including dial tone, busy tone, ringback and error tones.
- Silence detection/suppression level software adjustable.

DTMF Tone Detection

Table 147: DTMF Tone Detection

Parameter	Description
16-Digit DTMF Decoding	0 to 9, *, #, A, B, C, D
Permitted Amplitude Tilt	High frequency can be +2 dB to -8 dB relative to low frequency
Dynamic Range	-35 dBm to +3 dBm per tone
Frequency Accept	± 1.5% of nominal frequencies
Minimum Tone Duration	40 ms, can be increased with software configuration
Interdigit Timing	Detects like digits with a 40 ms interdigit delay

DTMF Tone Generation

Table 148: DTMF Tone Generation

Parameter	Description
Per Frequency Nominal	-6 dBm to -4 dBm
Frequency Deviation	Less than 1%

MTBF Value

The Mean Time Before Failure (MTBF) value of the Mediatrix 2102 is 250 000 hours at 25 degrees Celsius ambient temperature. It has been defined using RelCalc v5.0, Bellcore method (LimitedStress - Method I, Case 3), Desktop unit without the external power supply.

Power Consumption

Measurements at the DC input

Table 149: Power Consumption at the DC Input

Parameter	Description
Idle Mode, 12Vdc (Hardware revision 7)	I = 415 mA P = 5 W
Idle Mode, 24Vdc (Hardware revision 6	I = 130 mA P = 3.15 W
Ringing Mode (worst case, 4 REN load); 12Vdc (Hardware revision 7	I = 625 mA P = 7.5 W
Ringing Mode (worst case, 3 REN load); 24Vdc (Hardware revision 6	I = 255 mA P = 6.15 W

Operating Environment

Table 150: Operating Environment

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

Dimensions and Weight

Table 151: Dimensions and Weight

Parameter	Description
Dimensions	14 cm x 20 cm x 5 cm - 5.5 in. x 8 in. x 2 in. (approx.)
Weight	454 g (1.2 lb) with power supply unit

Warranty

All Mediatrix products carry Mediatrix Telecom, Inc.'s standard one-year hardware and software warranty. An extended warranty is available.

APPENDIX C

Cabling Considerations

This Appendix describes the pin-to-pin connections for cables used with the Mediatrix 2102.

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

Straight Through (RJ-45) Cable

The RJ-45 connector is commonly used for network cabling and for telephony applications. It is used to wire both ends identically so the signals pass straight through.

RJ-45 cabling is also known as Twisted-pair Ethernet (TPE), Unshielded twisted pair (UTP) and 10/100 Base-T.

Figure 41: RJ-45 Cable

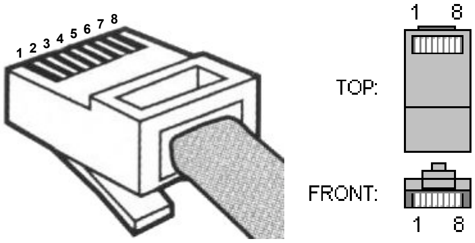
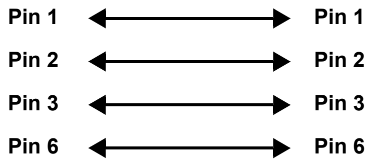


Table 152: RJ-45 Pinout Information

Pin #	Function	Colour Coding	
		EIA/TIA 568A	EIA/TIA 568B AT&T 258A
1	Transmit +	White with green stripe	White with orange stripe
2	Transmit -	Green with white stripe or solid green	Orange with white stripe or solid orange
3	Receive +	White with orange stripe	White with green stripe
4	N/A	Blue with white stripe or solid blue	Blue with white stripe or solid blue
5	N/A	White with blue stripe	White with blue stripe
6	Receive -	Orange with white stripe or solid orange	Green with white stripe or solid green
7	N/A	White with brown stripe or solid brown	White with brown stripe or solid brown
8	N/A	Brown with white stripe or solid brown	Brown with white stripe or solid brown

The RJ-45 cable uses two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 1 & 2 are on one twisted pair and pins 3 & 6 are on a second pair according to common wiring standards which meet the EIA/TIA T568A and T568B requirements.

Figure 42: Straight Through Connectivity



Pin Name And Function

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

Table 153: Pin Name and Function

Pin #	Name	Function
1	Transmit Data Plus	The positive signal for the TD differential pair. This signal contains the serial output data stream transmitted onto the network.
2	Transmit Data Minus	The negative signal for the TD differential pair. This contains the same output as pin 1.
3	Receive Data Plus	The positive signal for the RD differential pair. This signal contains the serial input data stream received from the network.
4	not connected	
5	not connected	
6	Receive data minus	The negative signal for the RD differential pair. This signal contains the same input as pin 3.
7	not connected	
8	not connected	

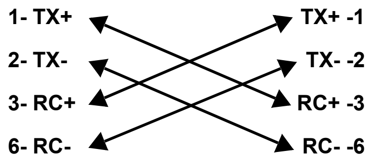
Crossover Cable

A RJ-45 crossover cable is used when only two systems are to be connected to each other, peer to peer, at the Ethernet Cards by “crossing over” (reversing) their respective pin contacts. An example would be connecting two computers together to create a network. The crossover eliminates the need for a hub when connecting two computers. A crossover cable may also be required when connecting a hub to a hub, or a transceiver to transceiver or repeater to repeater. When connecting a hub to a transceiver, a straight through cable is always used.

Note: This is not an IEEE supported configuration and should be used for test purposes only.

A crossover cable is sometimes called a null modem. The coloured wires at either end are put into different pin numbers, or crossed over.

Figure 43: Crossover Connectivity



APPENDIX

D

Country-Specific Parameters

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

Definitions

The following are some useful definitions.

Table 154: Definitions

Term	Description
Dial Tone	Indicates the line is ready to receive dialing.
Busy Tone	Indicates the line or equipment is in use, engaged or occupied.
Ringback Tone	Indicates the called line is ringing out.
Special Information Tone	Identifies network-provided announcements.
Stutter Dial Tone	Notifies the user that they have a voice mail message when the phone does not or cannot have a message-waiting light.
Confirmation Tone	Confirms a command performed by the user (such as activate a service).
Receiver Off Hook (ROH) Tone	Indicates that the telephone is not hung up correctly.
Message Waiting Indicator Tone	Indicates there is a message waiting somewhere for the owner of the phone
Network Congestion Tone	Indicates that all switching paths are busy, all toll trunks are busy, or there are equipment blockages.

Conventions

The following conventions apply to this Appendix.

Frequencies

- Symbol "*" means modulated. For instance: 425 Hz * 25 means 425 Hz modulated at 25 Hz.
- Symbol "+" means added. For instance: 425 Hz + 330 Hz means that both 425 Hz and 330 Hz sines are played at the same time.
- When a tone is composed of more than one frequency, if not otherwise specified, the given electrical level applies to each frequency taken separately.

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

When representing an impedance, the following applies:

- Symbol "//" means parallel.
- Symbol "+" means serial.

Furthermore, there are two types of impedances:

- Input Impedance
- Terminal Balance Return Loss (TBRL) Impedance

Input Impedance

Impedance of the Mediatrix 2102 at the Tip and Ring wires.

Terminal Balance Return Loss (TBRL) Impedance

Balance return loss attributable to transmission loss between two points. It is used to characterize an impedance balancing property of the 2-wire analog equipment port.

Each country has its own definition of the TBRL value. For instance, in North America, TIA/EIA 464 (and TIA/EIA 912) define two TBRL values:

- 600 Ω for "on-premise" or short loop ports.
- 350 Ω + (1000 Ω || 21 nF) for "off-premise" or long loop ports.

A wire length above 2.5 km is considered long loop according to TIA/EIA 912 section 6.4 (7)(b)).

In Europe, ETSI 300 439 also mentions a TBRL value. However, most European countries have different requirements regarding the TBRL Impedance. This is also true for other countries around the world. Each one of them has different requirements.

Line Attenuation

Values are given in dBr (deciBel relative):

- A "+" for input means that the digital side is attenuated by x decibels relative to the analog side.
- A "+" for output means that the analog side is amplified by x decibels relative to the digital side.
- A "-" for input means that the digital side is amplified by x decibels relative to the analog side.
- A "-" for output means that the analog side is attenuated by x decibels relative to the digital side.

On-Off Sequences

Values in bold are "on" cycles, where tones are audible. Values in normal style are "off" cycles, where tones are not audible. When not otherwise specified, sequences repeat forever. A "x" symbol means that the sequences between parenthesis is repeated x times. The next cycle(s) repeat forever, unless otherwise specified. Values are in seconds.

For instance:

```
3*(0.1 -  0.1) then 0.6 - 1.0 - 0.2 - 0.2
```

means that the 0.1s on and 0.1s off sequence is repeated 3 times, afterwards the 0.6s on, 1.0s off, 0.2s on and 0.2s off sequence repeats forever.

Distinctive Ring

The distinctive ring service allows you to have three different numbers with each their own ring. The numbers ring through a single line coming into the business or residence and each number can be distinguished by the pattern of the ring. These ring patterns are made up of various combinations of ring bursts.

This feature uses the "*Alert-Info*" header from the initial INVITE of a call to know if the call requires a distinctive ringing.

The supported vaue of the "A*lert-Info*" are:

Table 155: Distinctive RIng Patterns

Alert-Info value	Ring Name	On – Off Sequence (s)
<http://127.0.0.1/Bellcore-dr2>	Bellcore-dr2	**0.8** – 0.4, **0.8** – 4.0
<http://127.0.0.1/Bellcore-dr3>	Bellcore-dr3	**0.4** – 0.2, **0.4** – 0.2, **0.8** – 4.0

Table 155: Distinctive RIng Patterns (Continued)

Alert-Info value	Ring Name	On – Off Sequence (s)
<http://127.0.0.1/Bellcore-dr4>	Bellcore-dr4	**0.3** – 0.2, **1.0** – 0.2, **0.3** – 4.0

The Mediatrix 2102 plays the default ring of the country selected if the *Alert-Info* value is not present or the value is not supported.

☞ **Note:** Since the first pause of the distinctive ring is lower that 1 second, a splash ring followed by an Off of 1 second precedes the distinctive ring pattern.

Australia

The following parameters apply if you have selected Australia as location.

Australia 1

The following parameters apply if you have selected Australia1 as location.

Table 156: Australia 1 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	**CONTINUOUS**	-18 dBm
Busy Tone	425 Hz	**0.375** – 0.375	-18 dBm
Ringback Tone	425 Hz * 25	**0.4** – 0.2, **0.4** – 2.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	**CONTINUOUS**	-18 dBm
Confirmation Tone	450 Hz	(**0.15** – 0.15 – **0.15**) x 2 End	-18 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2067 Hz 2467 Hz 2600 Hz	**0.1** – 0.1	-21 dBm -21 dBm -21 dBm -21 dBm
Message Waiting Indicator Tone	425 Hz * 25	**0.1** – 0.04, x72	-18 dBm
Network Congestion Tone	400 Hz	**0.375** – 0.375	-18 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6 dBr

Australia 2

The following parameters apply if you have selected Australia2 as location.

Table 157: Australia 2 Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz * 25	**CONTINUOUS**	-18 dBm
Busy Tone	425 Hz	**0.375** – 0.375	-18 dBm
Ringback Tone	425 Hz * 25	**0.4** – 0.2, **0.4** – 2.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	**CONTINUOUS**	-18 dBm
Confirmation Tone	450 Hz	(**0.15** – 0.15 – **0.15**) x 2 End	-18 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2067 Hz 2467 Hz 2600 Hz	**0.1** – 0.1	-21 dBm -21 dBm -21 dBm -21 dBm
Message Waiting Indicator Tone	425 Hz * 25	**0.1** – 0.04, x72	-18 dBm
Network Congestion Tone	400 Hz	**0.375** – 0.375	-18 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-6 dBr

Australia 3

The following parameters apply if you have selected Australia3 as location.

Table 158: Australia 3 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz * 25	**CONTINUOUS**	-18 dBm
Busy Tone	425 Hz	**0.375** – 0.375	-18 dBm
Ringback Tone	425 Hz * 25	**0.4** – 0.2, **0.4** – 2.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	**CONTINUOUS**	-18 dBm
Confirmation Tone	450 Hz	(**0.15** – 0.15 – **0.15**) x 2 End	-18 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2067 Hz 2467 Hz 2600 Hz	**0.1** – 0.1	-21 dBm -21 dBm -21 dBm -21 dBm
Message Waiting Indicator Tone	425 Hz * 25	**0.1** – 0.04, x72	-18 dBm
Network Congestion Tone	400 Hz	**0.375** – 0.375	-18 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
Default Caller ID	BELLCORE		
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 159: Austria Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	**CONTINUOUS**	-20 dBm
Busy Tone	450 Hz	**0.3** – 0.3	-20 dBm
Ringback Tone	450 Hz	**1.0** – 5.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Stutter Dial Tone	450 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-20 dBm
Confirmation Tone	450 Hz	(**0.1** – 0.1) x 3 End	-20 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	450 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-20 dBm
Network Congestion Tone	450 Hz	(**0.1** – 0.1) x10, **CONTINUOUS**	-20 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	**1.0** – 5.0	
Input Impedance	270 Ω + 750 Ω // 150 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr

Brazil

The following parameters apply if you have selected Brazil as location.

Table 160: Brazil Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-15 dBm
Busy Tone	425 Hz	**0.25** – 0.25	-10 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-15 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	(3 x **0.3** – 2 x 0.03) – 1.0	-15 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-15 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3 End	-15 dBm
Receiver Off Hook (ROH) Tone	425 Hz	**0.25** – 0.25	-10 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-15 dBm
Reorder Tone	425 Hz	**0.75** – 0.25, **0.25** – 0.25	-10 dBm
Network Congestion Tone	450 Hz	**0.2** – 0.2	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	900 Ω		
Default Caller ID	TELEBRAS_DTMF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

China

The following parameters apply if you have selected China as location.

Table 161: China Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	450 Hz	**CONTINUOUS**	-10 dBm
Busy Tone	450 Hz	**0.35** – 0.35	-10 dBm
Ringback Tone	450 Hz	**1.0** – 4.0	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-10 dBm
Stutter Dial Tone	450 Hz	**0.4** – 0.04	-10 dBm
Confirmation Tone	450 Hz	(**0.1** – 0.1) x 3, End	-10 dBm
Receiver Off Hook (ROH) Tone	950 Hz 950 Hz 950 Hz 950 Hz	**15.0** – 15.0 – 15.0 15.0 – **15.0** – 15.0 15.0 – 15.0 – **15.0** 15.0 – 15.0 – 15.0 – **CONTINUOUS**	-25 dBm -16 dBm -8 dBm -6 dBm
Message Waiting Indicator Tone	450 Hz	**0.4** – 0.04	-10 dBm
Network Congestion Tone	450 Hz	**0.7** – 0.7	-10 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Denmark

The following parameters apply if you have selected Denmark as location.

Table 162: Denmark Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-15 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-10 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-15 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-15 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-15 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-15 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-15 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	300 Ω + 1000 Ω // 220 nF		
Default Caller ID	TDK_DTMF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6 dBr

France

The following parameters apply if you have selected France as location.

Table 163: France Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	440 Hz	**CONTINUOUS**	-16.9 dBm
Busy Tone	440 Hz	**0.5** – 0.5	-19.9 dBm
Ringback Tone	440 Hz	**1.5** – 3.5	-19.9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	(3 x **0.3** – 2 x 0.03) – 1.0	-19.9 dBm
Stutter Dial Tone	440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-16.9 dBm
Confirmation Tone	440 Hz	(**0.1** – 0.1) x 3, End	-16.9 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	440 Hz	(**0.1** – 0.1) x 10	-16.9 dBm
Network Congestion Tone	440 Hz	**0.25** – 0.25	-19.9 dBm
Ring	AC: 45 VRMS, 50 Hz DC: 15 Vdc	**1.5** – 3.5	
Input Impedance	215 Ω + 1000 Ω // 137 nF		
Default Caller ID	FRANCE: BELLCORE FRANCE_ETSI_FSK: ETSI_FSK FRANCE_ETSI_DTMF:ETSI_DTMF		
FXS Line Attenuation (Input)			+1.9 dBr
FXS Line Attenuation (Output)			-8.9 dBr

Germany

The following parameters apply if you have selected Germany as location.

Germany 1

The following parameters apply if you have selected Germany 1 as location.

Table 164: Germany 1 Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-16 dBm
Busy Tone	425 Hz	**0.48** – 0.48	-16 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-16 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-16 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10	-16 dBm
Network Congestion Tone	425 Hz	**0.24** – 0.24	-16 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr

Germany2

The following parameters apply if you have selected Germany 2 as location.

Table 165: Germany 2 Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-16 dBm
Busy Tone	425 Hz	**0.48** – 0.48	-16 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-16 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-16 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10	-13 dBm
Network Congestion Tone	425 Hz	**0.24** – 0.24	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
Default Caller ID	BELLCORE		
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 166: Hong Kong Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	350 + 440 Hz	**CONTINUOUS**	-13 dBm
Busy Tone	480 + 620 Hz	**0.5** – 0.5	-13 dBm
Ringback Tone	440 + 480 Hz	**0.4** – 0.2, **0.4** –3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-16 dBm
Stutter Dial Tone	350 + 440 Hz	(**0.1** – 0.1) x 20, **CONTINUOUS**	-16 dBm
Confirmation Tone	350 + 440 Hz	**0.1** – 0.1, **0.3** – End	-16 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	350 + 440 Hz	(**0.2** – 0.2, **0.5** – 0.2) x 4, **CONTINUOUS**	-16 dBm
Network Congestion Tone	480 + 620 Hz	**0.25** – 0.25	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** –3.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6 dBr

Indonesia

The following parameters apply if you have selected Indonesia as location.

Table 167: Indonesia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-9 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-9 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** – 0.03, **0.33** – 0.03, **0.33** – 1.0	-9 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-9 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-9 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	950 Hz	**0.33** – 0.03	-9 dBm
Network Congestion Tone	425 Hz	**0.25** – 0.25	-9 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
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 168: Israel Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	**CONTINUOUS**	-15 dBm
Busy Tone	400 Hz	**0.5** – 0.5	-15 dBm
Ringback Tone	400 Hz	**1.0** – 3.0	-15 dBm
Special Information Tone	1000 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-15 dBm
Stutter Dial Tone	400 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-15 dBm
Confirmation Tone	400 Hz	**0.17** – 0.14, **0.34**	-15 dBm
Receiver Off Hook (ROH) Tone	1440 Hz 2060 Hz 2452 Hz 2600 Hz	**0.12** – 0.88	-20 dBm -20 dBm -20 dBm -20 dBm
Message Waiting Indicator Tone	400 Hz	(**0.16** – 0.16) x 10, **CONTINUOUS**	-15 dBm
Network Congestion Tone	400 Hz	**0.25** – 0.25	-15 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 3.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
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 169: Italy Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**0.2** – 0.2, **0.6** – 1.0	-13 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **0.2** – 0.2, **0.6** – 1.0	-13 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-13 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **0.2** – 0.2, **0.6** – 1.0	-13 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	180 Ω + 630 Ω // 60 nF		
Default Caller ID	BELLCORE		
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 170: Japan Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	400 Hz	**CONTINUOUS**	-13 dBm
Busy Tone	400 Hz	**0.5** – 0.5	-13 dBm
Ringback Tone	400 Hz * 16	**1.0** – 2.0	-16 dBm
Special Information Tone	400 Hz	**0.1** – 0.1	-13 dBm
Stutter Dial Tone	400 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-13 dBm
Confirmation Tone	400 Hz	(**0.1** – 0.1) x 3, End	-13 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	400 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-13 dBm
Network Congestion Tone	400 Hz	**0.5** – 0.5	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**1.0** – 2.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
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 171: Malaysia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-14 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-18 dBm
Ringback Tone	425 Hz	**0.4** – 0.2, **0.4** – 2.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**1.0** **1.0** **1.0** – 1.0	-14 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-14 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3 End	-14 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-14 dBm
Network Congestion Tone	425 Hz	**0.** – 0.25	-18 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr

Mexico

The following parameters apply if you have selected Mexico as location.

Table 172: Mexico Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-14 dBm
Busy Tone	425 Hz	**0.25** – 0.25	-18 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**1.0** **1.0** **1.0** – 1.0	-14 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-14 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-14 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-14 dBm
Network Congestion Tone	425 Hz	**0.25** – 0.25	-18 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr

Netherlands

The following parameters apply if you have selected Netherlands as location.

Table 173: Netherlands Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-17 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-17 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-17 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-17 dBm
Network Congestion Tone	425 Hz	**0.25** – 0.25	-17 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	270 Ω + 750 Ω // 150 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

New Zealand

The following parameters apply if you have selected New Zealand as location.

Table 174: New Zealand Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	400 Hz	**0.5** – 0.5	-17 dBm
Ringback Tone	400 Hz + 450 Hz	**0.4** – 0.2, **0.4** – 2.0	-19 dBm
Special Information Tone	1400 Hz	**0.1** – 0.1	-17 dBm
Stutter Dial Tone	400 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Confirmation Tone	400 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	400 Hz	(**0.1** – 0.1) x12, **CONTINUOUS**	-17 dBm
Network Congestion Tone	400 Hz	**0.25** – 0.25	-17 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	300 Ω + 1000 Ω // 220 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-9 dBr

North America

The following parameters apply if you have selected North America as location.

North America 1

The following parameters apply if you have selected North America 1 as location.

Table 175: North America 1 Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	350+440 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	480+620 Hz	**0.5** – 0.5	-21 dBm
Ringback Tone	440+480 Hz	**2.0** – 4.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-14 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-17 dBm
Network Congestion Tone	480+620 Hz	**0.25** – 0.25	-21 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**2.0** – 4.0	
Input Impedance	600 Ω		
Tbrl-Impedance[a]	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr

[a] TBRL-Impedance for “on-premise" or short loop ports.

North America 2

The following parameters apply if you have selected North America 2 as location.

Table 176: North America 2 Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	350+440 Hz	**CONTINUOUS**	-17 dBm
Busy Tone	480+620 Hz	**0.5** – 0.5	-21 dBm
Ringback Tone	440+480 Hz	**2.0** – 4.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-14 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-17 dBm
Network Congestion Tone	480+620 Hz	**0.25** – 0.25	-21 dBm
Ring	AC: 45 VRMS, 20 Hz DC: 15 Vdc	**2.0** – 4.0	
Input Impedance	600 Ω		
Tbrl-Impedance[a]	350 Ω + 1000 Ω // 210 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			0 dBr

[a] TBRL-Impedance for “off-premise" or long loop ports (wire length longer than 2.5 km).

Russia

The following parameters apply if you have selected Russia as location.

Table 177: Russia Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-10 dBm
Busy Tone	425 Hz	**0.4** – 0.4	-10 dBm
Ringback Tone	425 Hz	**0.8** – 3.2	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-17 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, End	-10 dBm
Confirmation Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Receiver Off Hook (ROH) Tone	425 Hz	3 x (**0.1** – 0.1), **CONTINUOUS**	-10 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-10 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.8** – 3.2	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			+2 dBr
FXS Line Attenuation (Output)			-2 dBr

Spain

The following parameters apply if you have selected Spain as location.

Table 178: Spain Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-10 dBm
Busy Tone	425 Hz	**0.2** – 0.2	-13 dBm
Ringback Tone	425 Hz	**1.5** – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-20 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-10 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-10 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-10 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2, **0.2** – 0.2, **0.2** – 0.6	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.5** – 3.0	
Input Impedance	220 Ω + 820 Ω // 120 nF		
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Sweden

The following parameters apply if you have selected Sweden as location.

Table 179: Sweden Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-12.5 dBm
Busy Tone	425 Hz	**0.25** – 0.25	-12.5 dBm
Ringback Tone	425 Hz	**1.0** – 5.0	-12.5 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-22 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-12.5 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-12.5 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-12.5 dBm
Network Congestion Tone	425 Hz	**0.25** – 0.75	-12.5 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 5.0	
Input Impedance	200 Ω + 1000 Ω // 100 nF		
Default Caller ID	BELLCORE		
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 180: Switzerland Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	425 Hz	**CONTINUOUS**	-8 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.333** **0.333** **0.333** – 1.0	-13 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-8 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-8 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-8 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	220 Ω + 820 Ω // 115 nF		
Default Caller ID	BELLCORE		
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 181: Thailand Parameters

Parameter	Value	On – Off Sequence (s)	Elect. Levels
Dial Tone	400 * 50 Hz	**CONTINUOUS**	-16 dBm
Busy Tone	400 Hz	**0.5** – 0.5	-10 dBm
Ringback Tone	400 Hz	**1.0** – 4.0	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-15 dBm
Stutter Dial Tone	400 * 50 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-16 dBm
Confirmation Tone	400 * 50 Hz	(**0.1** – 0.1) x 3, End	-16 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	400 * 50 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-16 dBm
Network Congestion Tone	400 Hz	**0.3** – 0.3	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Input Impedance	600 Ω		
Default Caller ID	BELLCORE		
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 182: UK Parameters

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	350+440 Hz	**CONTINUOUS**	-22 dBm
Busy Tone	400 Hz	**0.375** – 0.375	-19 dBm
Ringback Tone	400+450 Hz	**0.4** – 0.2, **0.4** – 2.0	-22 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** **0.33** **0.33** – 1.0	-19 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-22 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3, End	-22 dBm
Receiver Off Hook (ROH) Tone	1400 Hz 2060 Hz 2450 Hz 2600 Hz	**0.1** – 0.1	-19 dBm -19 dBm -19 dBm -19 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-22 dBm
Network Congestion Tone	400 Hz	**0.4** – 0.35, **0.225** – 0.525	-19 dBm
Ring	AC: 45 VRMS, 25 Hz DC: 15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Input Impedance	300 Ω + 1000 Ω // 220 nF		
Default Caller ID	UK: BRITISH_TELECOM UK_BELLCORE: BELLCORE UK_CCA: CCA UK_ETSI_FSK: ETSI_FSK		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-9 dBr

APPENDIX E

Glossary

10 BaseT

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

100 BaseT

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

Access Device

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

A-Law

The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (µ)-law standard. See also *mu (µ)-law*.

Access Concentrator

A device that merges many data transmission signals onto a single shared channel in such a way that all the data channels can be active at the same time. The access concentrator supports dial-up modem calls, ISDN connections, frame relay traffic and multiprotocol routing.

Analog Display Services Interface (ADSI)

Telecommunications protocol standard that enables alternate voice and data capability over the existing analog telephone network. This means that in addition to the familiar voice response audio interface (where you listen to voice recordings and make menu selections using the telephone keypad), you can now see the menu and information on the screen display and make selections using soft keys. To use ADSI, you would need an ADSI capable device (as you would if you want the caller ID service).

Area Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line. In North America, an area code has three digits and is used with a NXX (office code) number. For instance, in the North American telephone number *561-955-1212*, the numbers are defined as follows:

Table 183: North American Numbering Plan

No.	Description
561	Area Code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the area code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is *xZABPQ 12 34*, where:

Table 184: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.

Table 184: France Numbering Plan (Continued)

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

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

Cable Modem

A device that connects a computer to a local cable television line and receives data at about 1.5 Mbps. This data rate far exceeds that of the prevalent 28.8 and 56 Kbps telephone modems and the up to 128 Kbps of Integrated Services Digital Network (ISDN). It is about the data rate available to subscribers of Digital Subscriber Line (DSL) telephone service. A cable modem can be added to or integrated with a set-top box that provides your TV set with channels for Internet access. In most cases, cable modems are furnished as part of the cable access service and are not purchased directly and installed by the subscriber.

Country Code (CC)

In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Custom Local Area Signalling Services (CLASS)

One of an identified group of network-provided enhanced services. A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.

Digital Signal Processor (DSP)

Specialized computer chip designed to perform speedy and complex operations on digitized waveforms. Useful in processing sound (like voice phone calls) and video.

Digital Subscriber Lines (DSL)

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL.

Domain Name Server (DNS)

Internet service that translates domain names into IP addresses. To use a domain name, a DNS service must translate the name into the corresponding IP address. For instance, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF)

In telephone systems, multi-frequency signalling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “*”, the “*” being reserved for special purposes.

Dynamic Host Configuration Protocol (DHCP)

TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

Echo Cancellation

Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.

Far End Disconnect

Refers to methods for detecting that a remote party has hung up. This is also known as Hangup Supervision. There are several methods that may be used by a PBX/ACD/CO to signal that the remote party has hung up, including cleardown tone, or a wink.

Federal Communications Commission (FCC)

U.S. government regulatory body for radio, television, interstate telecommunications services, and international services originating in the United States.

Foreign Exchange Service/Station (FXS)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area’s central office. This is the station (telephone) end of an FX circuit. An FXS port will provide dial tone and ring voltage.

G.711

ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48 kbps, 56 kbps, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1

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

G.729

A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).

Gateway

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

International Telecommunication Union (ITU)

Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

Internet-Drafts

Internet-Drafts are working documents of the IETF, its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet Protocol (IP)

A standard describing software that keeps track of the Internet’s addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

Jitter

A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

Layer 2

Layer 2 refers to the Data Link Layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Data Link Layer is concerned with moving data across the physical links in the network.

The Data-Link Layer contains two sublayers that are described in the IEEE-802 LAN standards:

- Media Access Control (MAC)
- Logical Link Control (LLC)

Layer 3

Layer 3 refers to the Network layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Network Layer is concerned with knowing the address of the neighbouring nodes in the network, selecting routes and quality of service, and recognizing and forwarding to the transport layer incoming messages for local host domains.

Light Emitting Diode (LED)

A semiconductor diode that emits light when a current is passed through it.

Local Area Network (LAN)

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also WAN.

Management Information Base (MIB)

Specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

Management Server

Includes a web-based provisioning client, provisioning server, and SNMP proxy server used to manage all agents connected to the system. The Management Server provides Gateway provisioning, Monitoring, and Numbering Plan.

Media Access Control (MAC) Address

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

Mu (µ)-Law

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Network

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Off-hook

A line condition caused when a telephone handset is removed from its cradle.

On-hook

A line condition caused when a telephone handset is resting in its cradle.

Packet

Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection. The structure of a packet depends on the protocol.

Plain Old Telephone System (POTS)

Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

Point to Point Protocol over Ethernet (PPPoE)

A proposal specifying how a host personal computer interacts with a broadband modem (i.e., DSL, cable, wireless, etc.) to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dialup Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

Port

Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Portable Operating System Interface (POSIX)

POSIX is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturer's computer systems without having to be recoded.

POST

The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.

Private Branch Exchange (PBX)

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Programmable Read-Only Memory (PROM)

A memory chip where data is written only once as it remains there forever. Unlike RAM, PROMs retain their contents when the computer is turned off.

Protocol

A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between 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)

Measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).

Real Time Control Protocol (RTCP)

RTCP is the control protocol designed to work in conjunction with RTP. It is standardized in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

Realtime Transport Protocol (RTP)

An IETF standard for streaming realtime multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.

Registrar Server

A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

Request for Comment (RFC)

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

Router

A specialized switching device which allows customers to link different geographically dispersed local area networks and computer systems. This is achieved even though it encompasses different types of traffic under different protocols, creating a single, more efficient, enterprise-wide network.

Switched Circuit Network (SCN)

A communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

Server

A computer or device on a network that works in conjunction with a client to perform some operation.

Session Description Protocol (SDP)

Describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation. SDP communicates the existence of a session and conveys sufficient information to enable participation in the session. SDP is described in RFC 2327.

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.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Trivial File Transfer Protocol (TFTP)

A simplified version of FTP that transfers files but does not provide password protection, directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP)

An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Voice Over IP (VoIP)

The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN)

A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

Appendix F

List of Acronyms

AC	Access Concentrator
ADSI	Analog Display Services Interface
CE	Cummunauté européenne (French)
CHAP	Challenge Handshake Authentication Protocol
CNG	Comfort Noise Generator
CS-ACELP	Conjugate Structure-Algebraic Code Excited Linear Prediction
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Lines
DTMF	Dual Tone Multi-Frequency
FCC	Federal Communications Commission (USA)
FSK	Frequency Shift Keying
GMT	Greenwich Mean Time
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
Hz	Hertz
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
ISP	Internet Service Provider
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
MTU	Maximum Transmission Unit
MWI	Message Waiting Indicator
NAT	Name Address Translation

OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PBX	Private Branch eXchange
PCM	Pulse Code Modulation
PIN	Personal Identification Number
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol Over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
REN	Ringer Equivalence Number
RFC	Request For Comment
RTCP	Real Time Control Protocol
RTP	Real-Time Protocol
SCN	Switched Circuit Network
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SME	Small and Medium-sized Enterprise
SMI	Structure of Management Information
STP	Spanning Tree Protocol
STUN	Simple Traversal of User Datagram Protocol (UDP) through Network Address Translation (NAT)
TAS	Transparent Address Sharing
TBRL	Terminal Balance Return Loss
TCP/IP	Transmission Control Protocol/Internet Protocol
TPE	Twisted-Pair Ethernet
UDP	User Datagram Protocol
UL	Underwriters Laboratories Incorporated
UTC	Universal Time Coordinated
UTP	Unshielded Twisted pair
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

Appendix G

List of MIB Parameters

Index