

DGW Software Configuration Guide

All Mediatrix Units

DGW 49.2.2941

2023-08-09

Table of Contents

1 Getting started	7
1.1 Danger, Warning, Caution, and Note Definitions	7
1.2 Logon	7
1.3 Mediatrix Unit Reset	8
1.4 Personnal Data Usage and Protection	14
1.5 Management Interfaces	19
1.6 IPv6	20
1.7 Naming Conventions	23
1.8 Unit Macros	23
1.9 Command Line Interface (CLI)	24
1.10 File Servers	27
2 System	29
2.1 Information	29
2.2 Services	30
2.3 Hardware	38
2.4 Endpoints State Configuration	43
2.5 Event Log	49
2.6 Local Log	54
2.7 Packet Capture	55
2.8 Diagnostic	62
2.9 PCM Traces	63
2.10 VM	69
3 Network	84
3.1 Host	84

3.2 Interfaces	96
3.3 VLAN	106
3.4 QoS	108
3.5 Local Firewall	113
3.6 IP Routing	120
3.7 Network Firewall	124
3.8 NAT	128
3.9 DHCP Server	133
4 SIP Proxy	143
4.1 Configuring the SipProxy Service	143
5 SBC	145
5.1 Sentinel on the LAN	145
5.2 Sentinel on the Edge	146
5.3 Configuration	147
5.4 Rulesets	159
5.5 Registration	175
5.6 SBC Advanced Parameters	177
6 POTS	179
6.1 Basic Concepts	179
6.2 Basic FXS Tasks	183
6.3 Basic FXO Tasks	185
6.4 Advanced POTS Parameters	190
6.5 Examples of FXO Tone Detection	191
6.6 Cascade for Incoming Calls	193
6.7 Cascade for Outgoing Calls	194

7 ISDN	196
7.1 Cabling Information	196
7.2 Status	198
7.3 Primary Rate Interface	223
7.4 Basic Rate Interface (BRI)	227
7.5 Interop	230
7.6 Timer	231
7.7 Services	235
7.8 Other Advanced ISDN Parameters	236
8 R2 CAS	248
8.1 Status	248
8.2 R2 Configuration	250
8.3 Advanced R2 Tasks	253
8.4 Advanced R2 CAS Parameters	260
9 E and M CAS	261
9.1 Status	261
9.2 E and M Config	263
9.3 Advanced E and M Configuration Tasks	265
9.4 Advanced E&M CAS Parameters	269
10 SIP	270
10.1 Gateways	270
10.2 SIP Servers	275
10.3 Registrations	282
10.4 SIP Authentication	286

10.5 Transport	294
10.6 Interop	298
10.7 Misc	305
11 MEDIA	321
11.1 Codec	321
11.2 Security	338
11.3 RTP Statistics Configuration	343
11.4 Misc	348
12 Telephony	360
12.1 DTMF Maps	360
12.2 Call Forward	368
12.3 Telephony Services	369
12.4 Tone Customisation	378
12.5 Music on Hold	379
12.6 Misc	381
12.7 Advanced Telephony Parameters	386
12.8 Testing Telephony Services	388
12.9 Default Ports Used by DGW	396
13 Call Router	401
13.1 Call Router Basic Concepts	401
13.2 Basic Call Router Tasks	422
13.3 Routing Examples	449
13.4 Regular Expressions	450
14 Management	453

14.1 Configuration Scripts	453
14.2 Backup/Restore	471
14.3 Firmware	478
14.4 Certificates	483
14.5 SNMP Configuration	491
14.6 CWMP	493
14.7 Access Control	543
14.8 File	551
14.9 Misc	556
 15 Online Help	 558
 16 Acronyms	 559
 17 Glossary	 569
 18 DGW Documentation	 582
 19 Copyright Notice	 583

1 Getting started

1.1 Danger, Warning, Caution, and Note Definitions



Danger: Indicates a hazardous situation which, if not avoided, will result in death or serious injury.



Warning: Indicates a hazardous situation which, if not avoided, could result in death or serious injury.



Caution: Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury or damage to property or equipment.

Note: Indicates important information not related to personal injury.

1.2 Logon

1.2.1 Logging on to the Mediatrix Unit Web Interface

Before you start

The computer IP address must be in the same TCP/IP network as the Mediatrix unit.

Information

For better performances, it is recommended to use the latest available version of Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox.

Note: You may not be able to log on to the Mediatrix unit Web interface if you are using older browser versions.

Steps

- 1) In your Web browser, enter the IP address at which the Web interface of your Mediatrix unit can be reached.
 - If your network has an IPv4 DHCP server, connect the primary Ethernet port of the Mediatrix unit to the network (ETH1 port), use the provided DHCP server IP address.
 - You can also connect your computer to the secondary Ethernet port of the Mediatrix unit (ETH2), use the 192.168.0.10 IP address. However, the computer must also own an IP address in the 192.168.0.0/24 network.
- 2) Enter **admin** as your username and **administrator** as the password.

Note: You can also use **public** as a username and leave the password field empty; it has the full administration rights by default.

- 3) Click **Login**.

Result

The **Information** page of the Web interface is displayed.

1.3 Mediatrix Unit Reset

1.3.1 Basic Reset Concepts

1.3.1.1 Partial Reset

The partial reset provides a way to contact the Mediatrix unit in a known and static state while keeping most of the configuration unchanged.

A partial reset can be performed at the initial start-up of the Mediatrix unit or on a unit already in use where the configuration was modified in such a way that the user can no longer access the system by the Web page or otherwise. In both cases, the user can manage the Mediatrix unit through its Rescue interface, which is bound to the unit's WAN port (wan for the Mediatrix 4102S, and ETH1 for all other Mediatrix units). The IP address of the Rescue interface is 192.168.0.1 (IPv4) or an IPv6 Link Local address.. These connections give access to the Rescue Management Interface where the configuration of a new unit can be completed and where an existing configuration can be modified.

By default the Rescue Network Interface is disabled. When a partial reset is performed, the Rescue network Interface becomes enabled and the "Power" and "Ready" LEDs are blinking at 1Hz with 75% duty and all other LEDs are off. Once the configuration has been modified to solve the problem that required the partial reset, it is important to disable the Rescue Network Interface to make sure that you are no longer working in the Rescue Network Interface.

Performing a partial reset on a new unit will not modify the configuration, as it has not yet been modified to your needs. However, a partial reset performed on a unit already in use will:

- Rollback Local Firewall settings that are not yet applied.
- Add a Local Firewall rule to allow complete access to the Rescue interface.
- Rollback NAT settings that are not yet applied.
- Add NAT rule to allow complete access to the Rescue interface.
- Cancel the changes that were being modified but not yet applied to the configuration.
- Disable any Network Interface in conflict with the Network Rescue Interface.
- Configure and enable the Rescue Network Interface to:
 - use the link as the default value used by the Uplink Network Interface
 - set the IP address to 192.168.0.1 and the Network Mask to 255.255.255.0.
 - set the IPv6 link-local address on all network links. The IPv6 link-local address can be found underneath the unit.

A partial reset will also modify the following parameters and preserve the values below even after the Rescue interface has been disabled.

Note: These changes are valid when using a MX profile. If the Mediatrix unit is not using a MX profile, the default values and therefore the behaviour of the parameters may be different.

Service	Parameter	Default Value
AAA	Users.Password	User(s) from profile are restored with their factory password. All other usernames keep their password.
	Users.AccessRights	User(s) from profile are restored with their factory rights.
	ServicesAaaType (table)	Each service will be configured to use Local authentication and no accounting mechanism.
CLI	EnableTelnet	Disable
	TelnetPort	23
	EnableSsh	Enable
	SshPort	22
	InactivityTimeOut	15
Ha	servicesInfoExecState (Scm)	Stopped
	servicesInfoStartupType (Scm)	Manual
HOC	ManagementInterface	Rescue
SNMP	Port	161
	EnableSnmpV1	Enable
	EnableSnmpV2	Enable
	EnableSnmpV3	Enable
Web	ServerPort	80
	SecureServerPort	443

1.3.1.2 Factory Reset

The Factory reset reverts the Mediatrix unit back to its default factory settings.

It deletes the persistent configuration parameters of the unit, including:

- User files stored in the File service
- Certificates, except for factory installed ones
- Log files of the File service

The Factory reset should be performed with the Mediatrix unit connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, it will sent requests indefinitely. A Factory Reset can be triggered either:

- Directly on the unit. Refer to [Performing a Factory Reset](#) (p.13).
- Via the web interface of the Mediatrix unit (**Management/Firmware Upgrade**).
- Via the Command Line Interface of the Mediatrix unit by using the **fpu.defaultsetting** parameter.

1.3.1.3 RESET/DEFAULT Button

The **Reset/Default** button is a switch that can be used to perform a partial or factory reset while the unit is running.

In other words, the **Reset/Default** button can be used to:

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

The **Reset/Default** button will generate different actions depending on the amount of time the button is held.

IMPORTANT: It is the LED pattern that will indicate the action that is being applied to the unit. The action will occur more or less rapidly depending on the platform.

LED Pattern	Action	Comment
Power1 blinking, all other LEDs OFF	Restarts the Mediatrix unit.	No changes are made to the Mediatrix unit settings.
All LEDs blinking, 1 cycle per second, 50% duty	Initiates a Partial Reset of the Mediatrix unit. Note: The partial reset is optional as it can be disabled with the CLI Hardware.ResetButtonManagement parameter. For more details, refer to the DGW Configuration Guide - Reference Guide published on the Media5 Documentation Portal.	Restarts the unit in a known and static state while keeping most of the configuration unchanged.
All LEDs steady ON	Initiates a Factory Reset of the Mediatrix unit.	Reverts the unit back to its default factory settings.
All LEDs will become OFF after blinking and being steady on.	No action is taken. This is useful if you accidentally pushed the button and do not need an action to be applied.	The action is ignored.

1.3.2 Basic Reset Tasks

1.3.2.1 Performing a Partial Reset

Before you start

Note: It is not recommended to access the unit on a regular basis through the Rescue Network Interface.

Important: Make sure the unit is connected to the WAN port, as the Rescue interface is bound to the unit's WAN port (wan for the Mediatrix 4102S, and ETH1 for all other Mediatrix units). The IP address of the Rescue interface is 192.168.0.1 (IPv4) or an IPv6 Link Local address.

Steps

- 1) When the Power LED is steady or blinking rapidly, insert a small unbent paper clip into the hole of the **Reset/Default** button located on the Mediatrix unit.

Note: The Power LED will start blinking.

- 2) Wait a few seconds.

- 3) When all LEDs are blinking, but before they stop blinking, remove the paper clip.

Note: You have between 7 to 11 seconds.

Result

The Rescue Network Interface is displayed when accessing the Management Interface. Several parameters and services are modified, refer to [Partial Reset](#). Do not forget to perform the [Disabling the Rescue Interface](#) step.

1.3.2.2 Disabling Partial Reset - ResetButtonManagement

Steps

- 1) Open CLI (Command Line Interface).
- 2) Set **ResetButtonManagement** to **DisablePartialReset**.

Result

The Mediatrix unit will no longer partially reset the unit.

1.3.2.3 Performing a Factory Reset

Information

The Factory reset alters any persistent configuration data of the Mediatrix unit.

Steps

- 1) Insert a small, unbent paper clip into the hole of the **Reset/Default** button, located on the Mediatrix unit.

Note: Do not release the **Reset/Default** button before the LEDs stop blinking and are steadily ON. This can last from 12 to 16 seconds. If you leave the inserted pin longer, no action will be taken which is useful if you accidentally pushed the button and do not need any action to be applied.

- 2) Release the paper clip.

Result

All configuration parameters are reset to their default value. The unit can then be contacted via its WAN interface DHCP-provided IP address (ETH1 or WAN on the 4102S), or via its LAN interface default IP address 192.168.0.10 (ETH2 or LAN on the 4102S).

1.4 Personnal Data Usage and Protection

1.4.1 Personal Data Exposure

1.4.1.1 Personal Data Collection

Mediatrix products collect the basic personal data required for the proper delivery of the telecommunication service. The actual collected data depends on the type of users and how the Mediatrix products are administrated.

Type of users	Collected Personal Information	Collected Activity Information
End-Users	Name and phone number used to register to the telecommunication provider service.	Calls history for billing purposes and call details and recordings for troubleshooting purposes. For example: • Call date/time and duration • IP address • Voice or video stream • Fax or modem data stream • In-call digits dialled (DTMF) • E911 geo-localisation • Voicemail PIN • etc.

Type of users	Collected Personal Information	Collected Activity Information
System Administrators and Technical Support	Account name and password used to access the product for administrative and troubleshooting purposes.	- Logs of the administration and troubleshooting activities. - Audit trails of the administration and troubleshooting activities.

1.4.1.2 Personal Data Processing

Personal data is processed in Mediatrix products through the following activities:

- Configuring and storing end-user data
- Recording voice and fax calls
- Logging call history (CDR)
- Logging administration audit trails
- Access of the personal data by an authorised system administrator
- Provisioning data
- Maintenance, administration and technical support records
- Audit trails
- End-user activity records
- End-User personal content
- Recording voice and fax calls for troubleshooting

1.4.1.3 Personal Data Transfers

The following collected personal data may be transferred to other systems, depending on how the device administrators configure the Mediatrix products.

- Call Details Records (CDR) may be sent to an external call accounting system.
- Logs may be sent over an external monitoring system for live troubleshooting.
- Administration activity logs may be sent over an external monitoring system for auditing.
- Backups of the Mediatrix products, containing collected personal data, may be retrieved by an authorised system administrator.
- Network captures from the Mediatrix products, containing collected personal data, may be retrieved by an authorised system administrator for troubleshooting purposes.

1.4.2 Personal Data Protection

1.4.2.1 System and Data Protection

To protect the end-user personal data stored inside the Mediatrix devices, the device administrator should control and restrict access to the management interfaces by:

- Forcing the use of a strong authentication password
- Authorising LAN access only
- Using the device firewall service to limit the remote access to the device to only authorized peers and authorised services
- Using an external firewall
- Enabling IEEE 802.1x authentication of Ethernet link

The device administrator may also enforce the use of encryption and authentication for a secure administration of the Mediatrix devices:

- Authenticated Management Interfaces:
 - Web Interface: HTTPS with trusted certificates
 - CWMP: HTTPS with trusted certificates
 - CLI: SSH
- Secure Management Operations:
 - Consult or retrieve the stored personal data: HTTPS with trusted certificates
 - Provisioning: HTTPS with trusted certificates
 - Firmware upgrades: HTTPS with trusted certificates
 - Backup/restore: HTTPS with trusted certificates

1.4.2.2 Communications Protection (VoIP Calls)

The device administrator may configure the encryption of the data that transits through Mediatrix products:

- Call signalling: SIP over TLS with trusted certificates
- Media packets: SRTP

1.4.2.3 Access and Communications

The Mediatrix products have three (3) default account roles:

- Administrator
- User (no password access)
- Observer (read-only)

All the management interfaces are restricted to authorised accounts only, verified by username and password. Refer to the [System and Data Protection](#) (p.16) section for the list of management interfaces and how to protect them.

The account credentials may be stored locally in the Mediatrix devices or in an external RADIUS authentication server.

In all cases, the device administrator should restrict the physical access to the Mediatrix products.

1.4.2.4 Data Deletion

The Mediatrix products allow an authorised system administrator to delete end-user registration information (name and number).

A system administrator should also delete any temporary logs that may have been stored locally during a troubleshooting session such as:

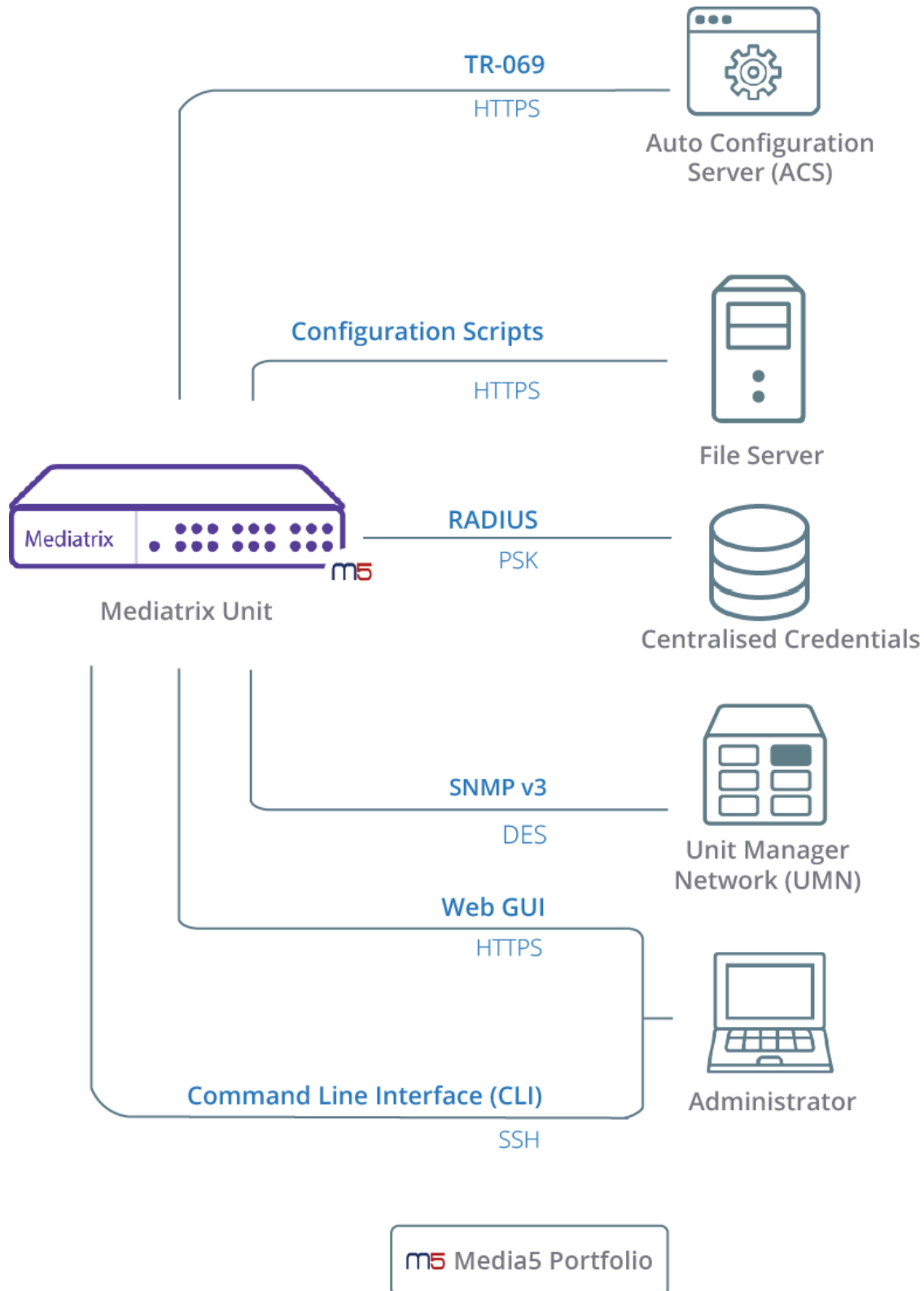
- call history
- call recordings
- network captures

A factory reset can be performed by a system administrator to revert a Mediatrix device back to its default factory state through a factory reset, thus erasing all the collected data and configuration.

1.4.2.5 Audit

Audit trail logs of the system administrator activities may be enabled by the device administrator. These audit logs may be temporarily stored locally or sent through syslog to an external monitoring system.

1.5 Management Interfaces



1.6 IPv6

1.6.1 Basic IPv6 Concepts

1.6.1.1 IPv6

IPv6 (Internet Protocol version 6) is the successor to the most common Internet Protocol today (IPv4).

This is largely driven by the fact that IPv4 32-bit addresses are quickly being consumed by the ever-expanding sites and products on the Internet. IPv6 128-bit address space should not have this problem for the foreseeable future.

IPv6 addresses, in addition to being longer, are distinguished from IPv4 addresses by the use of colons ":", e.g. 2001:470:8929:4000:201:80ff:fe3c:642f. An IPv4 address is noted by 4 sets of decimal numbers separated by periods ".", e.g. 192.168.10.1.

Please note that IPv6 addresses should be written between [] to allow port numbers to be set.

For instance, [fd0f:8b72:5::1]:5060.

1.6.1.2 IPv6 Availability

DGW supports IPv6 except for:

- CPE WAN Management Protocol (CWMP)/TR-069
- DHCP embedded sever
- IP Routing
- Local Firewall (LFW)
- Network Firewall (NFW)
- Network Address Translation (NAT)
- Online Certificate Status Protocol (OSCP)
- Remote Authentication Dial In User Services (RADIUS)
- Session Border Controller (SBC)
- Simple Network Management Protocol (SNMP)
- PPPoE

1.6.1.3 IPv6 link-local Addresses

IPv6 link-local addresses start with fe80 and must include the scope identifier

Therefore, the format of a link-local address is: [IPv6 link-local%ScopeIdentifier].

The scope identifier corresponds to:

- On Windows: the network link used to contact the IPv6 link-local address.
- On Linux: the link name or the interface number.

For example, if the unit must contact a server at the IPv6 link-local fe80::201:80ff:fe3c:642f address, you must check on which network link the server is available. Some units have WAN or LAN. If it is on the WAN link, the IP address would then be "[fe80::201:80ff:fe3c:642f%wan]".

1.6.2 IPv6 Basic Tasks

1.6.2.1 Locating the Scope Identifier of fe80 IPv6 Addresses on Windows

Information

IMPORTANT: If the Mediatrix unit is configured to use IPv6 addresses and the firmware is downgraded to a version that does not support IPv6, then all IPv6 networks are deleted.

Steps

- 1) Open the Windows Command Line interface.
- 2) Type **ipconfig**.
- 3) Locate the IPv6 address.

Note: The IPv6 address starts with fe80.

- 4) Locate the interface number in the IPv6 address.

Note: the interface number is at the end of the address, after the %.

Result

In the following example, the interface number of the [fe80::201:80ff:fe3c:642f%4] IPv6 address is 4.

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

Windows IP Configuration

Ethernet adapter Wan:

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

1.6.2.2 Locating the Scope Identifier of fe80 IPv6 Addresses on Linux

Information

IMPORTANT: If the Mediatrix unit is configured to use IPv6 addresses and the firmware is downgraded to a version that does not support IPv6, then all IPv6 networks are deleted.

Steps

- 1) Open the Linux Command Line interface.
- 2) Type **ipconfig**.
- 3) Locate the IPv6 address.

Note: The IPv6 address starts with fe80.

- 4) Locate the interface number in the IPv6 address.

Result

In the following example, to contact the IPv6 link-local IPv6 address "fe80::201:80ff:fe3c:642f", you would use: [fe80::201:80ff:fe3c:642f%2] or [fe80::201:80ff:fe3c:642f%eth0].

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

1.7 Naming Conventions

When defining a name for a parameter, only ascii characters are authorised.

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

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

1.7.1 ASCII Special Characters

The DGW v2.0 Application does not support ASCII special characters higher than 127.

1.8 Unit Macros

Macro	Description
%mac%	the MAC address of the unit
%version%	the MFP version of the unit (firmware version)
%product%	the Product name of the unit
%productseries%	the Product series name of the unit.

1.9 Command Line Interface (CLI)

1.9.1 CLI Basic Concept

1.9.1.1 Command Line Interface (CLI)

The Command Line Interface (CLI) provides an access to interactively configure all the Mediatrix unit parameters.

IMPORTANT: Although it is possible to configure existing ruleset parameters via the CLI, it is not possible to create or edit a ruleset from the CLI: it must be either imported or directly created or edited in the DGW Web interface.

The CLI is accessed through either a secure SSH session (default) or an unsecure TELNET session. When using a secure SSH session, all communications between Client and server are encrypted before being sent over the network, thus packet sniffers are unable to extract user names, passwords, and other potentially sensitive data. This is the default and recommended way to access the Command Line Interface.

The command interpreter interface of the CLI allows the user to browse the unit parameters, write the command lines, and display the system's notification log.

1.9.2 CLI Basic Tasks

1.9.2.1 Creating the Telnet Session Activation Configuration Script

Steps

- 1) Open a text editor.
- 2) Copy and paste the text included in the following Result section.

Note: If necessary, you can customise the value of the **Cli.InactivityTimeout** and **Cli.TelnetPort** parameters.

- 3) Save the file as **telnet.cfg**

Result

The configuration script to enable Telnet sessions is created but needs to be imported to the unit.


```
1
2
3 #####
4 # Configuration Script
5 # Activating the CLI access via Telnet.
6 #####
7 # CLI
8 # Set the inactivity expiration delay for exiting the CLI session.
9 # This value is expressed in minutes.
10
11 Cli.InactivityTimeout = "15"
12 # Enable Telnet access to the CLI
13 Cli.EnableTelnet = "Enable"
14 # Specify the port to use
15 Cli.TelnetPort = "23"
```

1.9.2.2 Accessing the CLI via a Telnet Session

Information

IMPORTANT: Remember that when using a Telnet session to access the CLI, communications between Client and server are not secured, thus packet sniffers are able to extract user names, passwords, and other potentially sensitive data. Therefore, Media5 Corporation strongly recommends using an SSH session.

Before you start

Your unit must be properly connected. Refer to the [Hardware Installation Guide](#) of your unit published on the [Media5 Documentation Portal](#).

Steps

- 1) Start your Telnet Client.
- 2) Enter the IP address of your unit.
- 3) Enter the port number **23**.
- 4) Select **Telnet** as the connection type.
- 5) When prompted for login, enter your login username (Default usernames are **public** or **admin**).
- 6) Enter your login password (for the default **admin** username, the password is **administrator**, for the **public** username, no password is required).

Note: If you are accessing the unit through the CLI for the first time or after a factory reset, you may be presented with a warning message regarding the unit's identification. You can accept the message and continue.

Result

After you have successfully connected to the Mediatrix unit by using a Telnet session, you can start using the CLI to configure the Mediatrix unit. For more details on the scripting language,

refer to the [DGW Configuration guide - Configuration Scripting Language Syntax](#) published on the [Media5 Documentation Portal](#).

1.9.2.3 Accessing the CLI via an SSH Session

Before you start

Your unit must be properly connected. Refer to the [Hardware Installation Guide](#) of your unit published on the [Media5 Documentation Portal](#).

Information

This is the recommended way to access the CLI.

Steps

- 1) Start your SSH Client.
- 2) Enter the IP address of your unit.
- 3) Use the SSH default port number, i.e. **22** unless, you have previously changed it in the DGW Web interface under **Management/Misc**.
- 4) Select **SSH** as the connection type.
- 5) When prompted for login, enter your login username (Default usernames are **public** or **admin**).
- 6) Enter your login password (for the default **admin** username, the password is **administrator**, for the **public** username, no password is required).

Note: If you are accessing the unit through the CLI for the first time or after a factory reset, you may be presented with a warning message regarding the unit's identification. You can accept the message and continue.

Result

After you have successfully connected to the Mediatrix unit by using an SSH session, you can start using the CLI to configure the Mediatrix unit. For more details on the scripting language,

refer to the [DGW Configuration guide - Configuration Scripting Language Syntax](#) published on the [Media5 Documentation Portal](#).

1.10 File Servers

1.10.1 Configuring the FTP Server

Before you start

If you are not familiar with the procedure on how to set the FTP root path, please refer to your FTP server's documentation.

Information

Perform this procedure if you plan to use the FTP transport protocol.

Steps

- 1) Set an FTP service on the assigned server.
- 2) Make sure the FTP server can be reached by the Mediatrix unit.

Note: If the file server is located behind a firewall, make sure that TCP port 21 is open.

1.10.2 Configuring the HTTP Server

Before you start

If you are not familiar with the procedure on how to set the HTTP root path, refer to your HTTP server's documentation.

Information

Perform this procedure if you plan to use the HTTP transport protocol.

Steps

- 1) Set an HTTP service on the assigned server.

- 2) Make sure the HTTP server can be reached by the Mediatrix unit.

Note: If the file server is located behind a firewall, make sure the TCP port 80 is open.

1.10.3 Configuring the HTTPS Server

Before you start

If you are not familiar with the procedure on how to set the HTTPS root path, please refer to your HTTPS documentation.

Make sure the unit is set to the proper date (refer to [Configuring the Mediatrix Unit to Use an SNTP Server](#) (p.94).

Information

Perform this procedure if you plan to use the HTTPS transport protocol.

Steps

- 1) Set an HTTPS service on the assigned server.
- 2) Make sure the HTTPS server can be reached by the Mediatrix unit.

Note: If the file server is located behind a firewall, make sure the TCP port 443 is open.

- 3) Make sure that in the **Management/Certificates** tab, in the **Certificate Import Through Web Browser** table, there is a certificate that authenticates the HTTPS server selected in the **Path** field, and that **Other** is selected in the **Type** field.
- 4) Set the configuration parameters.

1.10.4 Configuring the TFTP Server

Before you start

If you are not familiar with the procedure on how to set the TFTP root path, please refer to your TFTP server's documentation.

Information

Perform this procedure if you plan to use the TFTP transport protocol.

Steps

- 1) Set a TFTP service on the assigned server.
- 2) Make sure the TFTP server can be reached by the Mediatrix unit.

Note: If the file server is located behind a firewall, make sure the UDP port 69 is open.

2 System

2.1 Information

2.1.1 Activating a Licence Using the Web Interface

Before you start

You must have received the licence key for your specific unit .

Steps

- 1) Go to **System/Information**.
- 2) In the **Activate Licence** table, enter your licence key.

Note: A licence key is generated for one specific unit only, therefore it cannot be used on another unit.

- 3) Click **Apply**.
- 4) Validate that the Licences table now displays the Licences.
- 5) At the top of the screen, **restart required services**.

Result

Licences		
	CWMP/TR-069	
	SBC Licence for 10 concurrent sessions	
	Virtual Machine Licence	
	Survivability Licence with 25 users	

Activate Licence		
Licence Key:	\$Example	

2.2 Services

2.2.1 Basic Service Concepts

2.2.1.1 Services

The Mediatrix unit uses many services to carry out tasks and support features.

There are two types of services:

- system services : You cannot perform service commands on system services. The service is restarted by using the **Reboot** button located under the **Reboot** tab of the DGW Web interface.

Note: If the unit is in use when clicking **Reboot**, all calls are terminated.

- user services: You can perform service commands on user services. The service is restarted by using the start

 button located under the **Services** tab of the DGW Web interface, next to the service.

Note: Available services may differ depending on the Mediatrix unit you are using. Available services are displayed on the DGW Web page, under **System/Services**.

When a service needs to be restarted, the **restart required services** is systematically displayed. If you are not able to restart a service because it is a system service, click the Reboot link in the top menu. The Reboot page then opens. You must click Reboot. This restarts the Mediatrix unit. If the unit is in use when you click Reboot, all calls are terminated

Services can also be restarted via the CLI using the Scm.ServiceCommandsRestart parameter.

2.2.1.2 System Services vs User Services

The Mediatrix unit uses many services to carry out tasks and support features.

There are 3 service commands that can be used:

- Start
- Stop
- Restart

There are two types of services:

- **system services:** the user cannot perform service commands. The service can only be restarted by rebooting the unit. Refer to [Restarting a System Service](#) (p.36).
- **user services:** the user can perform service commands. The service can be restarted by the user. Refer to [Setting the Service Start-up Type](#) (p.34)

Note: Available services may differ depending on the Mediatrix unit you are using. Furthermore, some services are available only if a licence has been installed. Available services are displayed on the DGW Web page, under **System/Services**.

When a system or a user service needs to be restarted, the **Some changes require to restart a service to apply new configuration** message is systematically displayed on the DGW Web pages. Also, every service has the **NeedRestartInfo** CLI/MIB parameter to indicate if the service needs to be restarted for the configuration to fully take effect.

Note: For the complete list of parameters and commands available for the configuration of each service, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

2.2.1.3 DGW User Services

User Service	Description
Basic Network Interface (Bni)	Manages the layer 3 network interfaces.
Call Detail Record (Cdr)	Allows the administrator to generate custom call notifications with information such as endpoints, point of origin, duration, etc.
Command Line Interface (Cli)	Allows the administrator to manage the unit using the SSH or TELNET protocols.
Call Routing (Crout)	Transforms properties and routes calls between telephony interfaces and SIP endpoints.
CPE WAN Management Protocol (Cwmp)	Allows the administrator to manage the unit using the TR-069 protocol.
DHCP Server (Dhcp)	Manages a DHCP server on each network interface.
E&M Channel Associated Signaling (Eam)	Manages the E&M CAS telephony interfaces.
Element Management System for Virtuo (EMS)	Makes the unit compatible with the Virtuo EMS infrastructure.
Endpoint Administration (EpAdm)	Allows for high-level management of telephony endpoints.
Endpoint Services (EpServ)	Manages the telephony services of each endpoint.
IP routing (IpRouting)	Manages the unit's IP routing table.
Integrated Services Digital Network (Isdn)	Manages the ISDN parameters for BRI and PRI telephony interfaces.
Local Firewall (Lfw)	Allows the administrator to filter the network with the unit as final destination.
Link Layer Discovery Protocol (Lldp)	Manages the IEEE 802.1ab protocol used for advertising the unit's capabilities on the network.
Media IP Transport (Mipt)	Manages the voice and data encodings over the IP network.
Music on Hold (Moh)	Manages the option to play an audio file when a telephony endpoint is on hold.
Network Address Translation (Nat)	Allows the administrator to change the source or destination IP address of a packet.

User Service	Description
Network Firewall (Nfw)	Allows the administrator to filter traffic that is routed between networks.
Network Traffic Control (Ntc)	Allows the administrator to perform traffic shaping on the network interfaces.
Plain Old Telephony System Line (Pots)	Manages the FXS and FXO analog telephony interfaces.
R2 Channel Associated Signaling (R2)	Manages the E1 CAS telephony interfaces
Session Border Controller (Sbc)	Allows the administrator to perform SIP to SIP normalization, call routing, NAT traversal, and survivability.
SIP Endpoint (SipEp)	Allows the administrator to associate telephony endpoints with SIP user agents.
SIP Proxy (SipProxy)	The SIP Proxy (SipProxy) service is used to add local survivability for local endpoints and SIP phones.
Simple Network Management Protocol (Snmp)	Allows the administrator to manage the unit using the SNMP protocol.
Telephony Interface (TelIf)	Manages tone generation and detection on the telephony interfaces.
Virtual Machine (Vm)	Allows the administrator to manage virtual machines.
Web Service (Web)	Manage the unit using HTTP(S) web pages.

2.2.1.4 DGW System Services

System Service	Description
Authentication, Authorization and Accounting (Aaa)	Manages the administrator accounts and grants or denies access to various parameters.
Certificate Manager (Cert)	Manages the security certificates used for the authentication of the unit and its peers before establishing a secure connection.
Configuration Manager (Conf)	Allows executing configuration scripts as well as performing backup/restore of the unit configuration.
Device Control Manager (Dcm)	Manages the hardware properties as well as the licence activation keys.
Ethernet Manager (Eth)	Manages the unit Ethernet link interfaces.
File Manager (File)	Allows the administrator to manage the files stored on the unit.
Firmware Pack Updater (Fpu)	Manages firmware upgrade, downgrade and rollback operations.
Host Configuration (Hoc)	Manages the IP host parameters and other system settings.
Local Quality Of Service (LQos)	Manages the QoS parameters applicable to the unit.
Notifications and Logging Manager (Nlm)	Manages the routing and filtering of the unit's event notification messages.
Process Control Manager (Pcm)	Manages the startup and shutdown sequence of the system.
Service Controller Manager (Scm)	Allows the administrator to enable or disable services.

2.2.2 Basic Service Tasks

2.2.2.1 Setting the Service Start-up Type

Steps

- 1) Go to **System/Services**.

- 2) In the **User Service** table, from the **Startup Type** selection list located next to the service you wish to set.
 - choose **Auto** if you wish the service to start automatically when the system starts, or
 - choose **Manual** to start to the service manually when needed.
- 3) Click **Apply**.

Result

The services set to **Auto** will automatically start every time the unit boots, while the services set to **Manual** must be started each time by the administrator when needed.

2.2.2.2 Starting/Stopping/Restarting a User Service Using the DGW Web Page

Steps

- 1) Go to **System/Services**.
- 2) In the **User Service** table, on the line of the service you wish to set.
 - click  if you wish to start the service, or
 - click  to restart the service.
 - click  to stop the service.

Note: When stopping or restarting a service, some interruptions might occur, such as dropped calls, virtual machine shutdown or loss of network connectivity, depending on the affected services and/or its dependencies.

- 3) Click **Apply**.

Result

The status of the service (in the **Status** column) changes following the executed service command.

- If you clicked , the tab from which you can access the service from the Web pages are greyed out
- If you clicked , the tab from which you can access the service from the Web pages are no longer greyed out.

2.2.2.3 Disabling a Service

Steps

- 1) Go to **System/Services**.

- 2) In the **User Service** table, on the line of the service you wish to disable, click  to stop the service.

Note: When stopping a service, some interruptions might occur, such as dropped calls, virtual machine shutdown or loss of network connectivity, depending on the affected services and/or its dependencies.

- 3) In the **User Service** table, from the **Startup Type** selection list located next to the service you wish to disable, choose **Manual**.
- 4) Click **Apply**.

Result

The service will be stopped and will not be restarted automatically at the next unit start-up.

2.2.2.4 Restarting a Service with a Grace Delay

Information

If no service needs to be restarted, the table will be greyed out.

Steps

- 1) Go to **System/Services**.
- 2) In the **Restart Required Services** table, set the **Graceful Delay (min)** field.
- 3) Click **Restart Required Services**.

Result

The services that require a restart are restarted after the delay allowing ongoing calls to be completed. At the expiration of the delay, the services are forced to restart even if calls are still ongoing. Therefore, ongoing calls are abruptly disconnected without proper release. The users are not informed of the call disconnection event (ex.: end-of-call tone).

Restart Required Services	
Graceful Delay (min)	2 Cancel Restart Required Services

2.2.2.5 Restarting a System Service

Information

System services cannot be restarted by the user. To restart a system service, the unit must be restarted.

Steps

- 1) Go to **Reboot**.
- 2) In the **Reboot** page, click **Reboot**.

Note: If the unit is in use when clicking **Reboot**, all calls are terminated.

Result

The Web session will be lost and you will be redirected to the login page after the reboot process. All system services needing to be restarted, will be restarted.

2.2.3 Advanced Service Tasks

2.2.3.1 Starting/Stopping/Restarting a User Service Using a MIB Browser

Steps

- 1) Open a MIB Browser
- 2) Navigate to the Service that needs to be restarted.
- 3) Locate the **needRestartInfo** parameter to determine if the service needs to be restarted.
- 4) In the scmMIB, locate the serviceCommandsTable .
- 5) In the **serviceCommandsName** column, locate the service to restart.
 - a) To restart the service, set the **serviceCommandsRestart** column to **restart**
 - b) To start the service, set the **serviceCommandsStart** column to **Start**
 - c) To stop the service, set the **serviceCommandsStop** column to **Stop**

Note: Stopping or restarting a service will cause an interruption in that service, which may result for example in network lost, call interruption, or virtual machine shutdown, depending on the service(s) stopped or restarted.

2.2.3.2 Starting/Stopping/Restarting a Service Using the CLI

Information

For more details, refer to the [Technical Bulletin - Using the CLI via an SSH Session](#) published on the [Media5 Documentation Portal](#).

Steps

- 1) Log into the CLI using an SSH client.

2) Type : .

- a) scm.ServiceCommands[Name=ServiceName].Start=Start to start a service
- b) scm.ServiceCommands[Name=ServiceName].stop=stop to stop a service
- c) scm.ServiceCommands[Name=ServiceName].restart=restart to restart a service,

Note: Stopping or restarting a service will cause an interruption in that service, which may result for example in network lost, call interruption, or virtual machine shutdown, depending on the service(s) stopped or restarted.

2.3 Hardware

2.3.1 Hardware Basic Tasks

2.3.1.1 Selecting the Source of the Clock Reference

Steps

- 1) Go to **System/Hardware**.
- 2) From the **Clock Reference Configuration** table, select from the **Suggestion** list, several clock reference sources.
- 3) Click **Apply**.

Result

The selected **Clock Reference** sources for each available telephony card, according to the unit type, are displayed in the **Value** field of the **Clock Reference Configuration** table. The first selected source will be used as a the clock reference. The following one will be used as the fallback source, in the listed order, if the first one becomes unavailable. Only one source is used at a time for the **Clock Reference**.

Clock Reference Configuration			
	Value	Suggestion	
Clock Reference Source:	Telephony interface	--- Suggestion --- ▼	

2.3.1.2 Selecting the Port Used for Synchronisation

Steps

- 1) Access the DGW Web interface of your unit.
- 2) Go to **System/Hardware**.

- 3) In the **Clock Reference Configuration** table, from the **Suggestion** selection list, choose **SYNCIN**.

Result

The unit will be synchronised on the **SYNC IN** port.

Clock Reference Configuration		Suggestion	
Value			
Clock Reference Source:	SYNCIN	--- Suggestion ---	

2.3.1.3 Associating a PRI Port to a Line Type and Protocol

Steps

- 1) Go to **System/Hardware**.
- 2) In the **PRI Ports Configuration** table, from the **Line Type** selection list, select either E1 or T1.
- 3) From the **Signaling** selection list, associate a type of signaling to the PRI port.
- 4) Click **Apply**.
- 5) Restart the unit.

Result

The selected line type will appear under **ISDN/Primary Rate Interface**. This is an example of a PRI port association.

PRI Ports Configuration			
Port	Line Type	Signaling	
Slot1/E1T1	E1	Isdn	
Slot3/E1T1	E1	Isdn	

2.3.1.4 Setting the Mediatrix Unit to Use the R2 Signaling Protocol

Before you start

R2 signaling protocol can only be used on E1 line type.

Steps

- 1) Go to **System/Hardware**.

- 2) In the **PRI Cards Configuration** table, from the **Signaling** selection list, located on the same line as the port you wish to dedicate to R2 signaling, choose **R2**.

Note: When changing from R2 to ISDN or ISDN to R2, you must change your routes accordingly (Call Router/Route Config).

- 3) From the **Line Type** selection list, make sure **E1** is selected.
- 4) Click **Apply**.
- 5) Restart the unit.

Result

PRI Ports Configuration			
Port	Line Type	Signaling	
Slot1/E1T1	E1 ▼	Isdn ▼	
Slot2/E1T1	E1 ▼	R2 ▼	

2.3.1.5 Setting the Mediatrix Unit to Use the E&M Signaling Protocol

Steps

- 1) Go to **System/Hardware**.
- 2) In the **PRI Ports Configuration** table, located on the same line as the port you wish to dedicate to **E&M** signaling, from the **Signaling** selection list, choose **E&M**.

Note: When changing from E&M to ISDN/R2 or ISDN/R2 to E&M, you must change your routes accordingly. For instance, if you are in ISDN with a route isdn-Slot2/E1T1, then change to E&M, you must change the route to e&m-Slot2/E1T1.

- 3) From the **Line Type** selection list, choose **T1**.
- 4) Click **Apply**.
- 5) Restart the unit.

Result

PRI Ports Configuration			
Port	Line Type	Signaling	
Slot1/E1T1	T1 ▾	E&M ▾	

2.3.1.6 Cabling Several Units for TDM Synchronisation

Information

Cabling is done using straight cables in a daisy chain.

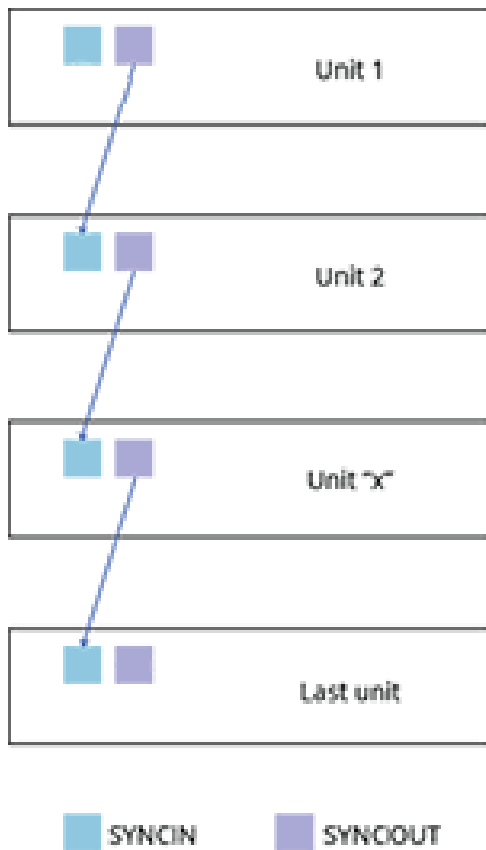
Before you start

The common practice is to have the first unit act as the Clock Master.

Steps

- 1) Connect a standard Ethernet cable to the **SYNC OUT** port of the first device.
- 2) Connect the other end of the Ethernet cable to the **SYNC IN** port of another device.
- 3) Connect all your units in the same fashion.

Result



2.3.2 Hardware Advanced Parameters

Some aspects of the Hardware configuration can only be completed with the MIB parameters.

These parameters can be accessed and configured by:

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

For the complete list of available parameters, refer to the Hardware section of the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

2.4 Endpoints State Configuration

2.4.1 Basic Endpoints State Concepts

2.4.1.1 Administrative State of Unit

The administrator can disable the use of specific endpoints or all endpoints of a unit through the administrative state configuration. It is also possible to select the initial endpoint state to be applied on unit start-up.

Disabling endpoints of a unit can be useful for example:

- in a multi-tenant environment, if a tenant stops its service subscription, the administrator can lock the unit so the FXS port can give either a fast busy tone or no tone to signal the line is decommissioned. Then later the administrator can send a technician on site to re-wire and make the port available to another tenant.
- if a user does not pay his service, the administrator can simply lock the endpoint.
- to prevent calls during unit maintenance

Note: Locking an endpoint also removes SIP registration from the endpoint prohibiting calls from and to the endpoint.

2.4.2 Basic Endpoint State Tasks

2.4.2.1 Locking All Unit Endpoints - Gracefully

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Unit States** table, from the **Action** selection list, choose **Lock**.

Result

New calls can no longer be sent or received.

- If the state of the unit is **Idle** or **Idle Unusable**, the unit is locked right away.

- If the unit is either **Busy** or **Active**, the unit will be locked only when it will become **Idle**.

Unit States				
Administrative	Operational	Usage	Action	
Locked	Disable	Idle Unusable	Force Lock Lock Unlock	

2.4.2.2 Locking All Unit Endpoints - Immediately

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Unit States** table, from the **Action** selection list, choose **Force Lock**.

Result

All telephone lines of the unit are locked immediately even if there are calls in progress, in which case the call will be immediately terminated (BYE sent to the SIP peer and end-of-call tone played to the endpoint). Locking all unit endpoints prevents any call activities.

Unit States				
Administrative	Operational	Usage	Action	
Locked	Disable	Idle Unusable	Force Lock Lock Unlock	

2.4.2.3 Unlocking All Unit Endpoints

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Unit States** table, from the **Action** selection list, choose **Unlock**.

Result

The unit becomes available for use.

Unit States	Administrative	Operational	Usage	Action	
Locked		Disable	Idle Unusable	v	
				Force Lock	
				Lock	
				Unlock	

2.4.2.4 Locking an Endpoint - Gracefully

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Endpoint States** table, from the **Action** selection list of an endpoint, choose **Lock**.

Result

The endpoint will no longer be able to send or receive a call.

- If the state of the endpoint is **Idle** or **Idle Unusable**, the endpoint is locked right away.
- If the endpoint is either **Busy** or **Active**, the endpoint will be locked only when the unit will become in **Idle**.

Endpoint States						
Endpoint	Administrative	Operational	Usage	Initial Administrative	Action	
Slot1/E1T1	Unlocked	Disable	Idle Unusable	Unlocked v	v	
Slot3/FXS1	Unlocked	Disable	Idle Unusable	Unlocked v		
Slot3/FXS2	Unlocked	Disable	Idle Unusable	Unlocked v	Force Lock	
Slot3/FXS3	Unlocked	Disable	Idle Unusable	Unlocked v	Lock	
Slot3/FXS4	Unlocked	Disable	Idle Unusable	Unlocked v	Unlock	
Slot4/FXO1	Unlocked	Disable	Idle Unusable	Unlocked v	v	
Slot4/FXO2	Unlocked	Disable	Idle Unusable	Unlocked v	v	
Slot4/FXO3	Unlocked	Disable	Idle Unusable	Unlocked v	v	
Slot4/FXO4	Unlocked	Disable	Idle Unusable	Unlocked v	v	

2.4.2.5 Locking an Endpoint- Immediately

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Endpoint States** table, from the **Action** selection list of an endpoint, choose **Force Lock**.

Result

All activities of the endpoint are stopped immediately, even if there are calls in progress, in which case the call will be immediately terminated (BYE sent to the SIP peer and end-of-call tone played to the endpoint).

Endpoint States							
Endpoint	Administrative	Operational	Usage	Initial Administrative	Action		
Slot1/E1T1	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot3/FXS1	Unlocked	Disable	Idle Unusable	Unlocked ▾			
Slot3/FXS2	Unlocked	Disable	Idle Unusable	Unlocked ▾	Force Lock		
Slot3/FXS3	Unlocked	Disable	Idle Unusable	Unlocked ▾	Lock		
Slot3/FXS4	Unlocked	Disable	Idle Unusable	Unlocked ▾	Unlock		
Slot4/FXO1	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO2	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO3	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO4	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		

2.4.2.6 Unlocking an Endpoint

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Endpoint States** table, from the **Action** selection list of an endpoint, choose **Unlock**.

Result

The endpoint becomes available for use.

Endpoint States							
Endpoint	Administrative	Operational	Usage	Initial Administrative	Action		
Slot1/E1T1	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot3/FXS1	Unlocked	Disable	Idle Unusable	Unlocked ▾			
Slot3/FXS2	Unlocked	Disable	Idle Unusable	Unlocked ▾	Force Lock		
Slot3/FXS3	Unlocked	Disable	Idle Unusable	Unlocked ▾	Lock		
Slot3/FXS4	Unlocked	Disable	Idle Unusable	Unlocked ▾	Unlock		
Slot4/FXO1	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO2	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO3	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		
Slot4/FXO4	Unlocked	Disable	Idle Unusable	Unlocked ▾	▾		

2.4.2.7 Setting the Endpoint Behavior after a Unit Restart

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Endpoint States** table, from the **Initial Administrative** selection list of an endpoint, choose **Lock** or **Unlock**.

Result

- If the **Initial Administrative** selection list is set to **Lock**, when the unit restarts, the endpoint will remain locked, therefore unusable.

- If the **Initial Administrative** selection list is set to **Unlocked**, when the unit restarts, the endpoint will become usable.

Endpoint States						
Endpoint	Administrative	Operational	Usage	Initial Administrative	Action	
Slot1/E1T1	Unlocked	Disable		Unlocked		
Slot3/FXS1	Unlocked	Disable		Locked		
Slot3/FXS2	Unlocked	Disable		Unlocked		
Slot3/FXS3	Unlocked	Disable		Unlocked		
Slot3/FXS4	Unlocked	Disable		Unlocked		
Slot4/FX01	Unlocked	Disable		Unlocked		
Slot4/FX02	Unlocked	Disable		Unlocked		
Slot4/FX03	Unlocked	Disable		Unlocked		
Slot4/FX04	Unlocked	Disable		Unlocked		

2.4.2.8 Disabling the Unit Endpoints when No Gateways are Ready

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Administration** table, select **Enable** next to **Disable Unit (All Endpoints) when No Gateways Are In State Ready**.

Result

The unit will be disabled, i.e. unusable, if none of the SIP gateways are ready to be used. As soon as a SIP gateway becomes ready, the unit will be enabled.

Administration			
Disable Unit (All Endpoints) When No Gateways Are In State Ready:		Enable	
Shutdown Endpoint When Operational State is Disable And Its Usage State Is 'idle-unusable':		Enable	
Disable All Gateways When Trunk Lines Are Down:		Enable	

2.4.2.9 Shutting Down Endpoint if in Idle-Unusable State

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Administration** table, select **Enable** next to **Shutdown Endpoint When Operational State is Disable And Its Usage State is idle-unusable**.

Note: The **Shutdown Endpoint When Operational State is Disable And Its Usage State is idle-unusable** parameter is always interpreted as disabled unless it has been specifically set to enable.

Result

When an endpoint usage state becomes **Idle-unusable** whatever the value of its operational state, the endpoint remains physically up but the calls are denied.

Administration	
Disable Unit (All Endpoints) When No Gateways Are In State Ready:	Enable ▾
Shutdown Endpoint When Operational State is Disable And Its Usage State Is 'idle-unusable':	Enable ▾
Disable All Gateways When Trunk Lines Are Down:	Enable ▾

2.4.2.10 Disabling All Gateways when Trunk Lines are Down

Steps

- 1) Go to **System/Endpoints**.
- 2) In the **Administration** table, select **Disable** next to **Disable Unit (All Endpoints) when No Gateways Are In State Ready**.

Note: This applies only to E1 or T1 telephony lines.

Result

When all E1 or T1 telephony lines are down, all SIP gateways will be stopped. All SIP gateways will be started when at least one E1/T1 line is up.

Administration	
Disable Unit (All Endpoints) When No Gateways Are In State Ready:	Enable ▾
Shutdown Endpoint When Operational State is Disable And Its Usage State Is 'idle-unusable':	Enable ▾
Disable All Gateways When Trunk Lines Are Down:	Enable ▾

2.4.3 Advanced System/Endpoints Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the Configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following advanced parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Setting the toggle delay to disable the SIP gateways when trunk lines are down

[EpAdm.DisableSipGatewaysWhenTrunkLinesDownToggleDelay](#)

Setting the Behavior of the unit While in Shutting Down State

[EpAdm.BehaviorWhileInUnitShuttingDownState](#)

2.5 Event Log

2.5.1 Basic Event Log Concepts

2.5.1.1 Event Notifications

An event is something that happens in the system and that needs to be reported. Event notifications are formatted text messages issued by the DGW software to signal something of interest to the unit administrator.

Event Notifications are used to generate alarms in the customer's system and to monitor the system. It is possible to control:

- for which service event notifications will be reported;
- which event notifications will be reported based on the severity level of the event;
- if a specific event notification should be reported or not;
- where the event notifications will be logged.

For example, it is possible to log all event notifications raised for the Call Router (Crout) service, or to log only one specific event notification for the Certification (Cert) service.

IMPORTANT: Unit performance is affected by the quantity of events that are reported.

Event Notifications can be sent to different destinations to be logged:

- Internal destination
 - [Log to File](#) (p.51) to a file in the DGW File management system (not available on the 4102S and the Mediatrix C7 series).
 - [Log Locally](#) (p.50) to the [Local Logs](#) page of the DGW Web interface.
- External destination
 - to a [SIP server via NOTIFY](#).
 - to a [Syslog](#) server via syslog transport.

2.5.1.2 Send via Syslog

Event notifications can be logged by a Syslog server.

The event notifications will be sent over UDP in the syslog format, to the syslog server specified in the configuration. Alternatively, the syslog server address can be provided through DHCP. It is

important to understand that if no syslog server address is provided by a DHCP server or specified by the administrator, no messages are sent.

IMPORTANT: In some cases, Mediatrix devices can generate more information than the syslog server can handle. In these cases, it is preferable to capture the information with Wireshark.

2.5.1.3 Send via SIP

It is possible to send the event notifications to a SIP server.

The event notifications sent to a SIP server are included in the SIP Notify messages. When choosing to send event notifications to a SIP server, it is not allowed to send all notifications, i.e. select the **All** criteria when configuring event notifications. This has been implemented to avoid sending high volumes of traffic and risking the overload of the SIP server.

The destination can be configured with the **sipEp.sipNotificationsGateway** parameter and the **sipEp.maxNotificationsPerNotify** parameter is used to define how many messages can be sent in a single "SIP NOTIFY" request the

For more details, refer to [DGW Configuration Guide - Reference Guide](#) published on the Media5 documentation portal at <https://documentation.media5corp.com>

2.5.1.4 Log Locally

The DGW Local Log displays the Event Notifications related to the events occurring on the Mediatrix unit that are generated by the Mediatrix Notifications and Logging Manager (Nlm) service.

Notifications will be displayed in the **Local Log Entries** table of the DGW Web interface provided the issuing of events for a service is enabled, and if the event meets the selected severity level chosen to be reported.

The **Local Log Entries** table has the following characteristics:

- Number of displayed event notifications is limited
- Newer notifications replace older ones.
- The routing criteria should be designed to avoid overloading the log.
- The local log has no persistence. Its content is erased when the unit or the Nlm service is restarted.
- The local log does not accept messages from the SNMP service with a 'Debug' severity level. This is to prevent an issue when reading the local log with SNMP. The SNMP walk through the table would not catch up with the increasing index because of the DEBUG events generated by the SNMP service itself.

2.5.1.5 Log to File

The event notifications can be logged in a file saved in the DGW File Management system.

Event notifications logged to a file will be available in the DGW Web interface, under **Management/File** tabs. The log to file feature is not available on the Mediatrix 4102S and C7 Series as they do not have more than 1MB or more user storage. The number of files stored in the unit is limited. When the maximal number is reached, the oldest stored file is deleted. The limit is configured in the **LogFileMaxNb** Mib parameter.

2.5.1.6 Send via SNMP

The event notification can be sent via the SNMP transport.

The Send via SNMP entries have the following characteristics:

- The traps will be sent according to the Trap Destination(s) and SNMP Protocols configured in the Management/SNMP tab of the unit.
- By default, Notifications are only sent at severity level Warning or higher. This means you will only get traps in case of an error. To also get the recovery events for a particular service, set its severity to « Info » in System/Event Log/Service Notification Configuration.
- For SNMP traps, the notification queue is limited to 100 notifications per second for bandwidth limitation purposes.
- Newer traps replace older ones.
- The routing criteria should be designed to avoid overloading the queue

2.5.2 Basic Event Notification Tasks

2.5.2.1 Logging Event Notifications

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, click + located next to **Services**.
- 3) For each service, choose the **Severity** level that will trigger the notifications.

Note: if you do not wish to log the event notifications of a service, select **Disable**.

Note: At this point, you have only enabled the possibility to log event notifications.

- 4) In the **Criteria** field, enter **All**.

- 5) From the **Action** drop-down list, select where and how the event notifications will be logged.
 - a) Choose [Log Locally](#) (p.50) to display the event notifications in the Local Log.
 - b) Choose [Log to File](#) (p.51) to send the event notifications to the DGW file management system (not available on the Mediatrix 4102S and C7 Series).
 - c) Choose [Send via Syslog](#) (p.49) to send the event notifications to a Syslog server.
 - d) Choose [Send via SNMP](#) (p.51) to send the event notification via the SNMP transport.

Note: You cannot choose **Send Via SIP** if you wish to log all event notifications, as this may overload the SIP gateway. The system will indicate **Not Supported**.

- 6) If you selected [Send via Syslog](#) in the previous step, make sure you have configured the address of the syslog server under **Syslog Configuration/Remote Host** field.
- 7) Click **+**.
- 8) Click **Apply**.

Result

All event notifications with the appropriate selected **Severity** level of each selected service will be logged to the chosen destination.

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable	All	Service	--- Suggestion ---	Send Via Syslog	Valid	-
3	Enable	All	Service	--- Suggestion ---	Send Via SIP	Valid	-
4	Enable	All	Service	--- Suggestion ---	Send Via SNMP	Valid	-
5	Enable	All	Service	--- Suggestion ---	Log Locally	Valid	-
6	Enable	All	Service	--- Suggestion ---	Log To File	Valid	-
							+

2.5.2.2 Logging Specific Event Notifications

Information

Instead of logging all the event notifications, as specified in [Logging Event Notifications](#), the **Criteria** can be refined to a subset of events.

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, click + located next to **Services**.
- 3) From the **Severity** drop-down list, for each service, choose the severity level that will trigger the notification.

Note: If you do not wish to log the event notifications of a service, select **Disable**.

Note: At this point, you have only enabled the possibility to log event notifications.

- 4) In the **Notification Events** table, select a **Service** for which Event Notifications must be issued.
- 5) From the **Notification** drop-down list, select one, or several, specific service notifications you wish to log.

Note: The **Criteria** field will be auto populated with the selection made in the **Notification** field.

Note: To log all the notifications of a specific service enter in the **Criteria** field the service code with all separated by a coma. For example: 200.all to log all the notifications of the Bni service. (The code can be found in the **Service** drop-down list.)

- 6) From the **Action** drop-down list, select where and how the event notifications will be logged.
 - a) Choose [Log Locally](#) (p.50) to display the event notifications in the Local Log.
 - b) Choose [Log to File](#) to send the event notifications to the DGW file management system. (not available on the Mediatrix 4102S and C7 Series).
 - c) Choose [Send via Syslog](#) (p.49) to send the event notifications to a Syslog server.
 - d) Choose [Send via SIP](#) (p.50) to send the event notifications to a SIP server.
- 7) This step is not necessary if you chose **Log To File** in the previous step. In **Syslog Configuration** table, in the **Remote Host** field, enter the IP address of the server.
- 8) Click **+**.
- 9) Repeat steps 4 to 7 for each notification you wish to publish.
- 10) Click **Apply**.

Result

The selected service notifications with the corresponding **Severity** level will be published to the selected destination.

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable	Criteria of chosen notification	Service	Choose Notification	Log Locally	Valid	-
2	Enable	Criteria of chosen notification	Service	Choose Notification	Send Via SIP	Valid	-
3	Enable	Criteria of chosen notification	Service	Choose Notification	Send Via Syslog	Valid	-
4	Enable	Criteria of chosen notification	Service	Choose Notification	Log To File	Valid	-
			--- Suggestion ---				+

2.5.2.3 Disabling Event Notification Reporting for a Service

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, from the drop-down list located next to a service name, select **Disable**.

Result

No event notifications will be issued for the service.

2.5.2.4 Modifying the Severity Level Triggering the Reporting of a Notification

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, from the drop-down list located next to a service name, select the severity level an event should have to issue a notification.

Result

Notifications will be issued for the service only if the severity level matches the selection.

2.6 Local Log

2.6.1 Basic Local Log Tasks

2.6.1.1 Clearing the Local Logs

Steps

- 1) Go to **System/Local Log**.
- 2) Click **Clear Local Log**.

Result

The entries in the **Local Log Entries** table will be permanently deleted.

2.6.1.2 Updating the Local Logs

Steps

- 1) Go to **System/Local Log**.
- 2) Click **Refresh Local Log**.

Result

All new entries generated by the Notifications and Logging Manager (NLM) of your Mediatrix unit will be displayed in the **Local Log Entries** table.

2.7 Packet Capture

2.7.1 Basic Packet Capture Concepts

2.7.1.1 Packet Captures

Packet captures are data packets intercepted when passing through a specific computer network.

Captured packets can be sent to a specific location where they can be analysed. The content of the capture can therefore be used to diagnose or troubleshoot network problems and determine if network security policies are being followed.

There are three different ways to perform a packet capture:

- With the **pcapture** CLI command available only via the CLI. This method displays the captured packet directly in the CLI or allows streaming the captured packet to a SSH tunnel to a remote Wireshark client.
- With the **Nlm.PCaptureStart** command. This is a muse command, it can be executed via SNMP, a script, and the CLI. This is the same command used when performing packet captures via the DGW Web page. This method sends the captured file to a file or to a HTTP server via a standard HTTP upload.
- With the DGW Web Interface, under **System/Packet Capture**.

2.7.2 Basic Packet Capture Tasks

2.7.2.1 Starting a Network Capture

Steps

- 1) Go to **System/Packet Capture**.

- 2) In the **Packet Capture Configuration** section, complete the fields as follows:
 - a) Max Number of Frames: Specifies the maximum number of frames after which the packet capture is automatically stopped. 0 means no limit.
 - b) Max number of seconds: Specifies the maximum number of seconds after which the packet capture is automatically stopped. 0 means no limit.
 - c) Filter: For more details on filters, refer to [Filter Examples](#) (p.59)
 - d) Link Name: Select the name of the link interface to capture
 - e) URL: The URL format must follow this syntax: protocol://[user[:password]@]hostname[:port]/[path/]filename

Note: The Link Name can be, for example, **eth1** to capture the traffic on the **ETH1** interface , or **any** to capture traffic on all interfaces.

Note: If the protocol is FILE, the captured trace is saved locally to the unit. For example, a if the URL is "file://my_trace.pcap" saves a capture file with the name "my_trace.pcap" in the Mediatrix unit, which can be downloaded under **Management/File**.

Note:

Available protocols are File, HTTP, and HTTPS but the File protocol is not available on Mediatrix 4102S units. If the protocol is HTTPS, the HTTP server must allow "slow HTTP requests" (mod_reqtimeout module for Apache HTTP Server) otherwise the pcapure feature may not work as expected. Depending on the nature of what is being captured, chunks can be sent very slowly and with long delays, causing the capture to be considered as an attack and therefore stopped.

- 3) Click **Apply**.
- 4) Click **Apply & Start Capture**.

Note: Remember to click **Apply & Stop Capture** when you have enough packets captured.

Result

Packets going trough the specified filter will be captured and sent to the specified URL.

2.7.2.2 Starting a Network Capture on a Specific VLAN

Before you start

The VLAN must first be created. Refer to [Creating a VLAN](#) (p.106)

Information

This method is performed with the PCaptureStart command of the Nml service.

Steps

- 1) Go to **System/Packet Capture**.
- 2) In the **Packet Capture Configuration** section, in the **Link Name** field, enter the name of the VLAN for which you want to capture packets. This corresponds to the chosen

Ethernet port followed by name given in the **VlanId** field of the **VLAN Configuration** table (**Network/VLAN**), when the Vlan was created (for example eth1.100)

Note: For the URL, if you choose the FILE transport protocol, it means that the file will be accessible under **Management/File**.

- 3) Click **Apply**.
- 4) Click **Apply & Start Capture**.

Note: Remember to click **Apply & Stop Capture** when you have enough packets captured.

Result

A capture will be started, and only the traffic going through the specified Vlan will be captured.

2.7.2.3 Starting a Network Capture Remotely On Windows

Information

This method is performed using the **pcapture** command of the CLI.

Before you start

- You must know the IP address of the unit running the DGW software.
- The Mediatrix unit must be running a DGW v2.0.39.689 firmware or higher.
- You must have a PC running Wireshark.
- The first time the unit is connected via plink/wireshark, do not forget to answer **y** to the **Store key in cache? (y/n)** question displayed in the CMD window.
- Make sure there are no other plink sessions already running.

Steps

- 1) From the PC, download the plink utility: [plink utility](#).
- 2) Save the plink utility in the same folder as the Wireshark executable is located.
- 3) Open a command line interface (e.g. cmd.exe).
- 4) Go to the Wireshark folder where the utility was saved. (e.g. cd "C:\Program Files\Wireshark")

5) Enter

```
plink.exe -ssh -no-antispoof -pw "PASSWORD" USERNAME@IP_ADDRESS  
"pcapture -raw -i any" | wireshark -k -i -
```

and replace the password, username, and IP address according to your setup.

Note: **any** is to make a capture on all ETH ports, including VLANs (for example ETH1.10 where). But it is possible to choose the port, either ETH1, ETH2, ETH5, ETH1-4, ETH2-5, WAN, or LAN depending on the type of unit.

Note: Since version 0.71, plink needs to be run with the -no-antispoof option. In addition, if you have previously configured plink to default to telnet, you will also need to add the -ssh option.

Note: Refer to [Examples of pcapure Commands for Windows](#) (p.59).

Result

The pcapure command will be executed in the CLI and the result will be sent to a new Wireshark window on the PC running the Wireshark.

2.7.2.4 Starting a Network Capture Remotely On MacOS or Linux

Information

This method is performed using the **pcapture** command of the CLI.

Before you start

- The Mediatrix unit must be running a DGW v2.0.17.285 firmware or higher.
- You must know the IP address of the unit running the DGW software.
- You must have a PC running Wireshark.

Steps

- 1) Open a command line interface.
- 2) Enter: and replace the password, username, and IP address according to your setup.

```
ssh USERNAME@IP_ADDRESS "pcapture -raw -i any" | wireshark -k -i -
```

Note: **any** is to make a capture on all ETH ports. But it is possible to choose the port, either ETH1, ETH2, ETH5, ETH1-4, ETH2-5, WAN, or LAN depending on the type of unit.

Note: Refer to [Examples of pcapure Commands on MacOS and Linux](#) (p.60).

Result

The `pcapture` command will be executed in the CLI and the result will be sent to a new Wireshark window on the PC running the Wireshark.

2.7.3 Examples

2.7.3.1 Filter Examples

- Filter: port 5060
 - Captures all traffic on (either source or destination) port 5060 (SIP)
- Filter: port 5060 and host 192.168.0.99
 - Captures all traffic on port 5060 and source or destination IP 192.168.0.99
- Filter: port 5060 and dst host 192.168.0.99
 - We can enter “dst” or “src” before “host” (or “port”) to specify the destination or source host (or port)
- Filter: not broadcast and not multicast
 - Filter out the broadcast and multicast traffic

2.7.3.2 Examples of `pcapture` Commands for Windows

Capture from the uplink interface of the Mediatrix unit, and filtering out the broadcast and multicast traffic.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1 not broadcast and not multicast" | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets of the VLAN for which the VlanId is 100 only.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1.100" | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using RTP only.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1 -t rtp " | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 only (either source or destination).

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1 port 5060 " | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 as the source only.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1 src port 5060 " | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 as the destination only.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -raw -i eth1 dst port 5060 " | wireshark -k -i -
```

Capture the packets going through the Ethernet port eth1, for traffic for which the source or the destination is the unit with the 00:90:F8:07:5A:6D MAC address.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -i eth1 ether host 00:90:F8:07:5A:6D " | wireshark -k -i -
```

Capture the packets going through the Ethernet port eth1, for traffic for which the source or the destination is the units with the 10.5.128.11 or host 10.5.128.4 IP addresses.

```
plink.exe -ssh -no-antispoof -pw "administrator" admin@192.168.0.10
"pcapture -i eth1 host 10.5.128.11 or host 10.5.128.4 " | wireshark -k -i -
```

2.7.3.3 Examples of pcapure Commands on MacOs and Linux

Capture from the uplink interface of the Mediatrix unit, and filtering out the broadcast and multicast traffic.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 not broadcast and not
multicast" | wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets of the Vlan for which the VlanId is 100 only.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1.100" | wireshark -k -i -
```

Forces capture to interpret all packets as rtp packets. Typically, this is used with a filter that only keeps rtp packets.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 -T rtp " | wireshark -k -i -
```

Capture only rtp packets, going through the Ethernet port eth1, but using port 5006 only (either source or destination)

```
ssh admin@192.168.0.10 "pcapture -raw -i -T rtp eth1 port 5006 " |  
wireshark -k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 only (either source or destination).

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 port 5060 " | wireshark -k -  
i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 as the source only.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 src port 5060 " | wireshark  
-k -i -
```

Capture from the uplink interface of the Mediatrix unit, the packets going through the Ethernet port eth1, but using port 5060 as the destination only.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 dst port 5060 " | wireshark  
-k -i -
```

Capture the packets going through the Ethernet port eth1, for traffic for which the source or the destination is the unit with the 00:90:F8:07:5A:6D MAC address.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 ether host 00:90:F8:07:5A:6D  
" | wireshark -k -i -
```

Capture the packets going through the Ethernet port eth1, for traffic for which the source or the destination is the units with the 10.5.128.11 or host 10.5.128.4 IP addresses.

```
ssh admin@192.168.0.10 "pcapture -raw -i eth1 host 10.5.128.11 or host  
10.5.128.4 " | wireshark -k -i -
```

2.8 Diagnostic

2.8.1 Basic Diagnostic Concept

2.8.1.1 Diagnostic Traces

Diagnostic Traces are specifically used for troubleshooting purposes. As for Event Notifications, they report errors, warnings, or system information.

Diagnostic Traces do not need to be activated, except at the specific demand of Media5 Technical Assistance Center.

2.8.2 Basic Diagnostic Trace Tasks

2.8.2.1 Enabling the Automatic Diagnostic Log Dump

Steps

- 1) Go to **System/Diagnostic**.
- 2) In the **Diagnostic Log Configuration** table, select **Enable**.
- 3) Click **Apply**.

Result

If the unit unexpectedly closes, the diagnostic logs will be automatically generated in an *.tgz file, available under **Management/File** in the **Internal files** table.

2.8.2.2 Manually Starting a Diagnostic Log Dump

Steps

- 1) Go to **System/Diagnostic**.
- 2) In the **Diagnostic Log Configuration** table, select **Dump Now**.

Result

The diagnostic logs will be generated in an *.tgz file, available under the **Management/File**, in the **Internal files** table.

2.9 PCM Traces

2.9.1 Basic PCM Traces Concepts

2.9.1.1 PCM Traces

The PCM traces are two different RTP streams made specifically to record all analog or digital signals that are either sent or received by the telephony ports of the Mediatrix unit.

These RTP streams are sent to a configurable IP address, normally an IP address on your network where it can be recorded with a packet sniffer (such as Wireshark). Moreover, they are independent from the regular RTP streams of the VoIP call. On the analog devices, the streams are sent instantly at device start-up, with an average ptime of 5 ms. The resulting streams, depending on the model, are around 15 kB/s.

Only the configured port, port #1 and/or #2 send the PCM traces for a maximum of four simultaneous RTP streams.

All streams are sent instantly at start-up with an average ptime of 15 ms. This means that until the PCM traces are disabled, even an idle unit will continuously send up to 66.6 packets/s X 4 streams = 267 packets/s using approximately 174 bytes each, for a total of 46 Kbytes of upstream bandwidth.

On digital devices, the streams will be sent once a call is in process of being established (ISDN SETUP, SIP INVITE). This means no data will be sent if the gateway is idle with no calls in progress.

PCM Traces are usefull at identifying problems with:

- Echo in the network
- DTMF signals
- Caller ID signals
- Fax signals (or false Fax detection)
- Message Waiting Indicator signals
- Any other analog signal
- Any voice quality issue

2.9.2 Basic PCM Tasks

2.9.2.1 Enabling the PCM Traces - SIP 5.0

Before you start

The PCM traces destination must be set so it can be recorded in a Wireshark capture on your network, normally sent to the PC doing the capture

Steps

- 1) Enable the PCM traces by setting the mxDebugPcmCaptureEnable MIB variable to enable.
- 2) Set the destination IP address for the PCM traces in the mxDebugPcmCaptureIpAddress MIB variable.

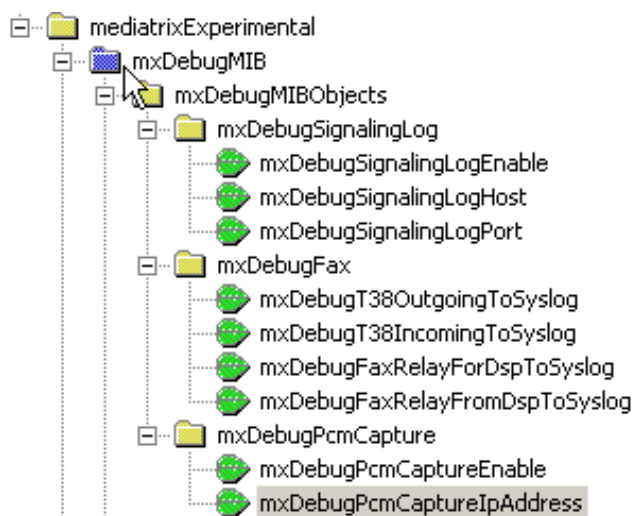
Note: This IP address does not have to be listening on ports 5001/2 – 6001/2, as it is easy to filter out ICMP “port unreachable” messages afterwards.

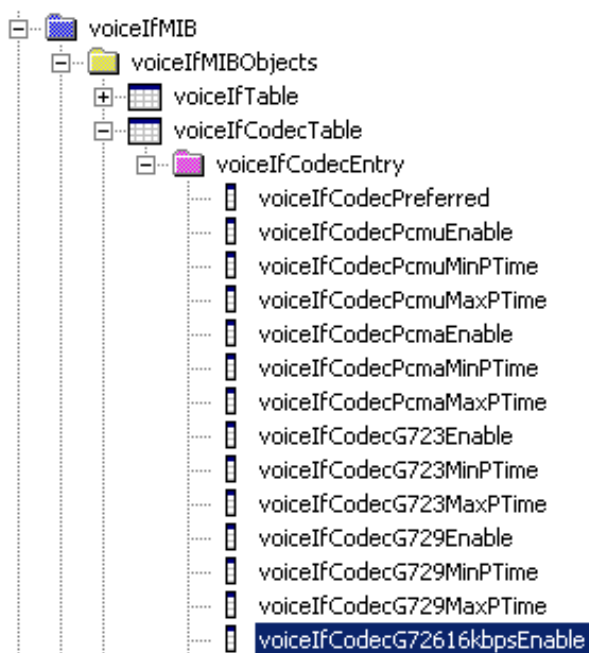
Note:

If G.723 is available, you MUST disable the G.723 and enable the G.726 codec to load the PCM code into the 1204. This can be done by setting the voicelfCodecG723Enable MIB variable to disable and the voicelfCodecG72616kbpsEnable MIB variable to enable in the voicelfMIB.

- 3) Reboot the unit.

Result





2.9.2.2 Enabling the PCM Traces of a Port Using UMN

Before you start

The PCM traces destination must be set so it can be recorded in a Wireshark capture on your network, normally sent to the PC doing the capture.

Information

If a port is receiving several calls at a time, the capture will be performed on the first call until it is completed, and only then will a capture be performed on another call. Traces are taken as soon as the port is opened.

Steps

- 1) Using UMN, right click the name of the unit and select **Edit SNMP...**
- 2) Browse to: mediatrixSystem/gen5/mediatrixCommon/mediatrixServices/miptMIB/miptMIBObjects/debugGroup/ pcmCaptureGroup.
- 3) Set the **pcmCaptureEnable** MIB parameter to **Enable**.
- 4) Set the **pcmCaptureEndpoint** MIB parameter to the unit's endpoint on which the PCM capture will be taken from. For endpoint examples, refer to [Endpoint Examples](#) (p.67).

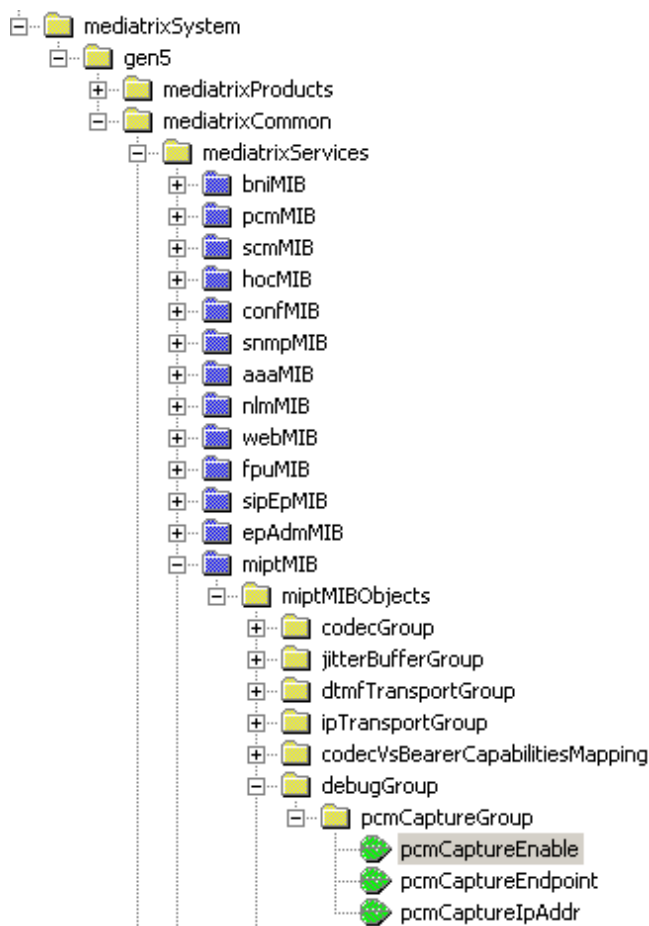
Note: To make sure that you are capturing the appropriate endpoint, please verify its naming by running the following command in CLI: **Epadm.Endpoint**. The output of the command displays a table with the unit's endpoints.

- 5) Set the **pcmCaptureIpAddr** MIB parameter to the IP address of the PC running Wireshark.

Note: This IP address does not have to be listening on UDP ports, as it is easy to filter out ICMP “port unreachable” messages afterwards.

- 6) When the capture is done, make sure to set the **pcmCaptureEnable** MIB parameter to **Disable**.

Result



2.9.2.2.1 Endpoint Examples

Endpoint Name	Description
Bri1-2	BRI port 1, channel 2
Slot2/E1T1-3	Channel 3 of the E1 port located in slot 2
Port09	Port 09 of a Mediatix 4108-16-24 unit
Phone-Fax1	Port 1 of a Mediatix 4102S unit
FXS1	Port 1 of the FXS card of a Mediatix C7 unit
FXO1	Port 1 of the FXO card of a Mediatix C7 unit

All possible endpoint names are listed in the Endpoint table displayed in the DGW Web interface (**System/Endpoints**). You may also access this table via the CLI by using the **EpAdm.Endpoint** command or directly via UMN.

2.9.2.3 Enabling PCM Traces of a Port Using the Configuration Script

Before you start

The PCM traces destination must be set so it can be recorded in a Wireshark capture on your network, normally sent to the PC doing the capture.

Information

If a port is receiving several calls at a time, the capture will be performed on the first call until it is completed, and only then will a capture be performed on another call. Traces are taken as soon as the port is opened.

Steps

- 1) Create a txt file, and save it as a *.cfg.
- 2) Enter **Mipt.PcmCaptureEnable = Enable** or **Mipt.PcmCaptureEnable=1**
- 3) Enter **Mipt.PcmCaptureEndpoint = Value**, where **Value** is the unit's endpoint on which the PCM capture will be taken from. For more information, refer to [Endpoint Examples](#) (p.67).

Note: To make sure that you are capturing the appropriate endpoint, please verify its naming by running the following command in CLI: **Epadm.Endpoint**. The output of the command displays a table with the unit's endpoints.

Note: The port names are case sensitive.

- 4) Enter **Mipt.PcmCaptureIpAddr = Value**, where **Value** is the IP address of the PC running Wireshark.

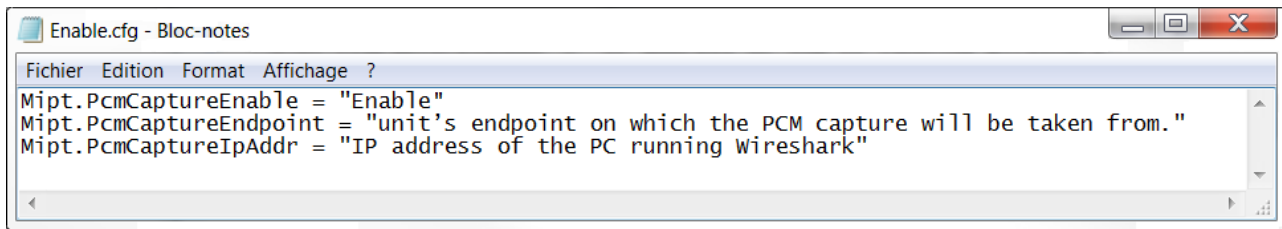
Note: The IP address does not have to be listening on UDP ports, as it is easy to filter out ICMP "port unreachable" messages afterwards.

- 5) Import the *.cfg file into the system. Refer to [DGW Configuration Guide - Configuration Scripts Import and Export](#) published on the [Media5 Documentation Portal](#).
- 6) When the capture is done, make sure to disable the **Mipt.PcmCaptureEnable** MIB parameter.

Note: For example **Mipt.PcmCaptureEnable = Disable** or **Mipt.PcmCaptureEnable = 0**

Result

In the configuration script, the value of **Mipt.PcmCaptureEnable**, **Mipt.PcmCaptureIpAddr** and **Mipt.PcmCaptureEndpoint** parameters should reflect the values configured..



2.10 VM

2.10.1 Virtual Machine Basic Concepts

2.10.1.1 Important Information on Virtual Machines

Note: It is not possible to modify the settings (RAM, name, etc.) once the virtual machine has been created. The only way to change the settings, is to delete the virtual machine and to create it once again.

Note: A maximum of 2 virtual machines can be added.

2.10.1.2 RAM and SSD Sizes

Table 1:

Description	Possible Values
RAM size ¹	• 0 - No DDR (slave device) (contact Media5 sales) • 1 - 2 GB DDR • 2 - 4 GB DDR • 3 - 8 GB DDR • 4 - 16 GB DDR (contact Media5 sales)
SSD size ²	• 0 - No SSD (slave device) (contact Media5 sales) • 1 - 16 GB SSD • B - 32 GB SSD (20k erase cycle) • C - 64 GB SSD (20k erase cycle) • D - 128 GB SSD (20k erase cycle) • E - 256 GB SSD (20k erase cycle)

¹ a minimum of 4 GB is required to use a VM

² a minimum of 32 GB is required to use a VM

2.10.1.2.1 RAM Allocation to Virtual Machines

To reduce the wear-and-tear of the Solid State Drive, make sure to allocate the maximum amount of RAM possible to the virtual machine.

Installed RAM on Mediatrix Units	Available RAM for Virtual Machine
2 Gb	1.5 Gb
4 Gb	3.5 Gb
8 Gb	7 Gb (87.5% of available RAM)
16 Gb	10 Gb

2.10.1.3 VM name

The name is set when adding a new virtual machine with the `CreateVm` command. The user cannot modify the name after.

When the `CreateVm` command is called without a name, the index is used to generate a unique name such as `VM_Index`.

2.10.1.4 VM Memory

When adding a VM with the `CreateVm` command, the amount of allocated memory is set; this amount cannot be modified after adding the VM.

When the `CreateVm` command is called without an amount of allocated memory, a minimal value of 128 MB is set.

Depending on the total amount of volatile memory in the system, the amount of memory reserved for DGW is

- a minimum of 512 MB, or
- 12.5% of the total volatile memory capacity if more than 512 MB is available

2.10.1.5 USB Usage

The VM config allows the user to associate none or all USB Ports to a virtual machine.

A USB port can be associated with one VM. The first VM that is configured with USB can use all available USB ports.

If an another VM tries to use a USB port already in use, the Vm service ignores this config and starts the VM as if it was configured with *NONE*, and sets its configuration status (**ConfigStatus**) to *USBNotAvailable*.

2.10.1.6 Virtual Switch

Enabling the Virtual Switch with the **Eth.Links.VirtualSwitch** parameter grants network access to the VM. Once enabled, the virtual switch creates a bridge between the VM and the associated Ethernet link.

When the Virtual Switch is enabled, the **Vm.Vm.NetworkAdapter** parameter configures its virtualised network adapter.

2.10.1.7 Behaviour on Factory Reset

The unit can be preinstalled with a factory-installed VM stored in the *vm/images/factory* folder. This folder can only be created in factory and must have the factory-installed VM files.

Two behaviors are possible for the VMs on a factory reset.

- When one or more factory-installed VM is present, VM images and configurations are returned to their original factory state.
- When no factory-installed VM is present, the VM images and configurations stay unchanged, i.e. the files present in *vm/images/* are not erased.

When a factory-installed VM is present, the factory reset is performed as follows:

- The files in the *vm/images/* folder are erased, which removes the VM snapshots and all VMs created, modified, or installed by users.
 - Note: this is done even if the *vm/images/factory* folder exists and is empty.
- For each factory-installed VM (visible in the *vm/images/factory* folder), the configuration file (.cfg) is copied in the *vm/images* folder and a snapshot of the VM image is also created in the *vm/images* folder. The snapshot file is given the *.snapshot extension* and is always in a QCOW2 format. When this VM is used, the snapshot file changes over time but the base image (located in *vm/images/factory*) is never modified, allowing the next factory reset to restore the factory VMs to their original state again.
- The admin can use, configure, convert, and delete a VM with a snapshot image like any other VM, but after a factory reset, the snapshot image is deleted and a new one is created.
- When a snapshot file is converted into a VM image file, the resulting file is a new image file combining the base VM plus the history contained in the snapshot file.
- Users cannot add or delete files on the *vm/images/factory* folder. This can only be done in factory.
- The VM images under *vm/images/factory* can have either the RAW or QCOW2 format.
- The *RestoreAfterFactory* parameter in the VM configuration file is ignored. The factory-installed VMs are always restored.

In all cases, the content of */vm/drives* is erased.

2.10.1.8 What are the Meltdown and Spectre Security Vulnerabilities

These vulnerabilities allow a non-privileged process to read sensitive data in memory, thus accessing privileged information from the kernel or other processes.

A Virtual Machine (VM) running inside the Sentinel 400 **may** be vulnerable to Meltdown (CVE-2017-5754) and to the two variants of Spectre (CVE-2017-5753 and CVE-2017-5715).

For more information on these vulnerabilities:

- [https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))
- [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))

2.10.1.8.1 How to Protect my VM against Spectre

There are different mitigation techniques against Spectre:

- Mitigation #1: A microcode update from the CPU vendor for better control over the branch speculation. Also need an updated kernel to enable these new features (IBRS and IBPB).
- Mitigation #2: Different techniques (like "retpoline" and "LFENCE") that require recompiling the kernel, packages and applications.

As the time this document was written, Mitigation #1 could not be applied, as Intel had not yet released a microcode update for the CPU of the Sentinel 400.

If your Virtual Machine is vulnerable, Media5 recommends applying Mitigation #2. See [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)#Mitigation](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)#Mitigation) for more details.

IMPORTANT: Mitigation techniques against Spectre may impact the performance of your Virtual Machine.

2.10.1.8.2 How to Protect my VM against Meltdown

Linux kernels have a new feature called KPTI (previously known as KAISER) that protects against Meltdown.

If your Virtual Machine is vulnerable, Media5 recommends that you upgrade your kernel to a version that supports KPTI, and enable it.

For more information on KPTI: https://en.wikipedia.org/wiki/Kernel_page-table_isolation

IMPORTANT: Enabling KPTI may impact the performance of your Virtual Machine.

2.10.1.9 SSD Lifespan

Mediatrix units running a Virtual Machine are equipped with various sizes of Solid State Drive (SSD) for storage.

A Solid State Drive (SSD) is a form of flash-based storage. Media5 uses high quality, enterprise grade SSDs in its products. However due to its technical nature, flash memory can handle so many read/write cycles. Beyond that, the performance may degrade or in extreme cases, the drive may fail. For customers using a Mediatrix unit running a Virtual Machine, special attention should be paid to the number of writes caused by the Operating System running in the virtual machine, as well as by the application. If the Virtual Machine is not optimised, it will lead to excessive read/write access to the SSD, and hence significantly reduce the lifespan of the SSD. For more details, please refer to [Technical Bulletins - Virtual machine installation](#) published on the [Media5 Documentation Portal](#).

2.10.1.10 SSD Lifespan Extrapolation

SSD lifespan can be extrapolated and Virtual Machine optimisation can be validated.

For example, let the virtual machine run for a month (or a week), read and compare the **WearPercentage** parameter at different times during this interval. Use the collected information to extrapolate the lifespan.

For example: the Wear Percentage increased from 19% to 20% in 2 months. Take the remaining 80% divided by a monthly increase of 0.5% gives 160 months left. Therefore at least 13 years left at the current increase rate.

If the lifespan does not meet the expectations, you may consider further optimisation measures e.g.:

- disable some of the logging
- log to an external device
- assign more RAM to the Virtual Machine
- consider ordering a bigger SSD for future installations

2.10.1.11 Is all the System Vulnerable?

The DGW firmware in the Mediatrix system, by itself, is not vulnerable since it does not allow running rogue code:

- <https://www.media5corp.com/media5-statement-meltdown-spectre-vulnerabilities/>

But it is theoretically possible, for a Virtual Machine compromised by the Spectre vulnerability, to read memory outside the Virtual Machine and access sensitive data of the Mediatrix system. The best protection against this is to secure your VM, to make sure there is no known means an attacker can use to break into your VM.

Media5 also recommends to always keep your Sentinel 400 up-to-date with to the latest DGW firmware version.

2.10.2 Basic Virtual Machine Actions

2.10.2.1 Stopping the Virtual Machine

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, click  located on the same row as the **VM** you wish to stop.

Result

The virtual machine stops. In the **Virtual Machine Status** table, **Stopped** will be displayed under the **State** column.

2.10.2.2 Stopping the Virtual Machine - Graceful Stop

Steps

- 1) Open the VNC Client located on a computer located on the network connected to the unit.

Note:

UltraVNC Viewer, TightVNC Viewer and VNC Viewer are presently supported.

- 2) Enter the **Unit.IP.Address: VNCid** .
- 3) In the **VNC** console, shutdown the OS using the recommended OS method.

2.10.2.3 Rebooting a VM

Information

If the virtual machine you wish to start requires resources equivalent to the available resources on the unit, then it will not be possible to start another virtual machine. It is only possible to start a virtual machine if there are enough resources on the unit.

Note: Rebooting a virtual machine does not have the same effect as Restarting the virtual machine.

Steps

- 1) Go to **System/VM**.
- 2) Click .

Result

The virtual machine is restarted. In the **Virtual Machine Status**, **Started** will be displayed under the **State** column.

2.10.2.4 Rebooting a VM - Graceful Reboot

Information

Although the virtual machine can be rebooted via the Web page, rebooting the virtual machine using a VNC Client is the preferred way to reboot the virtual machine.

Note: Rebooting the virtual machine does not have the same effect as restarting the virtual machine.

Steps

- 1) Open the VNC Client located on a computer located on the network connected to the unit.

Note:

UltraVNC Viewer, TightVNC Viewer and VNC Viewer are presently supported.

- 2) Enter the **Unit.IP.Address: 5900+VNCid**.
- 3) In the VNC console, shutdown the OS using the recommended OS method.

Result

The virtual machine is restarted. In the **Virtual Machine Status**, **Started** will be displayed under the **State** column.

2.10.2.5 Setting the Virtual Machine to Automatic Start

Information

If the virtual machine you wish to start requires resources equivalent to the available resources on the unit, then it will not be possible to start another virtual machine. It is only possible to start a virtual if there are enough resources on the unit.

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, from the **Startup** dropdown list, select **Auto**.
- 3) Click **Apply**.

Result

When the Vm Service is started, the virtual machine will also be started.

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
VirtualMachine_1		12:d8:38:0a:9e:8d	0	None	e1000	Auto	    	

2.10.2.6 Setting the Virtual Machine to Manual Start

Information

Manually starting the virtual machine can be useful when installing the virtual machine to check if the installation was done properly. However, on a day to day usage, the virtual machine should be set to start automatically. Refer to [Setting the Virtual Machine to Automatic Start](#) (p.76).

Note: If the virtual machine you wish to start requires resources equivalent to the available resources on the unit, then it will not be possible to start another virtual machine. It is only possible to start a virtual machine if there are enough resources available on the unit.

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, from the **Startup** dropdown list, select **Manual**.
- 3) Click **Apply**.

Result

The virtual machine will be started only if it is started manually. In the **Virtual Machine Status**, **Started** will be displayed under the **State** column.

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
VirtualMachine_1		12:d8:38:0a:9e:8d	0	None	e1000	Manual	    	

2.10.2.7 Deleting a VM

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, click  located on the same row as the virtual machine you wish to delete.

Result

The virtual machine and its configuration are deleted.

2.10.2.8 Monitoring the SSD Wear Percentage Using the CLI

Steps

- 1) Open the Command Line Interface (CLI).
- 2) At the prompt, enter the following command: `Dcm.PersistentWearPercentage`

Result

This parameter will provide the Wear Percentage of the SSD. It is taken from the SMART data obtained directly from the drive. When it reaches 100%, it means the technical lifespan of the SSD has been reached. The drive may not fail immediately, but this indicates that the SSD must be replaced to ensure continuous operation.

2.10.2.9 Monitoring the SSD Wear Percentage Using a MIB Browser

Information

The Mediatrix UMN Mib browser can be used for this procedure.

Steps

- 1) Open your Mib Browser.
- 2) Poll `.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.250`

Note: This is an SNMP (readonly) Mib.

Result

This parameter will provide the Wear Percentage of the SSD. It is taken from the SMART data obtained directly from the drive. When it reaches 100%, it means the technical lifespan of the SSD has been reached. The drive may not fail immediately, but this indicates that the SSD must be replaced to ensure continuous operation.

2.10.3 Virtual Machine Installation

2.10.3.1 Adding a Virtual Machine

Before you start

The **VirtualSwitch** parameter must be configured to enable the link you wish to use to contact the virtual machine. Refer to [Configuring a Link as a Virtual Switch](#) (p.104) .
You must have a virtual machine licence and the VM service must be started.



Caution: It is a best practice to create the Virtual Machine in a test environment. If not enough memory is allocated and swap is disabled, the Virtual Machine will stop, and the installation will need to be restarted from the beginning.

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Creation** table, complete the **Vm Name** field.

Note: Vm names must be unique.

- 3) In the **Ram(Mb)** field, enter the amount of RAM required to run the virtual machine.



Caution: To reduce the wear-and-tear of the Solid State Drive, make sure to allocate the maximum amount of RAM possible to the virtual machine.

Note: For instance, 87.5% of the actual available RAM, or 1.5 Gb for units with 2 Gb of RAM, 3.5 Gb with 4 Gb of RAM and for 7 Gb with 8 Gb of RAM.

- 4) Complete the **Storage(Gb)** field.

Note: 10 Gb is the maximum value one can allocate in a typical Sentinel equipped with a 16 Gb Solid State Drive.

- 5) From the **Image Format** selection list, choose the format of the image.

Note:

- Use QCOW2 for space efficiency and flexibility.
- Use RAW for improved performance

- 6) From the **Nb Cores** selection list, select the number of cores the virtual machine will be using.

IMPORTANT: It is not possible to modify the settings (RAM, name, etc.) once the virtual machine has been created. The only way to change the settings, is to delete the virtual machine and to create it once again.

- 7) Click **+**.

Note: A maximum of 2 virtual machines can be added.

Result

The virtual machine will be displayed in both the **Virtual Machine Configuration** and the **Virtual Machine Status** tables.

Virtual Machine Creation					
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
unique_Vm_Name	xxx(Mb)	Storage(Gb)	raw ▾	1 ▾	+

2.10.3.2 Configuring the VM Network Adapter (VirtIO)

Before you start

Configuring the Network Adapter is optional. By default, it is set to E 1000 (Intel 82545EM emulated network interface card). However, for enhanced network performance, the network adapter can be set to VirtIO, provided it is supported by the guest OS as paravirtualised drivers are required.

Steps

- 1) Go to **System/VM**.
- 2) From the Network Adapter drop down list, select **VirtIO**.

Note: Please refer to the OS documentation for specific information regarding VirtIO.

- 3) Click **Apply**.

Result

The virtual machine Network Adapter will be set to **VirtIO**.

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
Kali		12:2e:7f:c2:c4:d2	0	None ▾	virtio ▾	Manual ▾		

2.10.3.3 Installing the OS on the Virtual Machine Using an ISO image

Before you start

The [Importing an ISO image to the Unit File Management System](#) (p.553) procedure must be completed. When downloading an OS that provides architecture choices you need to choose either AMD64 (64 bit OS) or i386/i686 (32 bit OS). Basically you need to choose the architecture for an INTEL processor

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration**, in the **Iso Name** field, indicate the name of the ISO file containing the OS.
- 3) In the **Vnc Id** field, indicate the unique id used with the VNC Client to connect to the virtual machine console.
- 4) From the **Usb** field, select **None**.
- 5) Click

- 6) Open the VNC Client located on a computer of the network connected to the unit.

Note:

UltraVNC Viewer, TightVNC Viewer and VNC Viewer are presently supported.

- 7) Enter the IPAddressOftheUnit:VNCid.

Note: For example 192.168.0.12:1

- 8) Follow the on-screen instructions.



Caution:

To reduce the wear-and-tear of the Solid State Drive,

- On Linux OS, disable memory swapping or at least set swappiness to 0.
- On Windows OS, disable the virtual memory.

Note: If the Solid State Drive fails because it is inadequately used by a third party software or the operating system, the warranty of the Mediatrix unit will no longer be valid.

Note: The installation can take more than an hour depending on the image you are installing.

Result

The virtual machine will be started only if it is started manually.

Virtual Machine Configuration							
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
VirtualMachine_1	iso_file_name	12:d8:38:0a:9e:8d	0	None	e1000	Manual	    

2.10.3.4 Installing the Virtual Machine OS using a USB External Device

Before you start

Make sure your USB external device contains the Operating System installation media, is bootable, and is connected. When downloading an OS that provides architecture choices you need to choose either AMD64 (64 bit OS) or i386/i686 (32 bit OS). Basically you need to choose the architecture for an INTEL processor.

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, in the **Vnc Id** field, indicate the unique id of the virtual machine.
- 3) From the **Usb** field, select **All**.
- 4) Click .

- 5) Open the VNC Client located on a computer of the network connected to the unit.

Note: UltraVNC Viewer, TightVNC Viewer and VNC Viewer are presently supported.

- 6) Enter the **IPAddressOftheUnit:VNCid**

Note: For example 192.168.0.12:1

- 7) From the VNC client, wait for the following message to display "Press F12 for boot menu". If too late, restart the VM by clicking the  button.
- 8) Press F12, then select the USB device.
- 9) Follow the on-screen instructions.



Caution:

To reduce the wear-and-tear of the Solid State Drive:

- On Linux OS, disable memory swapping or at least set swappiness to 0.
- On Windows OS, disable the virtual memory.

Note: If the Solid State Drive fails because it is inadequately used by a third party software or the operating system, the warranty of the Mediatrix unit will no longer be valid.

Note: The installation can take more than an hour depending on the image you are installing.

Result

The virtual machine will be started only if it is started manually

Virtual Machine Configuration							
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
VirtualMachine_1		Unit MAC address	Unique ID	All v	e1000 v	Manual v	    

2.10.3.5 Disabling Swap on Linux

Information

Disabling swapping in the Operating System will optimise the virtual machine in such a way to reduce the wear-and-tear of the Solid State Drive.

Note: If the Solid State Drive fails because it is inadequately used by a third-party software or the operating system, the warranty of the Mediatrix unit will no longer be valid.

Steps

- 1) Open the VNC Client located on a computer of the network connected to the unit.

Note: UltraVNC Viewer, TightVNC Viewer and VNC Viewer are presently supported.

- 2) Open .../etc/sysctl.conf file
- 3) Add vm.swappiness = 0 to the file.
- 4) Open ... /etc/fstab.
- 5) Add noatime to the following lines
 - a) § UUID=32b414c0-This-is-an-example / ext4 defaults, noatime 1 1
 - b) § UUID=b4598e44-This-is-an-example /boot ext4 defaults, noatime 1 2
- 6) Comment out
 - a) § # UUID=72355f7a-497d-This-is-an-example swap swap defaults 0 0
- 7) Use the Shutdown command and then restart the Virtual Machine.

IMPORTANT: Do not use the Linux reboot command as the filesystem may not get mounted properly.

2.10.4 Virtual Machine Modification

2.10.4.1 Modifying the Virtual Machine Configuration

Steps

- 1) Go to **System/VM**.
- 2) In the **Virtual Machine Configuration** table, modify the fields as required.
- 3) Click **Apply**.

Result

The next time the virtual machine will be used, the new parameter values will be applied.

3 Network

3.1 Host

3.1.1 Basic Network Host Concepts

3.1.1.1 DNS Servers

The DNS server list is the ordered list of DNS servers that the device uses to resolve network names.

Up to four servers can be used. The DNS servers can be specified statically or obtained automatically (for example through DHCP or PPP). DNS query results are cached on the system to optimise name resolution time. For more details, refer to [DGW Configuration Guide - DNS Behavior with Mediatrix Gateways](#) published on the [Media5 Documentation Portal](#).

3.1.1.2 Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) is used to update and synchronise the clock of the Mediatrix unit (day, month, time) when it is restarted.

Mediatrix units do not all include a real time clock allowing them to maintain accurate time when they are shutdown. Your system needs to have access to accurate time, for example if you are using HTTPS or for the caller ID feature. The Mediatrix unit implements a SNTP client, which can synchronise the local clock with remote NTP/SNTP servers. The configuration can be automatic (through DHCP for example), with fallback, or static, with up to four servers.

3.1.1.3 Time Format

The time format (also known as 'TZ' format) is based on the format described by the IEEE 1003.1 standard (i.e. POSIX specification).

The Time Format contains two parts separated by a semicolon:

- The first part, mandatory, is the system timezone expressed in the IEEE 1003.1 POSIX format (also known as 'TZ' format).
- The second part, available since 46.0 is optional. It is the timezone used for the time displayed in some of the SBC Web pages (Live Calls, Events, and Registration). This part is only useful for units with the Sbc service. This string must be expressed in the IANA format. If this part is not present, the UTC time zone is used on the SBC Web pages.

The first part of the time format has this POSIX syntax:

```
STDOFFSET[DST[OFFSET], [START[/TIME], END[/TIME]]]
```

where:

- **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.

IMPORTANT: 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.

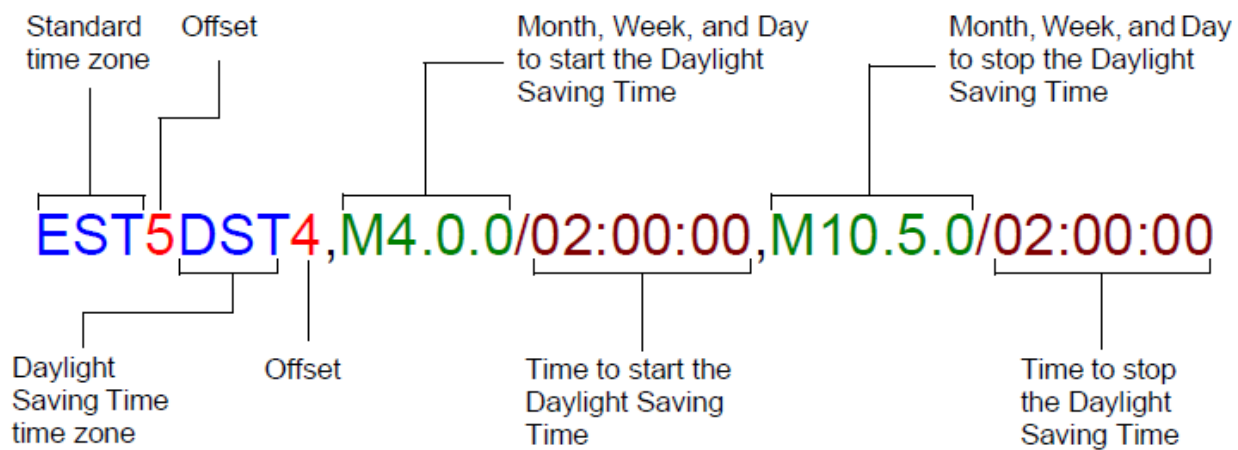
 - The minute and second values, if present, must be between 0 and 59.
- **START / END** Indicates when to change to and return from the daylight saving time. The START argument is the date when the change from the standard to the daylight save time occurs; END is the date for changing back. If START and END are not specified, the default is the US Daylight saving time start and end dates. The format for start and end must be one of the following:
 - **n** where n is the number of days since the start of the year from 0 to 365. It must contain the leap year day if the current year is a leap year. With this format, you are responsible to determine all the leap year details.
 - **Jn** where n is the Julian day number of the year from 1 to 365. Leap days are not counted. That is, in all years – including leap years – February 28 is day 59 and March 1 is day 60. It is impossible to refer to the occasional February 29 explicitly. The TIME parameter has the same format as OFFSET but there can be no leading minus (-) or plus (+) sign. If TIME is not specified, the default is 02:00:00.
 - **Mx[x].y.z** where x is the month, y is a week count (in which the z day exists) and z is the day of the week starting at 0 (Sunday). For instance: M10.4.0 is the fourth Sunday of October. It does not matter if the Sunday is in the 4th or 5th week. M10.5.0 is the last Sunday of October (5 indicates the last z day). It does not matter if the Sunday is in the 4th or 5th week. M10.1.6 is the first week with a Saturday (thus the first Saturday). It does not matter if the

Saturday is in the first or second week. The TIME parameter has the same format as OFFSET but there can be no leading minus (-) or plus (+) sign. If TIME is not specified, the default is 02:00:00.

More information on time zones are available at:

- https://en.wikipedia.org/wiki/List_of_time_zone_abbreviations
- https://en.wikipedia.org/wiki/List_of_tz_database_time_zones
- https://www.gnu.org/software/libc/manual/html_node/TZ-Variable.html

3.1.1.4 Time Format Examples



Time Zone	String	IANA format (Optional, 46.0+)
Atlantic Time (Canada)	AST4ADT,M3.2.0,M11.1.0	America/Halifax
Australia Eastern Standard Time	AEST-10AEDT,M10.1.0,M4.1.0/3	Australia/Sydney
Central European Time	CET-1CEST,M3.5.0,M10.5.0/3	Europe/Brussels
Central Time (Canada & US)	CST6CDT,M3.2.0,M11.1.0	America/Chicago
China Standard Time	CST-8	Asia/Shanghai
Eastern Time Canada & US)	EST5EDT,M3.2.0,M11.1.0	America/Toronto
Greenwich Mean Time	GMT0BST,M3.5.0/1,M10.5.0	Europe/London
Mountain Time (Canada & US)	MST7MDT,M3.2.0,M11.1.0	America/Denver
Pacific Time (Canada & US)	PST8PDT,M3.2.0,M11.1.0	America/Los_Angeles
Japan Standard Time	JST-9	Asia/Tokyo
UTC (Coordinated Universal Time)	UTC0	Etc/UTC
Western Europe Time	WET0WEST,M3.5.0/1,M10.5.0	Europe/Lisbon

3.1.2 Basic Network Host Tasks

3.1.2.1 Choosing the Network Providing the IPv4 Automatic configuration

Steps

- 1) Go to **Network/Host**.
- 2) In the **Automatic Configuration Interface** table, from the **Automatic IPv4 config source network** selection list, choose a network.
- 3) Click **Apply**.

3.1.2.2 Choosing the Network Providing the IPv6 Automatic configuration

Steps

- 1) Go to **Network/Host**.
- 2) In the **Automatic Configuration Interface** table, from the **Automatic IPv6 config source network** selection list, choose a network.

- 3) Click **Apply**.

3.1.2.3 Configuring the Host Name and Domain Name of the Mediatrix Unit

Steps

- 1) Go to **Network/Host**.
- 2) In the **Host Name Configuration** table, from the **Configuration Source** selection list, choose the source.

Note: When switching from the Static to Automatic IPv4 or Automatic IPv6 configuration source, the last value correctly obtained from the network (if any) is applied to the system.

- 3) If you are using a Static configuration source, in the **Domain Name** field, enter the domain name of your unit.

Note: The domain name is the network domain to which the unit belongs. For instance: example.com.

- 4) In the **Host Name** field, enter the host name of your unit.

Note: The host name is the unique name by which the unit is known on a network.

- 5) Click **Apply**.

Result

Host Name Configuration	
Domain Name	
Configuration Source:	Static
Domain Name:	domain name of unit
Host Name	
Host Name:	host name of the unit

3.1.2.4 Configuring the Default Network Gateway to a Static IP Address

Steps

- 1) Go to **Network/Host**.
- 2) In the **Default Gateway Configuration** table, from the **IPv4/Configuration Source** selection list, select **Static**.
- 3) In the **IPv4/Default Gateway** field, enter the IP address used as the **Static Default Router** for the Uplink Network Interface.
- 4) In the **Default Gateway Configuration** table, from the **IPv6/Configuration Source** selection list, select **Static**.

- 5) In the **IPv6/Default Gateway** field, enter the IP address used as the **Static Default Router** for the Uplink Network Interface.
- 6) Click **Apply**.

Result

The specified address is used as the current default router address.

Default Gateway Configuration	
IPv4	
Configuration Source:	Static
Default Gateway:	IP address
IPv6	
Configuration Source:	Static
Default Gateway:	IP address

3.1.2.5 Configuring the Default Network Gateway to an Automatic IP Address

Steps

- 1) Go to **Network/Host**.
- 2) In the **Default Gateway Configuration** table, from the **IPv4/Configuration Source** selection list, select **Automatic IPv4**.
- 3) In the **Default Gateway Configuration** table, from the **IPv6/Configuration Source** selection list, select **Automatic IPv6**.

Note: When switching from the Static to Automatic configuration source, the last value correctly obtained from the network (if any) is applied to the system.

- 4) Click **Apply**.

Result

Default Gateway Configuration	
IPv4	
Configuration Source:	Automatic IPv4 ▾
Default Gateway:	192.168.10.10
IPv6	
Configuration Source:	Automatic IPv6 ▾
Default Gateway:	

3.1.2.6 Configuring DNS Servers - Automatically

Steps

- 1) Go to **Network/Host**.
- 2) In the **DNS Configuration** table, from the **Configuration Source** selection list, choose **Automatic IPv4** or **Automatic IPv6**.
- 3) Click **Apply**.

Result

DNS Configuration	
Configuration Source:	Automatic IPv4 ▾
Primary DNS:	
Secondary DNS:	
Third DNS:	
Fourth DNS:	

3.1.2.7 Configuring DNS Servers - Manually

Steps

- 1) Go to **Network/Host**.
- 2) In the **DNS Configuration** table, from the **Configuration Source** selection list, choose **Static**.

- 3) For each DNS server, enter the IP address.

Note:

The best practice is to use the servers supplied by your Internet Service Provider (usually the primary and secondary DNS), then complement with publicly accessible DNS servers from a different network.

For example, when using IPv4: Google (8.8.8.8 and 8.8.4.4), CloudFlare (1.1.1.1 and 1.0.0.1), OpenDNS (208.67.222.222 and 208.67.220.220), Level3 (209.244.0.3 and 208.244.0.4), etc.

Or when Using IPv6: Google (2001:4860:4860::8888 and 2001:4860:4860::8844), CloudFlare (2606:4700:4700::1111 and 2606:4700:4700::1001), etc.

- 4) Click **Apply**.

Result

DNS Configuration	
Configuration Source:	Static
Primary DNS:	Example (Google): 8.8.8.8
Secondary DNS:	Example (Cloudflare): 1.1.1.1
Third DNS:	Example (OpenDNS): 208.67.222.222
Fourth DNS:	Example (Level3): 209.244.0.3

3.1.2.8 Configuring the SNTP Server to a Static IP Address

Before you start

Make sure there is an SNTP server available.

Steps

- 1) Go to **Network/Host**.
- 2) In the **SNTP Configuration** table, from the **Configuration Source** selection list, select **Static**.
- 3) Provide an IP address or domain name and port numbers for each SNTP server you are using.

Note: The best practice is to use the servers supplied by your Internet Service Provider, then complement with servers from a different network close to your geographical area. For example: time.nist.gov (USA), ntp4.sptime.se (Sweden), time1.isu.net.sa (Saudi Arabia), ntp.nict.jp (Japan), time.google.com (Worldwide), pool.ntp.org or one of their regional server pools (see <https://www.ntppool.org/> for more information).

- 4) If necessary, change the value of the **Synchronisation Period**.
- 5) If necessary, change the value of the **Synchronisation Period on Error**.
- 6) Click **Apply**.

Result

The SNTP host name and port will be displayed in the **Host Status** table under **Network/Status**.

SNTP Configuration	
Configuration Source:	Static v
Primary SNTP:	address of primary SNTP server
Secondary SNTP:	address of secondary SNTP server
Third SNTP:	address of third SNTP server
Fourth SNTP:	address of fourth SNTP server
Synchronization Period:	1440
Synchronization Period On Error:	60

3.1.2.9 Configuring the SNTP Server to an Automatic IP Address

Before you start

Make sure there is an SNTP server available.

Steps

- 1) Go to **Network/Host**.
- 2) In the **SNTP Configuration** table, from the **Configuration Source** selection list, select **Automatic IPv4** or **Automatic IPv6**.

Note: Some Uplink connection types (for example Static and PPPoE) cannot obtain SNTP information from the network, and therefore lead to no SNTP parameters being applied to the system.

- 3) If necessary, change the value of the **Synchronisation Period**.
- 4) If necessary, change the value of the **Synchronisation Period on Error**.
- 5) Click **Apply**.

Result

SNTP Configuration	
Configuration Source:	Automatic IPv4 v
Static Servers:	
Primary SNTP:	192.168.10.10:123
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

3.1.2.10 Configuring the SNTP Server to an Automatic IP Address with Fallback

Before you start

Make sure there is an SNTP server available.

Steps

- 1) Go to **Network/Host**.
- 2) In the **SNTP Configuration** table, from the **Configuration Source** selection list, select **Automatic IPv4** or **Automatic IPv6**.

Note: Some Uplink connection types (for example Static and PPPoE) cannot obtain SNTP information from the network, and therefore lead to no SNTP parameters being applied to the system.

- 3) Provide an IP address or domain name and port numbers for each SNTP server you are using.

Note:

The best practice is to use the servers supplied by your Internet Service Provider, then complement with servers from a different network close to your geographical area. For example: time.nist.gov (USA), ntp4.sptime.se (Sweden), time1.isu.net.sa (Saudi Arabia), ntp.nict.jp (Japan), time.google.com (Worldwide), pool.ntp.org or one of their regional server pools (see <https://www.ntppool.org/> for more information).

- 4) If necessary, change the value of the **Synchronisation Period**.
- 5) If necessary, change the value of the **Synchronisation Period on Error**.
- 6) Click **Apply**.

Result

SNTP Configuration	
Configuration Source:	Automatic With Fallback
Static Servers:	
Primary SNTP:	IP Address
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

3.1.2.11 Configuring the Mediatrix Unit to Use an SNTP Server

Before you start

Make sure there is an SNTP server available.

Information

Steps

- 1) Go to **Network/Host**.
- 2) In the **SNTP Configuration** table, from the **Configuration Source** selection list, select the connection type from which you wish to obtain the SNTP parameters.

Note: Complete [Step 3](#) only if you are using static SNTP server(s), otherwise go to [Step 4](#).

- 3) Provide an IP address or domain name and port numbers for each SNTP server you are using.
- 4) If necessary, change the displayed default value of the **Synchronisation Period**.
- 5) If necessary, change the displayed default value of the **Synchronisation Period on Error**.
- 6) Click **Apply**.

Result

The SNTP host name and port will be displayed in the **Host Status** table under **Network/Status**.

SNTP Configuration	
Configuration Source:	Automatic IPv4 ▾
Primary SNTP:	192.168.10.10:123
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization Period:	1440
Synchronization Period On Error:	60

3.1.2.12 Selecting the Unit's Time Zone

Information

Time Servers should be configured under Network/Host/SNTP Configuration. For more details refer to the [DGW Configuration Guide - Vlan Configuration](#) published on the [Media5 Documentation Portal](#).

Steps

- 1) Go to **Network/Host**.
- 2) In the **Time Configuration** table, in the **Static Time Zone** field, specify the time zone in which the Mediatrix unit is located.

Note: 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.

- 3) Click **Apply**.

Result

Any DGW parameter referring to a time value will use the local time described by this time zone reference. The **Hoc.SystemTime** will return the unit local time in accordance with the configured time zone.

3.1.3 Advanced Network Host Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by either:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Configuring Dns Cache Randomisation:

- **Hoc.DnsCacheRandomization**

Configuring Pre-resolved Static FQDNs

Up to 10 pre-resolved FQDNs can be configured. The StaticHosts table allows configuring FQDNs with static IP addresses. When a device attempts to reach a FQDN configured in this table, the static IP addresses will be used instead of resolving the FQDN.

- **Hoc.InsertStaticHost:** To insert a new static host
- **Hoc.StaticHosts.Delete:** To delete a static host:

Updating the system name or system location

The name and location of the Mediatrix unit can be specified. This information is for display purposes only and does not affect the behavior of the unit.

- Hoc.SystemName: To set the system name
- Hoc.SystemLocation: Set the system location

3.2 Interfaces

3.2.1 Basic Interface Concepts

3.2.1.1 IP Address Reservation

Before connecting the Mediatrix unit to the network, Media5 strongly recommends to reserve an IP address in your network server – if using one – for the unit you are about to connect.

This way, the IP address associated with a particular unit will be known. Network servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The Mediatrix unit unique identifier is the media access control (MAC) address. Refer to [Locating the MAC Address of Your Mediatrix Unit](#) (p.96).

3.2.1.1.1 Locating the MAC Address of Your Mediatrix Unit

Information

The MAC address of the unit is:

- printed on a label located under the Mediatrix unit

- displayed in the **Current Status** table of the Web Interface (**System/Information**)

3.2.1.2 Important Information About Network Interfaces

Naming

- The name of the network interface is case sensitive.
- Using the special values All, Loop, LoopV6, and Rescue are not allowed to name a network interface
- A valid network interface name:
 - must start with a letter
 - cannot contain characters other than letters, numbers, and underscores

Configuration

- It is not possible to have different IP addresses from the same subnet on one interface.
- It is possible to create up to 48 network interfaces.
- LLDP cannot be activated on multiple network interfaces simultaneously.
- If no network is configured in IPv6, the unit does not have any IPv6 address, not even the Link-Local address. When a network is configured in IPv6, the Link-Local (FE80 ::...) address is automatically created and displayed in the Network Status information.
- In case of address conflicts between two or more network interfaces, the network interface with the highest priority will remain enabled and the other interfaces will be disabled. If the priority is the same, only the first enabled network interface will be able to use the IP address. When a conflict ends, all network interfaces concerned automatically return to an operational state.
- Media5 recommends to reserve an IP address with an infinite lease for each Mediatrix unit on the network.
- The Rescue Network Interface cannot be deleted.

IMPORTANT: Use extreme care when configuring network interfaces, especially when configuring the network interface used to contact the unit for management. Be careful never to disable or delete the network interface used to contact the unit. Also be careful to always set the unit's management interface to be an interface that you can contact.

3.2.1.3 Default Network Interfaces

There are four Network Interfaces created by default on the Mediatrix unit: Uplink, Lan 1, UplinkV6, and Rescue.

- The **Uplink** network interface defines the uplink information required by the Mediatrix unit to properly connect to the WAN. (By default eth1 for all platforms, except for the 4102S which is

WAN . By default, this interface uses the **IpDhcp (IPv4 DHCP)** connection type. If you are using only one Network Interface, you must use **Uplink**.

- The **Lan1** network interface defines the information required by the Mediatrix unit to properly connect to the LAN.(By default eth2-5 for all platforms, except for the 4102 which is LAN) By default, the **Lan1** Network Interface uses the **IpStatic (IPv4 Static)** connection type. The **Lan1** network interface can only be added on units with 2 network ports.
- The **Rescue** network interface, is used to display the **Rescue** Management Interface when a partial reset of the unit is performed. By default, the **Rescue** network interface
 - is disabled and automatically enabled when a partial reset is performed.
 - uses the **IpStatic (IPv4 Static)** or the **Ip6Static (IPv6 Static)** addresses.

The **Rescue** Network Interface cannot be deleted. Refer to the [Technical Bulletin - Performing a Partial Reset](#) document published on the [Media5 Documentation Portal](#).

- The **UplinkV6** network interface defines the IPv6 uplink information required by the Mediatrix unit to properly connect to the WAN. By default, this interface uses the **IP6autoConf (IPv6 Auto-Conf)** configuration mode.

It is possible to create up to 48 Network Interfaces.

3.2.1.3.1 Link Default Values for the Uplink Network Interface

Unit Type	Link Default Value
Sentinel 400	eth1
Sentinel 100	eth1
Mediatrix G7	eth1
Mediatrix S7	eth1
Mediatrix C7 series	eth1
Mediatrix 4102S	Wan

3.2.1.3.2 Link Default Values for the Lan1 Network Interface

Unit Type	Link Default Value
Sentinel 400	eth2-5
Sentinel 100	eth2-5
Mediatrix G7 series	eth2-5
Mediatrix S7 series	eth2-5
Mediatrix C7 series	eth2
Mediatrix 4102	lan

3.2.1.4 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) service is used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, usually wired Ethernet.

LLDP cannot be activated on more than one network interface at a time.

3.2.1.5 Link Connectivity Detection

Each Ethernet port of the Mediatrix unit is associated with an Ethernet link.

An Ethernet link has connectivity if at least one of its port status is not disconnected. The link connectivity is periodically polled (every 500 milliseconds). It takes two consecutive detections of the same link state before reporting a link connectivity transition. This avoids reporting many link connectivity transitions if the Ethernet cable is plugged and unplugged quickly.

3.2.1.6 PPP Negotiation

When the Mediatrix unit restarts, it establishes the connection to the access concentrator in conformance with RFC 2516 section 5.1.

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

- **Discovery phase:** The Mediatrix unit broadcasts the value of the Service Name field. The access concentrator with a matching service name answers the Mediatrix unit.
 - If no access concentrator answers, this creates a **PPPoE failure** error.
 - If more than one access concentrators respond to the discovery, the Mediatrix unit tries to establish the PPP connection with the first one that supports the requested service name.

- **Authentication phase:** If the access concentrator requests authentication, the Mediatrix unit sends the ID/secret pair configured in the User Name and Password fields. If the access concentrator rejects the authentication, this creates an “authentication failure” error.
- **Network-layer protocol phase:** The Mediatrix unit negotiates an IP address. The requested IP address is the one from the last successful PPPoE connection. If the Mediatrix unit never connected by using PPPoE (or after a factory reset), it does not request any specific IP address.

3.2.1.7 IPv6 Autoconfiguration Interfaces

When the Type drop-down menu is set to IPv6 Auto-Conf, the network interface is an IPv6 over Ethernet connection with IP parameters obtained by stateless auto-configuration or stateful (DHCPv6) configuration.

Autoconfiguration of IPv6 address is first initiated using state-less autoconfiguration. Stateful autoconfiguration is initiated only if one of the following conditions is met:

- The router explicitly required stateful autoconfiguration by setting the “managed” or “other” flag of the router advertisement.
- No router advertisement was received after 3 router solicitations. RFC 4861 defines the number of router solicitations to send and the 4 seconds interval between the sent router solicitations.

3.2.1.8 Stateless Autoconfiguration

All IPv6 addresses present in the router advertisements are applied to the network interface

Each IPv6 address is assigned a network name based on the configured network name with a suffix in the following format: ConfiguredNetworkName-XX-Y. XX is the address scope

- GU (Global Unique)
- UL (Unique Local)
- LL (Link-Local)

Y is a unique ID for the address scope.

3.2.1.9 Spanning Tree Protocol vs Stateless Autoconfiguration

Many network switches use the Spanning Tree Protocol (STP) to manage Ethernet ports activity.

STP uses a detection timeout before a router advertisement is sent to the Mediatrix unit. The default value for this timeout is usually 30 seconds. However, when the unit wants to get an IPv6 address in Stateless autoconfiguration, this timeout is too long and the unit falls into Stateful Autoconfiguration mode before it receives the router advertisement. This results in the unit receiving a DHCPv6 address. To solve the issue, check if the default STP detection timeout value in your router can be modified. If so, set it to a value of 8 s or less. If you cannot modify the timeout value, Media5 recommends to disable the Spanning Tree Protocol on the network to which the unit is connected.

3.2.1.10 Statefull Autoconfiguration

Stateful autoconfiguration is managed by DHCPv6. The DHCPv6 lease is negotiated according to the limitations listed in section 1.5 of RFC 3315.

DHCPv6 may be used to obtain the following information (depending on the router advertisement flags):

- IPv6 addresses (when the router advertisement “managed” flag is set)
- Other configuration (when the router advertisement “other” flag is set)

If only the “other” flag is set in the router advertisement, the DHCPv6 client only sends an information request to the DHCPv6 server, otherwise it sends a DHCPv6 solicit message. If the flags change over time, only the transitions from “not set” to “set” are handled.

3.2.1.11 Speed and Duplex Detection Issues

There are two protocols for detecting the Ethernet link speed: parallel detection and auto-negotiation (IEEE 802.3u).

The auto-negotiation protocol allows the detection of the connection speed and duplex mode. It exchanges capabilities and establishes the most efficient connection. When both endpoints support the auto-negotiation, there are no problems. However, when only one endpoint supports auto-negotiation, the parallel detection protocol is used. This protocol can only detect the connection speed; the duplex mode cannot be detected. In this case, the connection may not be established. The Mediatrix unit has the possibility to force the desired Ethernet link speed and duplex mode by disabling the auto-negotiation and selecting the proper setting. When forcing a link speed at one end, be sure that the other end (a hub, switch, etc.) has the same configuration. To avoid any problem, the link speed and duplex mode of the other endpoint must be exactly the same.

3.2.2 Basic Interface Tasks

3.2.2.1 Creating a Network Interface

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **Network Interface Configuration** table, click +.
- 3) Enter a name in the **Name** field.

Note: The Network Interface name must be unique and is case sensitive.

- 4) From the **Link** selection list, select **Ip6Static (IPv6 Static)**.
- 5) In the **Static IP Address** field, enter the FQDN or IP address of
- 6) Click **Apply**.

Result

The new Network Interface will be available in the:

- **Media Interface Configuration** table under the **SBC/ Configuration** tabs (provided you have the Sbc service)
- **Signaling Interface Configuration** table under **SBC/ Configuration** tabs (provided you have the Sbc service)
- **DHCP Server Configuration** table under the **Network/ DHCP Server** tabs
- **Signaling Network** table under the **SIP/Gateways** tabs
- **Network Interface** table under the **SIP Proxy/Configuration** tabs.
- **Network Interface** table under the **Management/Misc** tabs.
- **Forward To Network** table under the **Network/IP Routing** tabs.

3.2.2.2 Configuring a Network Interface

Information

When configuring network interfaces, Media5 recommends to have a syslog client properly configured and enabled in order to receive any message related to the network interfaces behaviour. The interface used to access the syslog client must also be properly enabled.

Steps

- 1) Go to **Network/Interfaces**.

IMPORTANT: Use extreme care when configuring network interfaces, especially when configuring the network interface used to contact the unit for management. Be careful never to disable or delete the network interface used to contact the unit. Also be careful to always set the unit's management interface to be an interface that you can contact.

- 2) In the **Network Interface Configuration** table, complete the fields as required.
- 3) From the **Activation** drop-down list, select **Enable**.
- 4) Click **Apply**.

3.2.2.3 Associating an Ethernet Link to a Network Interface

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **Network Interface Configuration** table, from the **Link** field , select the link to be associated with a Network Interface (the link will appear as ethx.VlanId).

Note: Once the changes are applied, the connection with the unit might be lost. You may need to reconnect to the Web page.

- 3) Complete the fields as required.

- 4) Click **Apply**.

Result

The Network interface is associated with a physical interface i.e. an Ethernet Link.

Network Interface Configuration						
Name	Link	Type	Static IP Address	Static Default Router	Activation	
Lan1	eth1	IpStatic (IPv4 Static)	192.168.0.10/24		Enable	-
Uplink	eth2-5.4	IpDhcp (IPv4 DHCP)	192.168.10.1/24		Enable	-
						+

3.2.2.4 Configuring the PPPoE Connection Type

Before you start

The **User Name** and **Password** fields are not accessible if you have the User or Observer access right.

Information

Perform this procedure only if you have selected **Ppplpcp (IPv4 PPPoE)** as a connection type for your Network Interfaces.

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **PPPoE Configuration** table, complete the fields as required.
- 3) Click **Apply**.

Result

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

3.2.2.5 Configuring the Link Layer Discovery Protocol (LLDP)

Before you start

The Lldp service must be started.

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **LLDP Configuration** table, select the network interface name on which LLDP should be enabled.

Note: LLDP cannot be activated on multiple network interfaces simultaneously.

- 3) Select the address type to populate the chassis ID device identifier.
- 4) Select whether to enable the LLDP-MED protocol override of the VLAN ID.
- 5) Click **Apply** if you do not need to set other parameters.

Result

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

3.2.2.6 Configuring a Link as a Virtual Switch

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **Ethernet Link Configuration** table, from the **Virtual Switch** selection list, select **Enable** located on the same row as the link you wish to enable for the virtual switch.
- 3) Click **Apply**.

Result

Ethernet Link Configuration						
Link	MTU	802.1x Authentication	EAP Username	EAP Certificate Validation	Virtual Switch	
eth1	1500	Disable		Trusted And Valid	Enable	
eth2-5	1500	Disable		Trusted And Valid	Disable	

3.2.2.7 Configuring the Ethernet Link linked to a Network Interface

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **Ethernet Link Configuration** table, set the **MTU** field of a specific Ethernet link with required value.

Note: The MTU value applied for a PPPoE connection is the smallest of the value negotiated with the server and the value configured here.

Note: Each Network interface used by TCP/IP may have a different MTU value specified. All VLAN connections use the MTU size configured on their related Ethernet link.

- 3) From the **802.1x Authentication** select **Enable** for each Ethernet link requiring 802.1x Authentication.
- 4) Enter the **EAP username** used to authenticate each Ethernet link interfaces during the IEEE 802.1x EAPTLS authentication process..
- 5) From the **EAP Certificate Validation** field, choose the IEEE 802.1x level of validation used by the device to authenticate the IEEE 802.1x EAPTLS peer's certificate.
- 6) Click **Apply** if you do not need to set other parameters.

Result

The current status of the network interfaces is displayed in the **Status** page.

3.2.2.8 Selecting the IEEE 802.1x Version

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **EAP 802.1x Configuration** table, select the IEEE 802.1x version.
- 3) Click **Apply** if you do not need to set other parameters.

Result

EAP 802.1x Configuration	
EAP 802.1x Version:	Version 2001

3.2.3 Advanced Network Interface Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Network Interfaces Priority

Refer to **eth.networkInterfacesPriority**

DHCP Client Identifier Presentation

Refer to **bni.dhcpClientIdentifierPresentation**

Ethernet Connection Speed

Refer to **eth.portsSpeed**

3.3 VLAN

3.3.1 Basic VLAN Tasks

3.3.1.1 Creating a VLAN

Steps

- 1) Go to **Network/VLAN**.
- 2) In the **VLAN Configuration** table, from the **Link** selection list, select the Ethernet link the vlan will use.
- 3) Complete the **VlanId** and the **Default User Priority** fields as required.
- 4) Click **+** located at the end of the newly created Vlan.
- 5) Click **Apply**.

Note: Do not forget to enable the Vlan under **Network/Interfaces**

3.3.1.2 Associating a VLAN to an Ethernet Link

Steps

- 1) Go to **Network/VLAN**.
- 2) From the **Link** selection list, select the Ethernet link the VLAN interface will use.
- 3) In the VlanId field, set the VLAN ID used by the VLAN interface.
- 4) In the VLAN configuration table, click +.
- 5) Set the default user priority value.
- 6) To create another VLAN, repeat steps 1 to 5.
- 7) Click **Apply**.

Result

The Vlan will be associated with a physical interface i.e. an Ethernet Link.

VLAN

VLAN Configuration			
Link	VlanId	Default User Priority	
eth1	xxx		+

3.3.1.3 Configuring the Default User Priority on an Existing VLAN

Steps

- 1) Go to **Network/VLAN**.
- 2) Under the **Default User Priority** column, set the User Priority to the respective VLAN.

Note: For specific services (Signaling, Voice, T.38) you can override the values above by setting specific service class values. Refer to [Overriding the DiffServ and QoS Service Class Default Values](#) (p.111).

- 3) Click **Apply**.

Result

The value of the **Default User Priority** column will be applied to the existing VLAN.

3.3.1.4 Configuring the Default User Priority on a New VLAN

Steps

- 1) Go to **Network/VLAN**.
- 2) Under the **Link** column, select the physical link to which you want to add a VLAN.
- 3) Under the **VlanId** column, define the number of the VLAN you wish to create.
- 4) Click **+** located on the right hand side of the screen.
- 5) Under the **Default User Priority** column, set the User Priority for the respective VLAN.

Note: For specific services (Signaling, Voice, T.38) you can override the above values by setting specific service class values. Refer to [Overriding the DiffServ and QoS Service Class Default Values](#) (p.111).

- 6) Click **Apply**.

Result

The value of the **Default User Priority** column will be applied to the newly created VLAN.

3.4 QoS

3.4.1 Basic QoS Concepts

3.4.1.1 Quality of Service (QoS)

QoS (Quality of Service) features enable network managers to decide on packet priority queuing.

DGW supports:

- Differentiated Services (DS) Field (for IPv4)
- Traffic Class Field (for IPv6)
- 802.1Q taggings

3.4.1.2 Differentiated Services (DS) Field (for IPv4 only)

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 byte. In DGW the entire ToS byte is currently configurable, thus the ToS decimal value is used. Please refer to:

- <https://tools.ietf.org/html/rfc2474> for the definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.
- https://en.wikipedia.org/wiki/Differentiated_services for the differentiated services.

For example, for a DSCP value of 46, the ToS value of 184 should be used. For DSCP and ToS mappings, please refer to the following table:

TOS (Dec)	TOS (Hex)	TOS (Bin)	TOS Precedence (Bin)	TOS Precedence (Dec)	TOS Precedence Name	TOS Delay flag	TOS Throughput flag	TOS Reliability flag	DSCP (Bin)	DSCP (Hex)	DSCP (Dec)	DSCP/PHB Class
0	0x00	00000000	000	0	Routine	0	0	0	000000	0x00	0	none
4	0x04	00000100	000	0	Routine	0	0	1	000001	0x01	1	none
8	0x08	00001000	000	0	Routine	0	1	0	000010	0x02	2	none
12	0x0C	00001100	000	0	Routine	0	1	1	000011	0x03	3	none
16	0x10	00010000	000	0	Routine	1	0	0	000100	0x04	4	none
32	0x20	00100000	001	1	Priority	0	0	0	001000	0x08	8	cs1
40	0x28	00101000	001	1	Priority	0	1	0	001010	0x0A	10	af11
48	0x30	00110000	001	1	Priority	1	0	0	001100	0x0C	12	af12
56	0x38	00111000	001	1	Priority	1	1	0	001110	0x0E	14	af13
64	0x40	01000000	010	2	Immediate	0	0	0	010000	0x10	16	cs2
72	0x48	01001000	010	2	Immediate	0	1	0	010010	0x12	18	af21
80	0x50	01010000	010	2	Immediate	1	0	0	010100	0x14	20	af22
88	0x58	01011000	010	2	Immediate	1	1	0	010110	0x16	22	af23
96	0x60	01100000	011	3	Flash	0	0	0	011000	0x18	24	cs3
104	0x68	01101000	011	3	Flash	0	1	0	011010	0x1A	26	af31
112	0x70	01110000	011	3	Flash	1	0	0	011100	0x1C	28	af32
120	0x78	01111000	011	3	Flash	1	1	0	011110	0x1E	30	af33
128	0x80	10000000	100	4	FlashOverride	0	0	0	100000	0x20	32	cs4
136	0x88	10001000	100	4	FlashOverride	0	1	0	100010	0x22	34	af41
144	0x90	10010000	100	4	FlashOverride	1	0	0	100100	0x24	36	af42
152	0x98	10011000	100	4	FlashOverride	1	1	0	100110	0x26	38	af43
160	0xA0	10100000	101	5	Critical	0	0	0	101000	0x28	40	cs5
176	0xB0	10110000	101	5	Critical	1	0	0	101100	0x2C	44	voice-admit
184	0xB8	10111000	101	5	Critical	1	1	0	101110	0x2E	46	ef
192	0xC0	11000000	110	6	InterNetwork Control	0	0	0	110000	0x30	48	cs6
224	0xE0	11100000	111	7	Network Control	0	0	0	111000	0x38	56	cs7

3.4.1.3 Network Traffic Control

It is possible to apply bandwidth limitations to the network interfaces.

The limitations are applied on the raw data of the physical link and not only on the payload of the packets. All headers, checksums and control bits (TCP, IP, CRC, etc.) are considered in the actual bandwidth. A bandwidth limitation is applied on a physical link and not on a virtual network interface. All high-level network interfaces (including VLANs) using the same physical link are affected by a configured limitation. This limitation is applied to outgoing traffic only (egress). Bandwidth limitation is an average of the amount of data sent per second. Thus, it is normal that the unit sends a small burst of data after a period of silence.

3.4.2 Basic QoS Tasks

3.4.2.1 Creating the Default Unit QoS

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/QoS**.
- 2) In the **Differentiated Services Field Configuration** table, complete the fields as required, in order to define the default Differentiated Services value for all generated IPv4 packets and the default Traffic Class value for all generated IPv6 packets.

IMPORTANT: For specific services (Signaling, Voice, T.38) above values can be overridden by setting the specific service class values. Refer to [Overriding the DiffServ and QoS Service Class Default Values](#) (p.111).

- 3) Click **Apply**.

Result

The unit will apply the specified values as default values for all generated IPv4 and IPv6 packets respectively.

3.4.2.2 Configuring the Default User Priority on Physical Links (802.1Q Tagging)

Information

The 802.1Q standard recommends the use of the 802.1Q VLAN tags for Ethernet frames traffic prioritisation. 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 VLAN ID part of the 802.1Q tag is always set to 0.

Steps

- 1) Go to **Network/QoS**.
- 2) In the **Ethernet 802.1Q Tagging Configuration** table, select **Enable** for each interface on which you want to enable user priority tagging.
- 3) Set the **Default User Priority** value each interface uses when tagging packets in the **Default User Priority** column.

Note: For specific services (Signaling, Voice, T.38) you can override the values above by setting specific service class values. Refer to [Overriding the DiffServ and QoS Service Class Default Values](#) (p.111).

- 4) Click **Apply**.

Result

The selected **Default User Priority** values will be applied to the Physical Links (VLAN ID = 0) for which the 802.1Q tagging is set to **Enable**.

3.4.2.3 Overriding the DiffServ and QoS Service Class Default Values

Steps

- 1) Go to **Network/QoS**.
- 2) In the **Service Class Configuration** table, for each service class, set for IPv4 packets the **DiffServ** value or the **Traffic Class** value for IPv6 packets, .
- 3) Set a specific **User Priority** for each class under the **User Priority** column.
- 4) Click **Apply**.
- 5) Click **restart required services**, located at the top of the page.

Result

The values set for the **DiffServ** or the **Traffic Class** parameters will override any value already specified for the service class (Signaling, Voice, T.38).

3.4.2.4 Configuring Network Traffic Control

Before you start

The Network Traffic Control (NTC) service must be enabled. Refer to [Enabling the Network Traffic Control \(NTC\) Service](#) (p.236).

Steps

- 1) Go to **Network/QoS**.
- 2) In the **Network Traffic Control Configuration**, set the **Egress Limit** field for the selected link interface.

IMPORTANT:

The range is from 64 to 1,000,000 kilobits per second. The value 0 means no bandwidth limitation and no prioritisation. This value must be set according to the upstream bandwidth limit of the network on this link. Set to 0 (disable) if the network bandwidth exceeds 1,000,000 kbps or the effective limit of this device. NTC service sends packets on the physical link according to their respective priorities. The lower the value, the higher the priority. Packets with lower priority are dropped first. The maximum value of the HiddenMaxEgressLimit is :

- 1,000,000 kilobits on the Sentinel 400
- 500,000 kilobits on the Sentinel 100, Mediatrix G7 series, and Mediatrix S7 series
- 40,960 kilobits (5MB/s) on all other platforms

- 3) Click **Apply**.

Result

The defined egress limit is applied on the respective ETH interface.

3.4.3 Example

3.4.3.1 Default Unit QoS and Service Class Configuration for IPv4

Any IPv4 packet sent from the unit has the value applied in the **Default DiffServ (IPv4)** field of the **Differentiated Services Field Configuration** table under **Network/QoS** tab. This default value is overridden on what concerns the specific service classes defined under the same area and in the **Service Class Configuration** table.

In the following example, the ToS decimal value for the default egress IPv4 traffic is 120 (which corresponds to DSCP=30 or AF, Assured Forwarding), while for the Signaling service class, the DiffServ value is equal to 184 (DSCP=46 or EF, Expedited Forwarding)

QoS

Differentiated Services Field Configuration			
Default DiffServ (IPv4):	120		
Default Traffic Class (IPv6):	0		

Ethernet 802.1Q Tagging Configuration			
Physical Link	Enable	Default User Priority	
eth1	Disable	0	
eth2-5	Disable	0	

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

When the unit generates a DNS query (which does not belong to the Signaling service class) the default unit IPv4 DiffServ value is applied (ToS=120 or DSCP=30), as shown in the trace below:

```

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x78 (DSCP: AF33, ECN: Not-ECT)
    0111 10.. = Differentiated Services Codepoint: Assured Forwarding 33 (30)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 72
  Identification: 0x2068 (8296)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x960d [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.102
  Destination: 192.168.1.1
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  User Datagram Protocol, Src Port: 24449, Dst Port: 53
  Domain Name System (query)
  
```

When the unit generates a SIP packet (which belongs to the Signaling service class) the Signaling-specific DiffServ value is applied (ToS=184 or DSCP=46) as shown in the trace below:


```

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 188.40.86.131
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 441
  Identification: 0xa6e7 (42727)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0xbcd8 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.102
  Destination: 188.40.86.131
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  User Datagram Protocol, Src Port: 5060, Dst Port: 5060
  Session Initiation Protocol (REGISTER)

```

3.5 Local Firewall

3.5.1 Basic Local Firewall Concepts

3.5.1.1 Local Firewall

The local firewall allows you to create and configure rules to filter incoming packets that have the Mediatrix unit as destination.

The Local Firewall is therefore a security feature that allows you to protect your Mediatrix unit from receiving packets from unwanted or unauthorized peers. As a best practice, the way the Local Firewall should work is to, by default, drop all incoming packets (i.e. not forward the packet to its destination) and let incoming packets go through only if they match a rule requirements. However, incoming packets for an IP communication established by the Mediatrix unit are always accepted (Example : If the Mediatrix unit sends a DNS request, the answer will be accepted).

When configuring the Local Firewall, enabling the default policy to drop all incoming packets should be the last step you perform otherwise, you may lose contact with the Mediatrix unit, even if you are performing the initial configuration of your system. Therefore, start by creating the rules that allow the Mediatrix unit to accept some packets. This way communication will not be lost and you will not need to perform a partial or factory reset to reconnect with the Mediatrix unit.

You can use a maximum of 20 rules, but the more rules are enabled, the more overall performance is affected.

3.5.1.2 Firewall Rule Order - Important

The order in which the incoming packets are tested against the rules is important if you want to make sure that they actually have a filtering effect on incoming packets.

Rules can be configured to accept or to decline packets. But, always put the most restrictive rules first as they are executed sequentially starting with the first one listed at the top of the table i.e.

make sure that the order in which the rules are executed does not cause a rule to be systematically excluded.

For example:

- If the first rule excludes all packets coming from a specific net mask, providing a second rule for an IP address with that same net mask will have no effect.
- If the first rule indicates actions to be taken for a specific IP address with a given net mask, and the second rule indicates to exclude all IP addresses with that net mask, both rules will be applied and have a result on the incoming packets.

3.5.2 Basic Local Firewall Tasks

3.5.2.1 Configuring the Local Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Rules** table, complete the fields as required.
- 3) In the **Local Firewall Configuration** table, from the **Default Policy** selection list, select **Drop**.

IMPORTANT: Before setting the **Default Policy** to **Drop**, i.e. to apply the local firewall rules and to drop any incoming call that does not match a rule, review your rules to make sure that at least one rule accepts incoming packets for management, otherwise the communication with the Mediatrix Sentinel will be lost.

Note: For example, if the Web interface is used for management (HTTP port 80) via the unit's LAN interface (default IP address = 192.168.0.10), then the following rule could be added: **Activation=Enable / Destination Address=192.168.0.10 / Destination port=80 / Protocol=TCP / Action=Accept**

Note: For blacklisting to be used, at least one firewall rule must have the **Black listing enable** box checked.

Note: Before setting the **Default Policy** to **Drop**, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix Sentinel will be lost.

- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

The Local Firewall will drop packets without any notification message.

If a rule with the **Black listing enable** box checked matches a packet and no **Rate Limit Value** was set, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration of the **Blacklist Timeout**.

If a rule with the **Black listing enable** box checked matches a packet and the **Rate Limit Value** has been reached, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration set for the **Blacklist Rate Limit Timeout**.

3.5.2.2 Disabling the Local Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Configuration** table, set the **Default Policy** to **Accept**.
- 3) In the **Local Firewall Rules** table, from the **Activation** column, select **Disable** for all the rules.
- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

All incoming packets will be accepted.

3.5.2.3 Setting the No Match Local Firewall Default Policy

Steps

- 1) Go to **Network/Local Firewall**.

Note: Before setting the **Default Policy** to **Drop**, i.e. to apply the local firewall rules and to drop any incoming call that does not match a rule, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix Sentinel will be lost.

- 2) In the **Local Firewall Configuration** table, set the **Default Policy** to **Drop**.

Result

The local firewall rules will be applied and if an incoming call does not match a call it will be dropped.

3.5.2.4 Configuring Black Listing Duration

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Configuration** table, set the **Blacklist Timeout**
- 3) Set the **Blacklist Rate Limit Timeout**.
- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

Blacklisting parameters will be updated. Remember that for blacklisting to be used, at least one rule must have blacklisting enabled.

If a rule with the **Black listing enable** box checked matches a packet and no **Rate Limit Value** was set, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration of the **Blacklist Timeout**.

If a rule with the **Black listing enable** box checked matches a packet and the **Rate Limit Value** has been reached, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration set for the **Blacklist Rate Limit Timeout**.

3.5.3 Local Firewall Examples

3.5.3.1 Generic Whitelist

All incoming calls are dropped unless they match one of the firewall rules which are acting on the incoming packets going towards the Mediatrix gateway.

Local Firewall

Configuration Modified: Yes	
Local Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable	Lan1/		Lan1		All	☐	Accept	10	60	^	v + -
2	Enable	Uplink/		Uplink		All	☐	Accept	10	60	^	v + -
3	Enable	IP address		Uplink	80	TCP	☐	Accept	10	60	^	v + -
4	Enable	IP address		Uplink	443	TCP	☐	Rate limit source	10	60	^	v + -
5	Enable	Subnet		Uplink	22	UDP	☐	Accept	10	60	^	v + -
6	Enable	Subnet		Uplink	5060	UDP	☐	Accept	10	60	^	v + -
7	Enable	Subnet		Uplink	5004-6020	UDP	☐	Accept			^	v + -
												+

Result:

Rule #	
1	Any incoming packet from the LAN subnet having the unit's LAN host IP address as a destination is allowed.
2	Any incoming packet from the Uplink subnet is allowed (assuming this is a private network).
3	Any HTTP incoming packet from the selected IP address having the unit's Uplink IP address as a destination through TCP port 80 is allowed.
4	Any HTTPS incoming packets from the selected IP address having the unit's Uplink IP address as a destination through TCP port 443 is allowed, but rate limited to 10 new connection attempts per 60 sec.
5	Any SSH incoming packets from the selected subnet having the unit's Uplink IP address as a destination through TCP port 22 is allowed.
6	Any SIP incoming packets from the selected subnet having the unit's Uplink IP address as a destination through UDP port 5060 is allowed.
7	Any RTP and T.38 incoming packet from the selected subnet having the unit's Uplink IP address as a destination through UDP port range 5004-6020 is allowed.
Default	All other incoming packets are rejected.

3.5.3.2 Whitelist for Internet Hacker Protection

Simple Local Firewall rules to protect the unit from Internet hackers. All incoming calls are dropped unless they match one of the local firewall rules which are acting on the incoming traffic towards the Mediatrix gateway.

Local Firewall

Configuration Modified:	Yes
-------------------------	-----

Local Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable	Lan1/		Lan1		All	☐	Accept	10	60	^	v + -
2	Enable	Uplink/		Uplink		All	☐	Accept	10	60	^	v + -
3	Enable	IP address		Uplink		All	☐	Accept	10	60	^	v + -
4	Enable	Subnet		Uplink		All	☐	Accept			^	v + -
												+

Result:

Rule #	Description
1	Any incoming packet from the LAN subnet is allowed.
2	Any incoming packet from the Uplink subnet is allowed (assuming this is a private network).
3	Any incoming packet from selected IP address is allowed (e.g. this is the management server).
4	Any incoming packet from the selected subnet is allowed (e.g. this is the Core SIP server, SBC and its media gateways).
Default	Any incoming packet not meeting the criteria of these rules is dropped.

3.5.3.3 Generic Blacklist

The default policy is set to "Accept" but the firewall rules are Blacklists acting on incoming traffic towards the Mediatrix gateway:

Local Firewall

Configuration Modified:	Yes
-------------------------	-----

Local Firewall Configuration	
Default Policy:	Accept
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable			Uplink	22	TCP	☐	Drop	10	60	▲▼+ -	
2	Enable	Subnet				All	☐	Drop	10	60	▲▼+ -	
3	Enable	IP address		Uplink	80	TCP	☐	Drop	10	60	▲▼+ -	
4	Enable	Subnet		Lan1		All	☐	Reject	10	60	▲▼+ -	
5	Enable	IP address		Lan1	5060	UDP	☐	Rate limit source	10	60	▲▼+ -	
												+

Subnet example: 192.168.1.0/24

Result:

Rule #	Description
1	Any incoming packet going to the Uplink interface through TCP port 22 (SSH) is dropped.
2	Any incoming packet coming from the specified subnet is dropped.
3	Any HTTP incoming packet coming from the specified IP address to the Uplink interface through TCP port 80 is dropped.
4	Any incoming packet from the specified subnet to the Lan1 interface is rejected, and an ICMP message is returned.
5	Any SIP incoming packets from the specified IP address to the Lan1 interface through UDP port 5060 is rate limited to 10 new connection attempts per 60 sec.
Default	All other incoming packets are accepted.

3.6 IP Routing

3.6.1 Basic IP Routing Concepts

3.6.1.1 Important Information About IP Routing

- The Mediatrix unit's IP Routing settings do not support IPv6.
- A packet matching a route uses the custom routing table first and then the main routing table if no route in the custom routing table was able to send the packet to the desired destination IP address.
- When creating an advanced IP routing Rule, leaving the **Source Address** or/and **Source Link** fields empty, indicate that any source of address or/and link will match the rule
- IP Routing works together with the following services:
 - Network Firewall
 - NAT
 - DHCP server
 - Network Traffic Control
- When the IP Routing service is started and the IPv4 Forwarding is enabled, IP routing is activated even if there is no configured rule (the Mediatrix unit will forward received packets). If the IP Routing service is stopped, IP forwarding is disabled, this tab is greyed out and the parameters are not displayed.

- Enabling the IP routing service and adding rules has an impact on the Mediatrix unit's overall performance as IP routing requires additional processing. The more rules are enabled, the more overall performance is affected.

Note: Media5 recommends to use a 30 ms packetization time when IP routing is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

3.6.1.2 IP Routing Rule Order - Important

The IP routing rules sequence is very important because only one forwarding rule is applied on a packet. Rules priority is determined by their position in the **Advanced IP Routes** table. If you want the unit to try to match one rule before another one, you must put that rule first. Make sure to put the most restrictive rules before the less restrictive ones.

3.6.1.3 Static IPv4 vs Advanced IP Routing

Network IP routing defines the routes for outgoing network traffic, where each route is associated with a network interface. The selection of which route a network packet should follow is generally based on the destination IP address criteria.

The Static IPv4 Routes are used to specify additional routes from the default ones automatically created by the configuration of the various network interfaces (see the BNI service).

The Advanced IP Routes are used only when IPv4 Forwarding is enabled, and allow to select a route, not just from the destination IP address, but also from the source IP address and interface criteria.

3.6.2 Basic IP Routing Tasks

3.6.2.1 Enabling IPv4 Forwarding

Steps

- 1) Go to **Network/IP Routing**.
- 2) In the **IP Routing configuration** table, select **Enable**.
- 3) Click **Save**.

Result

If IP Forwarding is disabled, the **Advanced IP Routes** table is greyed out.

IP Routing configuration	
IPv4 Forwarding:	Enable 

3.6.2.2 Creating an IP Routing Rule

Steps

- 1) Go to **Network/IP Routing**.
- 2) In the **Advanced IP Routes** table, click .
- 3) Complete the fields as required.

Note: Leaving the **Source Address** or/and **Source Link** fields empty, indicate that any source of address or/and link will match the rule

Note: Do not forget to **Enable** the route.

Note: The yellow Yes displayed at the top of the window indicates that the configuration has been modified but not applied (i.e., the Advanced IP Routes section of the Status page differs from the IP Routing page).

- 4) Click **Save & Apply**

Result

The enabled rules are displayed under **Network/ Status**, in the **Advanced IP Routes** section, The yellow Config Modified Yes flag is cleared.

Advanced IP Routes						
Priority	Activation	Source Address	Source Link	Forward To Network		
1	Enable 	Source Address	Source Link 	link 	  	
2	Enable 	Source Address	Source Link 	link 	  	
						

3.6.2.3 Creating a Static IPv4 Route

Steps

- 1) Go to **Network/IP Routing**.
- 2) In the **Static IP Routes** table, click .
- 3) Complete the fields as required.

Note: When the **Link** field is left empty, the link is automatically selected according to the gateway IP address and the information already present in the routing table.

4) Click **Save & Apply**

Result

Static IP Routes				
Index	Destination	Link	Gateway	
1	Destination IP Address	Link ▼	Gateway IP Address	–
2	Destination IP Address	Link ▼	Gateway IP Address	–
				+

The current routes available are displayed in the **Network/Status** under the **IP4 Routes** IPv4 Routes table.

IPv4 Routes				
Link	Destination	Gateway	Protocol	
eth1	0.0.0.0/0		Static	
eth1	static.ip.route	your.default.gateway	Kernel	
eth1	uplink.network/subnet	static.gateway.ip	Static	
eth1	10.5.0.0/16	0.0.0.0	Kernel	

3.6.3 Advanced IP Routing Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on advanced parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- To define whether or not the Classless Static Route Option is enabled:
Bni.DhcpClientClasslessStaticRouteOption
- To define a list of user classes: **Bni.DhcpClientUserClass**

3.6.4 IP Routing Configuration Examples

Refer to the [Technical Bulletin - Port Forwarding for a Web Server located on the LAN](#) published on the [Media5 Documentation Portal](#).

3.7 Network Firewall

3.7.1 Basic Network Firewall Concepts

3.7.1.1 Network Firewall

The Network firewall allows you to dynamically create and configure rules to filter incoming packets forwarded by the Mediatrix unit among its network interfaces, when the unit is used as a router. Its main functionality is to secure the traffic routed from and to the devices inside the local network.

Since this is a network firewall, rules only apply to incoming packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured. If no rule matches the incoming packet, the default policy is applied. A rule's priority is determined by its index in the table. Rules using Network Names are automatically updated as the associated IP addresses and network mask are modified. If the Network Firewall service is stopped, all forwarded traffic is accepted, this tab is greyed out and the parameters are not displayed.

Of course, the more rules are enabled, the more overall performance is affected. You can use a maximum of 20 rules.

3.7.1.2 Firewall Rule Order - Important

The order in which the incoming packets are tested against the rules is important if you want to make sure that they actually have a filtering effect on incoming packets.

Rules can be configured to accept or to decline packets. But, always put the most restrictive rules first as they are executed sequentially starting with the first one listed at the top of the table i.e. make sure that the order in which the rules are executed does not cause a rule to be systematically excluded.

For example:

- If the first rule excludes all packets coming from a specific net mask, providing a second rule for an IP address with that same net mask will have no effect.
- If the first rule indicates actions to be taken for a specific IP address with a given net mask, and the second rule indicates to exclude all IP addresses with that net mask, both rules will be applied and have a result on the incoming packets.

3.7.2 Basic Network Firewall Tasks

3.7.2.1 Configuring the Network Firewall

Steps

- 1) Go to **Network/Network Firewall**.
- 2) In the **Network Firewall Configuration** table, set the **Default Policy** to **Accept**.

Note: Setting the Default Policy to "Accept" means that all forwarded traffic is accepted. for more details on network firewalls, refer to the [DGW Configuration Guide - Configuring the Network Firewall](#) published on the [Media5 Documentation Portal](#).

- 3) Click **Save & Apply**.

Result

Network Firewall Configuration	
Default Policy:	Accept ▼

3.7.2.2 Disabling the Network Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Network Firewall**.
- 2) In the **Network Firewall Configuration** table, set the **Default Policy** to **Accept**.
- 3) In the **Network Firewall Rules** table, from the **Activation** column, select **Disable** for all the rules.
- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.

Result

All incoming packets will be accepted.

3.7.2.3 Configuring Black Listing Duration

Steps

- 1) Go to **Network/Network Firewall**.
- 2) In the **Network Firewall Configuration** table, set the **Blacklist Timeout**
- 3) Set the **Blacklist Rate Limit Timeout**.
- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

Blacklisting parameters will be updated. Remember that for blacklisting to be used, at least one rule must have blacklisting enabled.

If a rule with the **Black listing enable** box checked matches a packet and no **Rate Limit Value** was set, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration of the **Blacklist Timeout**.

If a rule with the **Black listing enable** box checked matches a packet and the **Rate Limit Value** has been reached, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration set for the **Blacklist Rate Limit Timeout**.

3.7.3 Firewall Port Opening Example

This generic example shows how to allow remote clients to communicate with the IP office located at the LAN side of the Mediatrix unit.

In this example:

- The default policy is **Drop**, meaning that any packet that does not match the network firewall rules configured in the **Network Firewall Configuration** table will be dropped.
- To use the network firewall, IPv4 Forwarding (under IP Routing" tab), must be enabled. Without the forwarding, the network firewall is irrelevant because no packet will get passed from Uplink to LAN.

Network Firewall

Configuration Modified:	Yes
-------------------------	-----

Network Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Network Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Connection State	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable					All	☐	Established or Related	Accept	10	60	^ v + -
2	Enable					UDP	☐	All	Accept	10	60	^ v + -
3	Enable	IP address 1	port 1	IP address 9	port 7	TCP	☐	New	Accept	10	60	^ v + -
4	Enable	Subnet 2	port 2	Subnet 10	port 8	TCP	☐	New	Accept	10	60	^ v + -
5	Enable	IP address 3	port 3	IP address 11		TCP	☐	New	Accept	10	60	^ v + -
6	Enable	Subnet 4	port 4	Subnet 12		TCP	☐	New	Accept	10	60	^ v + -
7	Enable	IP address 5	port 5			TCP	☐	All	Accept	10	60	^ v + -
8	Enable	Subnet 6	port 6			TCP	☐	All	Accept	10	60	^ v + -
9	Disable	IP address 7				UDP	☐	All	Accept	10	60	^ v + -
10	Enable	Subnet 8				All	☐	All	Accept	10	60	^ v + -
												+

Table 2:

Rule	
1	All packets matching an existing connexion are accepted.
2	All packets coming through UDP are accepted.
3	New packets coming from the IP address 1 and port 1 with a destination to IP address 9 and port 7 through TCP, will be allowed.
4	New packets coming from Subnet 2 and port 2 with a destination to Subnet 10 and port 8 through TCP, will be allowed.
5	New packets coming from the IP address 3 and port 3 with a destination to IP address 11 with any port through TCP, will be allowed.
6	New packets coming from the Subnet 4 and port 4 with a destination to Subnet 12 with any port through TCP, will be allowed.
7	Any packet coming from IP address 5 and port 5 to any destination and port through TCP, will be allowed.
8	Any packet coming from Subnet 6 and port 6 to any destination and port through TCP, will be allowed.
9	This rule will not be applied as it is disabled.
10	Any packet coming from Subnet 8 and any port to any destination and port through TCP, will be allowed.
Default	Packets are dropped.

3.8 NAT

3.8.1 Basic Concepts

3.8.1.1 Network Address Translation (NAT)

Network Address Translation (NAT, also known as network masquerading or IP masquerading) rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet.

The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. The Mediatrix unit's NAT service allows the dynamic creation and configuration of network address translation rules. Depending on some criteria, the packet matching the rule may see its source or destination address modified.

There are two types of NAT rules:

- Source rules: They are applied on the source address of outgoing packets.
- Destination rules: They are applied on the destination address of incoming packets.

A rule's priority is determined by its index in the Source NAT or Destination NAT tables (Network/NAT). If the NAT service is stopped, this tab is greyed out and the parameters are not displayed.

The maximum number of rules allowed in the configuration is 10 of each Source NAT and Destination NAT.

Note: Adding source or destination NAT rules has an impact on the Mediatrix unit's overall performance as the NAT requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 recommends to use a 30 ms packetization time when the NAT is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

Note: The Mediatrix unit NAT service does not support IPv6

3.8.1.2 Understanding Network Address Translation Rules

A NAT rule specifies a set of matching conditions for network packets.

Each rule can use one or more of the following criteria:

- Source Address
- Destination Address

- Protocol (All, TCP, UDP or ICMP).

If the protocol is set to TCP or UDP, the following criteria can also be used:

- Source Port
- Destination Port

When all the criteria of a rule match, the NAT will modify the packet to use the **New Address** field, either for the **Source Address** or the **Destination Address**, according to the type of NAT for which the rule is applied.

3.8.1.3 NAT Rule Order - Important

The NAT rules are applied on a first match basis, in the order they appear in the configuration.

Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired.

3.8.1.4 Destination or Source IP Address Format

IP Addresses can take the form of:

- An empty string, meaning that the rule will match any IP address
- An IP address, for example 192.168.0.11
- A network address, for example 192.168.1.0/24, which corresponds to all IP addresses in the range 192.168.1.0 to 192.168.1.255

It is also possible to use the name of a network interface to represent either the current IP address or network of that interface.

- Specifying the interface name without a trailing slash represents the IP address
- The same name with the trailing slash represents the network.

Note: This is case sensitive (the first letter must be uppercase)

For example, if your lan interface is configured as 192.168.0.10/24

- **Lan1** will be replaced by the current IP address of the lan interface, 192.168.0.10
- **Lan1/** will be replaced with the network of the lan interface, /24, meaning the range from 192.168.0.0 to 192.168.0.255.

If the specified interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

3.8.1.5 Source or Destination Port Format

Ports can take the form of either:

- An empty string, meaning that the rule will match any port
- Single port, for example for a web server: 80
- A range of ports, for example to forward RTP: 5004-5099

3.8.1.6 Interaction of NAT rules with the Firewall Service

When using the Network Firewall service, it is important to configure it with respect to the Destination NAT rules because:

- Source NAT (SNAT) rules are executed after the routing decision, before the packet leaves the unit.
- Destination NAT (DNAT) rules are executed before the routing decision, as the packet enters the unit.

An example of this would be port forwarding where the DNAT changes the routed address of a packet to a new IP address/port. The Network Firewall must also accept connection to this IP/port in order for the port forwarding to work.

3.8.2 Basic Tasks

3.8.2.1 Starting/Stopping/Restarting the NAT Service Using the DGW Web Page

Steps

- 1) Go to **System/Services**.
- 2) In the **User Service** table, on the line of the NAT service set the **Startup Type** selection list to **Auto**.
- 3) Then,
 - click  if you wish to start the service, or
 - click  to restart the service.
 - click  to stop the service.

Note: When stopping or restarting a service, some interruptions might occur, such as dropped calls, virtual machine shutdown or loss of network connectivity, depending on the affected services and/or its dependencies.

- 4) Click **Apply**.

Result

The status of the service (in the **Status** column) changes following the executed service command.

- If you clicked , the tab from which you can access the service from the Web pages are greyed out
- If you clicked , the tab from which you can access the service from the Web pages are no longer greyed out.

3.8.2.2 Creating a Source NAT Rule

Before you start

IPv4 forwarding must be enabled under **Network/IP Routing**.

Steps

- 1) Go to **Network/NAT**.
- 2) In the **Source Network Address Translation Rules**, click 

Note: To add a rule before an existing entry, locate the proper row in the table and click the  button of this row. To add a rule at the end of the existing rows, click the  button at the bottom right of the section.

Note: The yellow Yes in the Config Modified section at the top of the window indicates that the configuration has been modified but not applied (i.e., the Network Address Translation section of the Status page differs from the NAT page).

- 3) Complete the fields as required.
- 4) Click **Apply**.

Result

The applied enabled rules are displayed in the **Network/Status/Network Address Translation** section, which contains the active configuration in the NAT. The yellow Config Modified Yes flag is cleared.

3.8.2.3 Creating a Destination NAT Rule

Steps

- 1) Go to **Network/NAT**.

- 2) In the **Destination Network Address Translation Rules**, click **+**

Note: To add a rule before an existing entry, locate the proper row in the table and click the **+** button of this row. To add a rule at the end of the existing rows, click the **+** button at the bottom right of the section.

Note: The yellow Yes in the Config Modified section at the top of the window indicates that the configuration has been modified but not applied (i.e., the Network Address Translation section of the Status page differs from the NAT page).

- 3) Complete the fields as required.
- 4) Click **Apply**.

Result

The applied enabled rules are displayed in the **Network/Status/Network Address Translation** section, which contains the active configuration in the NAT. The yellow Config Modified Yes flag is cleared.

3.8.3 NAT Rule Examples

3.8.3.1 Creating a Source NAT Rule to Forward the Lan to the Uplink Network Interface

Steps

- 1) Go to **Network/NAT**.
- 2) In the **Source Network Address Translation Rules**, click **+**.
- 3) From the **Activation** selection list, click **Enable**.
- 4) In the **Source Address** field, enter **Lan1/**.
- 5) From the **Protocol** selection list, choose **All**.
- 6) In the **New Address** field, enter **Uplink**.
- 7) Click **Save & Apply**.

Result

Source Network Address Translation Rules							
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	New Address
1	Enable	Lan1/				All	Uplink

3.9 DHCP Server

3.9.1 Basic Concepts

3.9.1.1 DHCP Service

The DHCP service allows the Mediatrix unit to act as a DHCP server. The Mediatrix will be able to allocate a range of IP addresses to use on a network, reserve, and distribute the IP addresses and network configuration parameters for specific devices using the MAC address as unique identifier for each device.

3.9.1.2 DHCP Server

The Mediatrix unit contains an embedded DHCP server that allocates IP addresses and provides leases to the various subnets that are configured

These subnets could have PCs or other IP devices connected to the unit's LAN Ethernet connectors. These devices could be any combination of switches, PCs, IP phones, etc. If the DHCP service is stopped (which is the default configuration), the **DHCP Server** tab is greyed out and the parameters are not displayed.

IMPORTANT: There can only be one subnet per Network Interface.

3.9.1.3 Default vs Specific DHCP Server Configurations

You can use two types of configuration:

- Default configurations that apply to each subnet of all network interfaces of the Mediatrix unit
- Specific configurations that override the default configurations. You can define specific configurations for each subnet in your Mediatrix unit. For instance, you could define a lease time for all the subnets of the Mediatrix unit and use the specific configuration parameters to set a different value for one specific subnet.

The parameters available differ according to the subnet you have selected. The Default subnet has less parameters than the specific subnets available on the Mediatrix unit.

IMPORTANT: There can only be one subnet per Network Interface.

3.9.1.4 Available Configuration Sources

A parameter's configuration source can be toggled. Here are the possible configuration sources:

Static	Parameter is defined as a static parameter locally
Automatic	Parameter is obtained from the Uplink network via DHCP or IPCP (PPPoE)
HostConfiguration	Parameter is obtained from the HOC Service
HostInterface	Parameter is obtained from network interface matching the subnet

3.9.1.5 Parameters Configuration Sources

The following table lists the configuration parameters and their available configuration sources:

Parameter name	Configuration sources			
	Static	Automatic	HostConfiguration	HostInterface
Domain name	X		X	
Lease time	X			
Default router	X			X
List of DNS servers	X	X	X	
List of NTP servers	X	X	X	
List of NBNS servers	X			

3.9.1.6 Subnet Server

The DHCP server manages hosts' network configuration on a given subnet. Each subnet can be seen as having a distinct DHCP server managing it, which is called a subnet server.

To activate a subnet server for a given network interface, the name of that network interface and the name of the subnet must match, the subnet enable option must be enabled and the configuration of the subnet must be valid. Only one subnet can be defined per network interface.

The network interface can be a physical interface or a logical interface (ex: sub-interface using VLAN). The subnet server status is updated dynamically according to many parameters.

Note: The subnet configuration is invalid when the range of the start or end addresses is out of the network interface's CIDR range, or both parameters are incompatible.

3.9.1.7 Sending Configuration Parameters to a Client

When an address is leased to a host, several network configuration parameters are sent to that host at the same time according to the options found in the DHCP request. Parameters are set to default at subnet creation time. A parameter can be defined with a subnet specific configuration.

The subnet server will not send a parameter with an empty value. This means that if a client requests a domain name and the subnet server domain name parameter contains an empty field, the subnet server will not add the domain name option in the DHCP response.

3.9.1.8 Lease Assignment

In order to assign leases, the subnet server draws from an IP address pool (or subnet scope) defined by a start address and an end address. The subnet mask assigned to hosts is taken directly from the network interface. All hosts on the same subnet share the same configuration. The maximum number of supported hosts on a subnet is 254.

Specific IP addresses (static leases), designated by their MAC address, can be defined as reserved for specific hosts.

The subnet server will always assign leases within the IP address pool with an exception for static leases. When a static lease is defined for the host requesting an address, this lease will be assigned to the host if the IP address is within the subnet range even if the address is not within the IP address pool.

3.9.1.9 DHCP Server Configuration Options

- **Lease Time (Option 51):** The Mediatrix unit DHCP server offers a lease time to its subnets. You can use a default lease time for all subnets or define a lease time specific to one or more subnets.
- **Domain Name (Option 15):** The Mediatrix unit DHCP server offers a domain name to its subnets. You can use a default domain name for all subnets or define a domain name specific to one or more subnets.
- **Default Gateway (Option 3):** The Mediatrix unit DHCP server offers a default gateway (also called default router) to its subnets.

Note: The default gateway parameters are not available in the Default interface. You must access the specific subnets configuration to set its parameters.

- **DNS (Option 6):** The Mediatrix unit DHCP server offers up to four DNS addresses to its subnets. You can use the default DNS addresses for all subnets or define static DNS addresses specific to one or more subnets.
- **NTP (Option 42):** The Mediatrix unit DHCP server offers the addresses of up to four NTP (Network Time Protocol) servers to its subnets. You can use the default NTP addresses for all subnets or define static NTP IP addresses specific to one or more subnets.
- **NBNS (Option 44):** The NetBIOS Name Server (NBNS) protocol, also called Windows Internet Name Service (WINS) can be configured through this option. This is only needed if you need file sharing on old Windows 95/98/Me/NT PCs. The Mediatrix unit DHCP server offers up to four NBNS addresses to its subnets. You can use the default NBNS addresses for all subnets or define static NBNS addresses specific to one or more subnets.
- **Server Name (Option 66):** The Mediatrix unit DHCP server offers a server name to its subnets. You can use a default server name for all subnets or define a server name specific to one or more
- **Bootfile Name (Option 67):** The Mediatrix unit DHCP server offers a Bootfile name to its subnets. You can use a default Bootfile name for all subnets or define a Bootfile name specific to one or more.

3.9.2 Basic DHCP Tasks

3.9.2.1 Configuring the LAN1 DHCP Server Subnet

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Information

Although the parameters of these steps can be configured differently, the values suggested will work for almost every scenario.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) In the **Select Subnet** drop down menu located at the top of the page, select **Lan1**.
- 3) In the **DHCP Server Configuration** table, set the **DHCP Server Enable** to **Enable**.
- 4) In the **Start IP Address** and **End IP Address** fields, indicate the IP range to use
- 5) Set **Automatic Configuration Interface** to **Uplink**.
- 6) Complete the fields of the **Lease Time (Option 51)** section. Make sure to set the
 - **Subnet Specific** selection list to **Yes**

- 7) Complete the fields of the **Domain Name (Option 15)** section. Make sure to set the
 - **Enable Option** selection list to **Enable**
 - **Subnet Specific** selection list to **Yes**
 - **Configuration Source** selection list to **Static**
- 8) Complete the fields of the **Default Gateway (Option 3)** section. Make sure to set the
 - **Enable Option** selection list to **Enable**
 - **Configuration Source** selection list to **Host Interface**.
- 9) Complete the fields of the **DNS (Option 6)** section. Make sure to set the
 - **Enable Option** selection list to **Enable**
 - **Subnet Specific** selection list to **Yes**
 - **Configuration Source** selection list to **Static**
- 10) Complete the fields of the **NTP (Option 42)** section. Make sure to set the
 - **Enable Option** selection list to **Enable**
 - **Subnet Specific** selection list to **Yes**
 - **Configuration Source** selection list to **Static**
- 11) Complete the fields of the **NBNS (Option 44)** section. Make sure to set the
 - **Enable Option** selection list to **Enable**
 - **Subnet Specific** selection list to **Yes**
- 12) Do not enable Option 66 or 67.
- 13) Click **Apply**.

3.9.3 Advanced DHCP Tasks

3.9.3.1 Creating A VLAN DHCP Server Subnet

Before you start

If you are not using a secure connection, **Activate unsecure script transfers and execution through web browser** to be able to execute script via the Web browser. To enable a VLAN in the DHCP server, make sure the VLAN is configured in the Network/VLAN tab and has an IP address configured in Network/Interfaces.

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.

Note: the following step is crucial to make sure the subnet is available in the **Select Subnet** field under **Network/DHCP Server**.

- 2) In the **Execute Inline Script** field enter `Dhcp.AddSubnet Network=Vlan10`.
- 3) Click **Execute**.

Result

Execute Inline Script	
<code>Dhcp.AddSubnet Network=Vlan10</code>	(Clear Script)
Execute	

The Vlan10 subnet will be available for configuration from the **Select Subnet** field under **Network/DHCP Server**.

3.9.3.2 Adding a Static Lease Using the DGW Web Interface

Before you start

If you are not using a secure connection, **Activate unsecure script transfers and execution through web browser** to be able to execute script via the Web browser.

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) To add a Static Lease, in the **Execute Inline Script** field enter the `Dhcp.AddStatic Lease` with the Mac address of the device and its desired static IP address. For example, **`Dhcp.AddStaticLease MacAddress=0090f8000000 IpAddress=192.168.0.9`**.

Note: To delete a static lease, use the Delete operation on the `Dhcp.StaticLeases` table. For example: **`Dhcp.StaticLeases[MacAddress=0090f8000000].Delete=Delete`**

- 3) Click **Execute**.

Result

The Vlan10 subnet will be available for configuration from the **Select Subnet** field under **Network/DHCP Server**. Adding a static lease can also be done via the command-line interface via SSH. To list all static leases, execute the **`Dhcp.StaticLeases`** command (only available by SSH): **`Global>Dhcp.StaticLeases`**

3.9.3.3 Configuring the DHCP Server Subnet Lease Time (Option 51)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.

- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 51 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **Lease Time (Option 51)** section, from the **Subnet Specific** selection list, choose
 - **No** to use the default lease time
 - **Yes** to override the default lease time.
- 5) If you chose **Yes**, complete the **Lease Time** field.
- 6)
- 7) Click **Apply**.

3.9.3.4 Configuring the DHCP Server Domain Name Parameters (Option 15)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 15 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **Domain Name (Option 15)** section, from the **Enable Option** selection list, choose
 - **Disable** to use the default domain name
 - **Enable** to override the default domain name.
- 5) If you chose **Enable**, complete the fields as required.
- 6) Click **Apply**.

3.9.3.5 Configuring the DHCP Server Default Gateway (Option 3)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 3 configuration.

- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.

Note: The default gateway parameters are not available in the Default interface. You must access the specific subnets configuration to set the parameters.

- 4) Under the **Default Gateway (Option 3)** section, from the **Enable Option** selection list, choose
 - **Disable** to use the default router
 - **Enable** to override the default router.
- 5) If you chose **Enable**, complete the fields as required.
- 6) Click **Apply**.

3.9.3.6 Configuring the DHCP Server DNS Parameters (Option 6)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 6 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **DNS (Option 6)** section, from the **Enable Option** selection list, choose
 - **Disable** to use the default DNS address
 - **Enable** to override the default router.
- 5) If you chose **Enable**, complete the fields as required.
- 6) Click **Apply**.

3.9.3.7 Configuring the DHCP Server NTP Parameters (Option 42)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 42 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.

- 4) Under the **NTP (Option 42)** section, from the **Enable Option** selection list, choose
 - **Disable** to use the default NTP servers
 - **Enable** to override the NTP servers.
- 5) If you chose **Enable**, complete the fields as required.
- 6) Click **Apply**.

3.9.3.8 Configuring the DHCP Server NBNS (Option 44)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 51 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **NBNS (Option 44)** section, make sure the **Enable Option** is set to **Enable**
- 5) from the **Subnet Specific** selection list, choose
 - **No** to use the default configuration,
 - **Yes** to override the specific configuration as defined in the following parameters:
SpecificNbnsServers.StaticNbns1 , **SpecificNbnsServers.StaticNbns2** ,
SpecificNbnsServers.StaticNbns3 , and **SpecificNbnsServers.StaticNbns4**.
- 6) If you chose **Yes**, complete the fields as required.
- 7) Click **Apply**.

3.9.3.9 Configuring the DHCP Server Name Parameters (Option 66)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed. To use specific files, you must know their name, their path and your server must be accessible by the unit.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 66 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **Server Name (Option 66)** make sure the **Enable Option** is set to **Enable**,

- 5) From the **Subnet Specific** selection list, choose
 - **No** to use the default server name
 - **Yes** to override the default server name.
- 6) If you chose **Yes**, complete the fields as required.
- 7) Click **Apply**.

3.9.3.10 Configuring the DHCP Server Bootfile Parameters (Option 67)

Before you start

Make sure the DHCP service is started (**System/Services/User Service**) otherwise the **DHCP Server** tab will be greyed. To use specific files, you must know their name, their path and your server must be accessible by the unit.

Steps

- 1) Go to **Network/DHCP Server**.
- 2) From the **Select Subnet** selection list, choose the subnet requiring Option 67 configuration.
- 3) In the **DHCP Server Configuration** table, make sure the **DHCP Server Enable** selection list is set to **Enable**.
- 4) Under the **Bootfile Name (Option 67)** section, from the **Enable Option** selection list, choose **Enable** to override the default DHCP Server Bootfile Name.
- 5) From the **Subnet Specific** selection list, choose
 - **No** to use the default configuration.
 - **Yes** to override the default configuration.
- 6) If you chose **Yes**, complete the **Bootfile Name** field.
- 7) Click **Apply**.

4 SIP Proxy

4.1 Configuring the SipProxy Service

Steps

- 1) Go to **SIP Proxy/Configuration**.
- 2) In the **Monitoring** section of the **Configuration** table, in the **Interval** field, enter the interval at which monitoring requests are sent to verify the SIP server status, in seconds.
- 3) In the **Toggle Delay** field, enter the delay before reporting a status change of the monitored destination, in seconds.
- 4) In the **Destination** field, enter the server IP address or FQDN to monitor.

Note: In most cases, this will be the Registrar Host.

- 5) In the **Keep Alive Error Code** field, list the response codes (comma-seperated) that indicate that the server is down.

Note: To detect that the server is down, use the error codes the server will return when it is not available. This will be much faster than using the timeout.

- 6) In the **Outbound Proxy Host** field, if required by your SIP provider, enter the IP address or FQDN of their outbound proxy.

Note: This parameter was added in firmware version 45.3 for TCP and TLS transports only. UDP will be supported in a later release.

- 7) Click **Apply** to apply all changes to the configuration.
- 8) Located at the top of the page, click **restart required services**.

Result

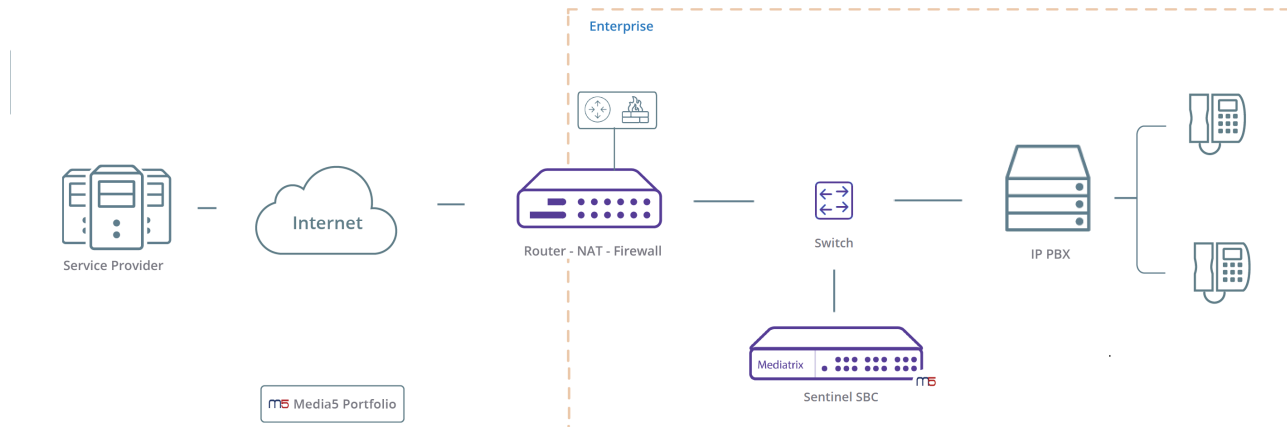
Configuration	
Survivability	
Survivability Mode:	Automatic ▼
Monitoring	
Interval:	30
Toggle Delay:	0
Destination:	
Keep Alive Error Codes:	
Network	
Network Interface:	Uplink ▼
Port:	0
Secure Port:	0
Registration	
Contact Override:	Enable ▼
Endpoint Survivability Expiration:	90
Registration Throttling	
Endpoint Throttling Expiration:	120
Relayed Throttling Expiration:	0
Outbound Proxy	
Outbound Proxy Host:	
Interop	
OPTIONS Method Support:	Default ▼
Request Transaction Timeout:	32

Apply

5 SBC

5.1 Sentinel on the LAN

The Sentinel 100 or 400 is designed to fit different network roles and topologies. It can be deployed inside a LAN behind a NAT firewall.

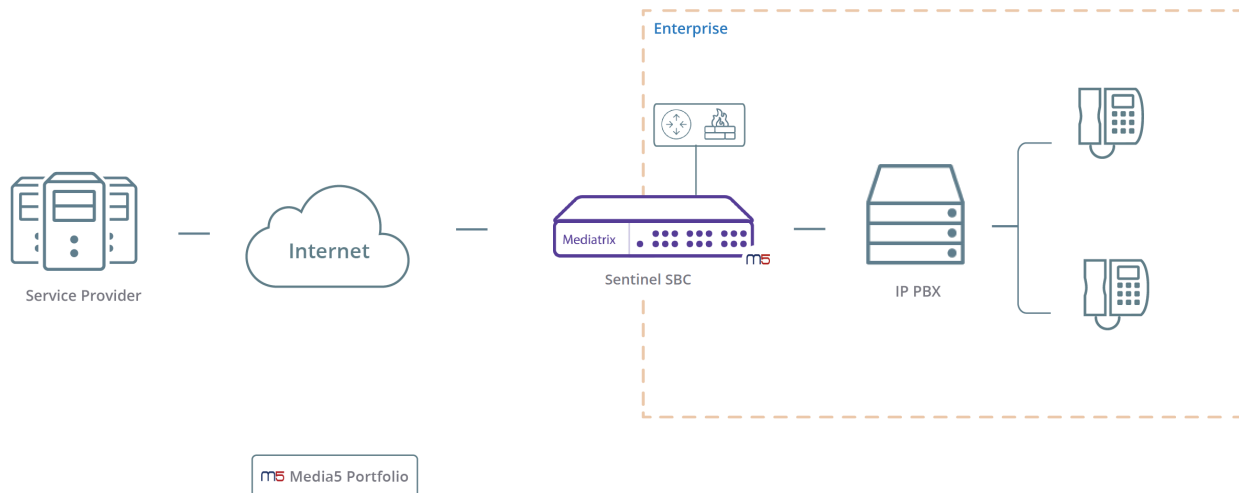


In this scenario, the Sentinel is usually configured as follows:

- Private (local) IP assigned to LAN port, Internal SIP clients (e.g. IP phones and IP PBX) also on the same LAN network.
- The Uplink Network interface is associated with the Wan/Eth1 physical link.
- The Lan1 Network interface is associated with the LAN/Eth2-5 physical link.
- The LAN signaling and media interfaces are not used.
- A signaling and media interface (pbx_s and pbx_m) will be created to avoid port conflicts when configuring the Call agents. They will be assigned associated to the LAN/Eth2-5 network interface
- Local firewall rules created to protect the SBC from outside attack (to complement the Edge NAT firewall router, optional). For more details refer to the [Configuring Local Firewalls](https://documentation.media5corp.com) Configuration guide published on the Media5 documentation portal at <https://documentation.media5corp.com>
- Port forwarding for SIP and RTP ports set up on the edge NAT firewall router
- SBC SIP near end NAT traversal is configured
- SBC rules to process VoIP calls

5.2 Sentinel on the Edge

The Sentinel 100 or 400 is designed to fit different network roles and topologies. It can be deployed on the network Edge, with a public IP address and firewall enabled.



The Sentinel located on the Edge is usually configured as follows:

- Public IP assigned to WAN/Eth1 port
- Uplink Network interface is associated with the WAN/Eth1
- Lan1 network interface is associated with the LAN/eth2-5
- Private (local) IP assigned to LAN port
- Local firewall rules created to protect the SBC from outside attack, for reference: <https://documentation.media5corp.com/display/DGWLATEST/Configuring+Local+Firewalls>
- NAT, IP forwarding and Network Firewall are enabled if Sentinel is used as a router (this is optional, the Sentinel by default does not forward any IP packets between the WAN and LAN) for local IP clients, for reference: <https://documentation.media5corp.com/display/DGWLATEST/Configuring+a+Mediatix+unit+as+a+NAT-Firewall+between+the+LAN+and+the+Internet> , <https://documentation.media5corp.com/display/DGWLATEST/Configuring+the+Network+Firewall>
- SBC rules to process VoIP calls

5.3 Configuration

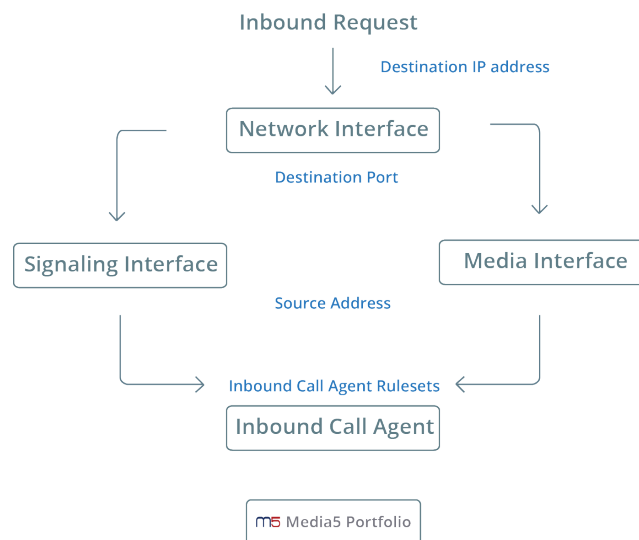
5.3.1 Basic SBC Configuration Concepts

5.3.1.1 Call Agents

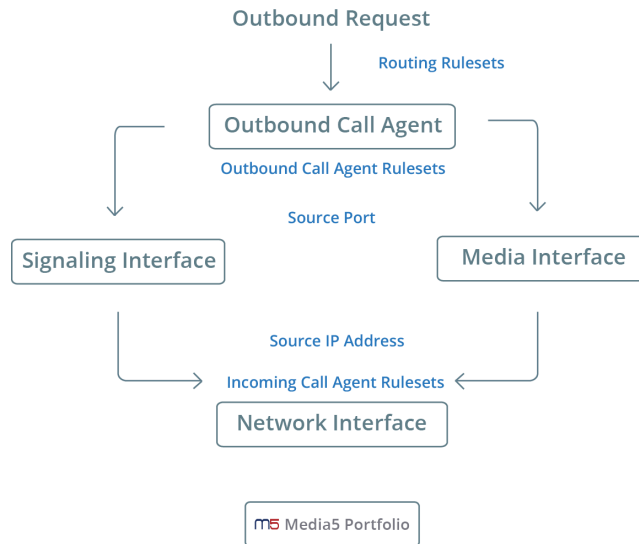
Call Agents represent logical end-points that connect the Mediatrix unit to peers.

For security reasons, the Mediatrix unit communicates by default only with well-known and defined peers. When a request cannot be associated with a Call Agent, it is rejected. Each Call Agent is tied to a specific peer, ensuring all inbound and outbound communications with that peer. Routing rulesets are used to route SIP signaling between Call Agents, where inbound requests from a Call Agent are sent to another (or the same) Call Agent that will send an outbound request to its related peer. Call Agents can be associated with one or several Rulesets which can be applied to the inbound or the outbound requests.

When there is an inbound request, to determine the Call Agent the inbound request will go through, the Mediatrix unit uses the destination IP address to choose the Network interface. Then the destination port of the inbound request will determine the Signaling or Media Interface used. Finally, the source address and the source port, will allow the Mediatrix unit to direct the request to the appropriate Call Agent. At this point any Rulesets associated with the Call Agent will be applied in order of priority.



When a request is sent out, i.e. there is an outbound request, the Routing Rulesets will determine which Call Agent will be used. Then the Call Agent Rulesets will be applied to the outbound request, in reverse priority order. The outbound request will then be sent through the Signaling and Media Interface associated with the Call Agent. If the public IP address is used, then the SIP request will use this address as the source IP address. The outbound request will then be sent to the peer address of the Call Agent or according to the routing Ruleset if the peer is a Network.

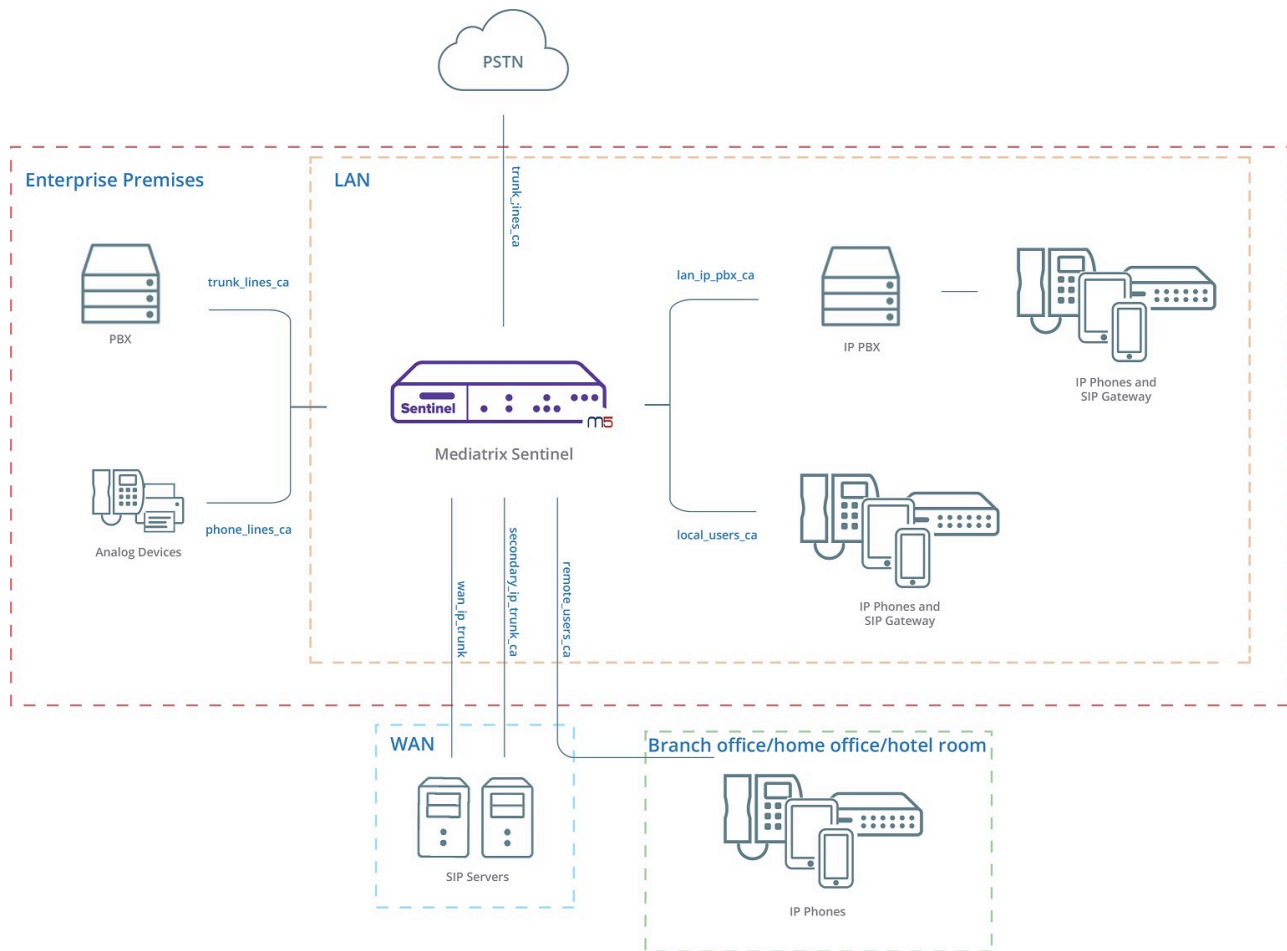


In addition, a Call Agent tracks REGISTER requests or monitor the peer host using SIP options. When these features are activated, the Call Agent registration state and monitoring state are updated allowing a Routing Ruleset to select another Call Agent based on the state of a primary Call Agent.

Eight default types of Call Agents were created for Mediatix unit. This should be enough to cover all your needs. However, for advanced users, it is possible to create new Call Agents.

Seven of the eight default Call Agents allow the Mediatix unit to communicate with seven different types of end-points.

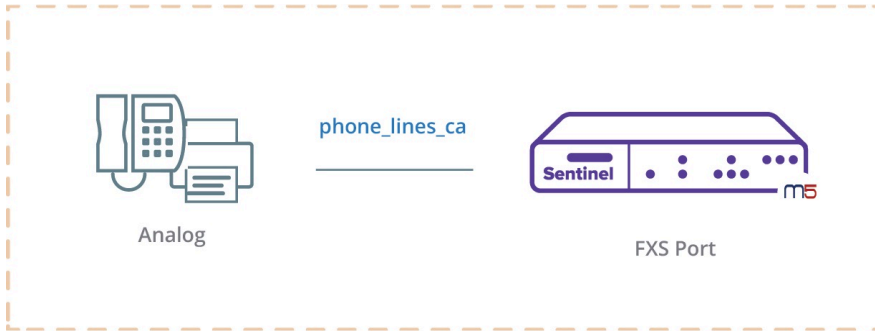
Call Agent Name	SIP or Endpoint Peer
wan_ip_trunk_ca	SIP server located on the WAN.
trunk_lines_ca	Public Switch Telephony Network (PSTN), through PRI, BRI or FXO ports.
phone_lines_ca	Telephones, through FXS ports.
lan_ip_pbx_ca	IP Private branch exchange (PBX) located on the LAN.
local_users_ca	Users via SIP telephony located on the LAN.
remote_users_ca	Users using SIP telephony located on the WAN.
registration_ca	Used to route the registrations issued by the Registration Agent.
secondary_ip_trunk_ca	SIP server if the wan_ip_trunk_ca Call Agent is not available.



5.3.1.2 phone_lines_ca Call Agent

The **phone_lines_ca** Call Agent is used to route calls via an FXS port of the Mediatrix unit.

Typically it will route calls to and from analog phones and faxes within the enterprise premises. This Call Agent will be used for example when a call is routed from one colleague to another using analog phones connected on the FXS ports of the Mediatrix unit. In such a scenario, the call does not go through the LAN network nor the Internet. Since by default this Call Agent uses the **loop_m** Media Interface to route the media, the **media_relay** Ruleset is usually associated with this Call Agent.



The **phone_lines_ca** Call Agent is associated with the **phone_lines_gw** gateway of the SipEp service. By default, each FXS port sends a REGISTER by the **phone_lines_ca** Call Agent. Therefore, the administrator must make sure to route these REGISTERS to a server, or to disable them in the SipEp service. If needed, FXS ports can be configured in the Pots service.

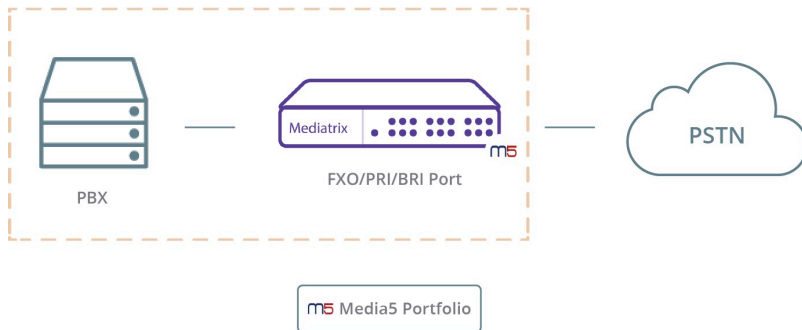


5.3.1.3 trunk_lines_ca Call Agent

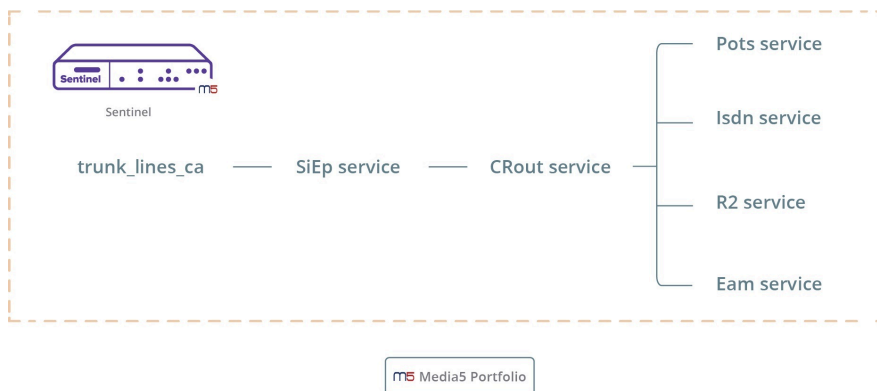
The **trunk_lines_ca** Call Agent is used to route calls to the Public Switch Telephony Network (PSTN) or a enterprise's existent PBX through the PRI, BRI or FXO ports of the unit.

Calls made outside the enterprise premises to telecommunication service providers or calls made within the enterprise through a PBX will typically be routed through this Call Agent. Since by default this Call Agent uses the **loop_m** Media Interface to route the media, the **media_relay** Ruleset is usually associated with this Call Agent.

If there are no PRI, BRI or FXO card on the unit, calls through trunk lines can also be routed by the **wan_ip_trunk_ca** or **secondary_ip_trunk_ca** Call Agent, provided there is an analog or digital gateway to convert the VoIP call to an analog or digital call, or vice versa.



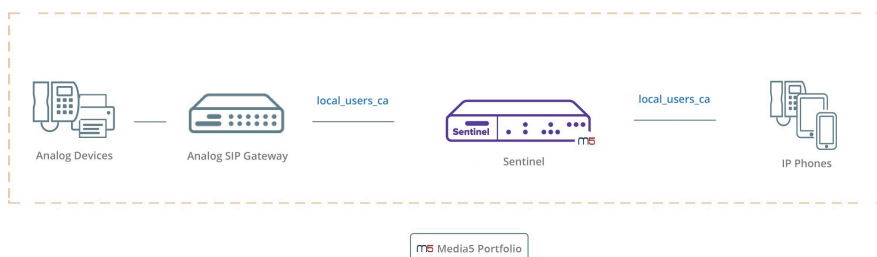
Further more, the **trunk_lines_ca** Call Agent is associated with the **trunk_lines_gw** of the SipEp service. FXO/PRI/BRI ports will need to be configured in either the Pots, Isdn, R2 or Eam services for the calls to be routed properly.



5.3.1.4 local_users_ca Call Agent

The **local_users_ca** Call Agent is used to route calls from and to local users, i.e. located in the LAN, via VoIP calls.

For the call to use this Call Agent, the endpoint must belong to the company and use the company's system. This Call Agent is often used as a regrouping point of all local endpoints to be routed to a PBX or Trunk lines. For instance, if you are a Media5 corporation employee, with a cell phone using the Media5 fone application and the enterprise IP-PBX, then your call will be routed through the **local_users_ca** Call Agent. If an internal employee is using an analog phone, the call can also be routed through this Call Agent provided the call goes first through a gateway to convert the analog call into a VoIP call.

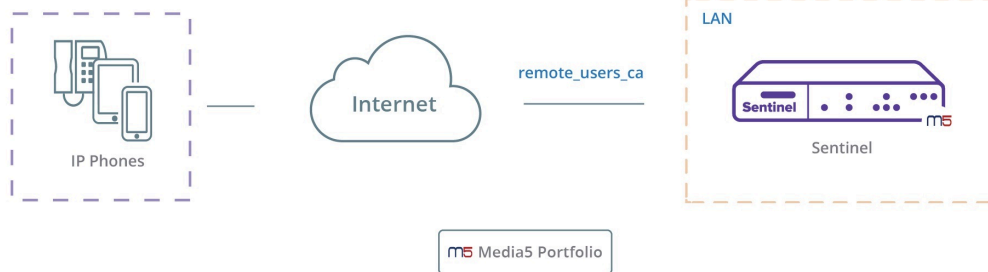


5.3.1.5 remote_users_ca Call Agent

The **remote_users_ca** Call Agent is used to route calls from users working out the office and using VoIP calls through an external network or Internet.

Calls are routed through a WAN then to the Mediatrix unit via the **remote_users_ca** Call Agent.

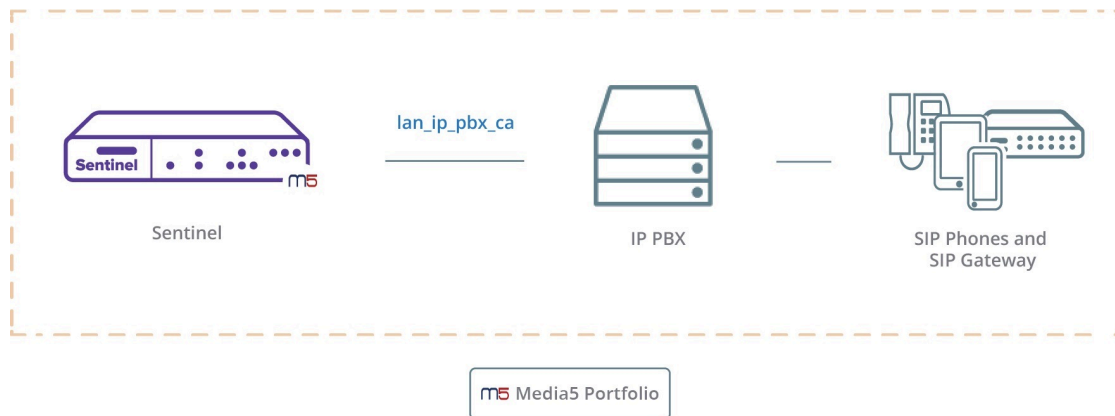
Branch Office/Home Office/Hotel room



5.3.1.6 lan_ip_pbx_ca Call Agent

The **lan_ip_pbx_ca** Call Agent routes calls to and from an IP PBX located in the LAN. The IP PBX manages all internal communications between different SIP clients (soft phones or SIP gateways).

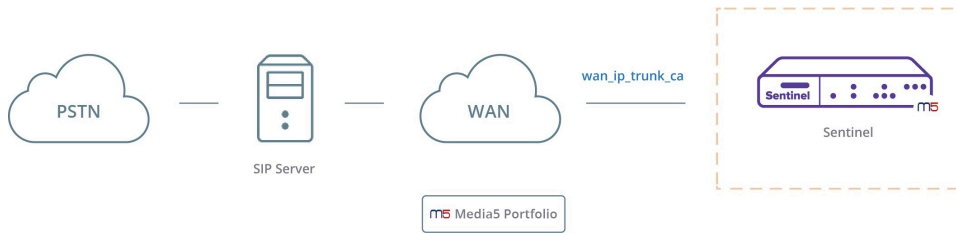
This Call Agent is usually used to link a local PBX with an external trunk (IP or PSTN).



5.3.1.7 wan_ip_trunk_ca Call Agent

The **wan_ip_trunk_ca** Call Agent is used to route VoIP calls.

Calls are routed from or to the main SIP server or provider located in the WAN. Typical peers for this Call Agent are the head office of the enterprise, an Internet telephony service provider (ITSP) or an IP Multimedia Core Network Subsystem (IMS).



5.3.1.8 secondary_ip_trunk_ca Call Agent

The **secondary_ip_trunk_ca** Call Agent is used to route VoIP calls.

This Call Agent is identical to the **wan_ip_trunk_ca** Call Agent. The **secondary_ip_trunk_ca** can be used for different purposes. The most common use for this Call Agent, is to route calls to and from the backup server in the event the primary server does not respond. However, this Call Agent can also be used, for example, to route calls directly to and from a Branch Office or route a specific type of call such as international calls. Typical peers for this Call Agent are the head office of the enterprise, an Internet telephony service provider (ITSP) or an IP Multimedia Core Network Subsystem (IMS).

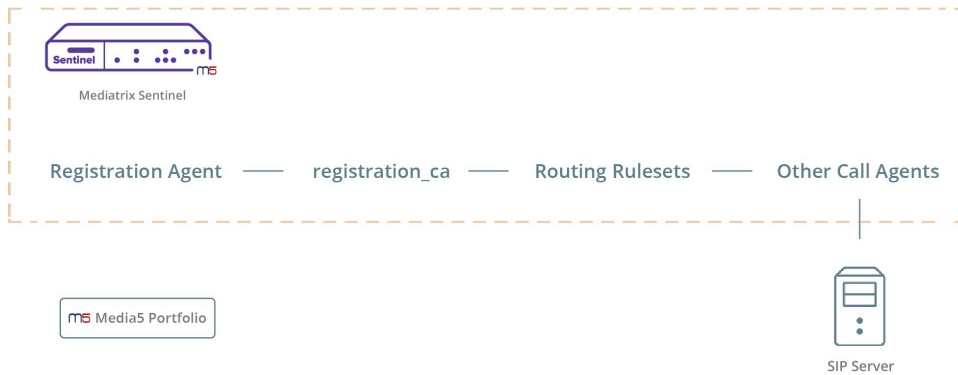


5.3.1.9 registration_ca Call Agent

The **registration_ca** Call Agent is used to route the registrations issued by the Registration Agent.

The **registration_ca** Call Agent should not be used for other purposes. The registrations issued by the Registration Agent must be routed from the **registration_ca** to the Call Agent facing the destination Sip registrar (typically **wan_ip_trunk_ca** or **secondary_ip_trunk_ca**).

The registration is routed using the User Name, Password and Domain to build the AOR and the R-URI. The Contact is the contact header of the registration, it should contain the IP-address or FQDN of the Mediatrix unit.



5.3.1.10 Signaling and Media Interfaces

The Signaling Interface is used for SIP signaling and the Media Interface is used for media (RTP, UDPTL) processing.

When configuring a Call Agent, you must select a Signaling Interface and a Media Interface. These interfaces are used whenever SIP signaling or media packets are sent to or received by the Call Agent.

It is possible to create several Signaling and Media Interfaces on the same Network Interface but for different purposes. For example, one set of Signaling and Media Interfaces for a WAN SIP Trunk and another set of Signaling and Media Interfaces for remote user calls. This means, for instance, that two Signaling Interfaces will be created on the same Network Interface, using the same IP address, but with a port range that will differ according to their intended use and to avoid conflicts.

A Media or Signaling Interface can be used by more than one Call Agent, but a specific Signaling or Media Interface can be created for a specific Call Agent. This provides the liberty to define non conflicting range of contactable interfaces on any physical network interfaces of the units for your network structure needs (such as Vlans, PPPoE interfaces, multiple Ethernet ports or multiple addresses on a link).

The following Signaling and Media Interfaces are supplied by default:

- **lan1_m**
- **lan1_s**
- **loop_m**
- **loop_s**
- **uplink_s**
- **uplink_m**

loop_m and **loop_s** interfaces are used to communicate with the internal services of the unit. For example, the loop interfaces can be used to communicate with the SipEp service to access phone ports.

5.3.1.11 Penalty Box

The penalty box feature is enabled for a specific Call Agent to temporarily avoid contacting the peer hosts (addresses) that are expected not to answer.

Without the use of the penalty box, DNS SRV failover is delayed until the SIP transaction times out. In a DNS SRV failover, without the use of the penalty box, the Call Agent will first try to communicate with the peer host on the first server, then once the SIP transaction has timed out, it will try the second and so on, always waiting for the SIP transaction timer to expire. With the penalty box, the call Agent will not try any servers that are already in the penalty box. Remember, dynamic call routing (e.g. survivability) based on server availability requires the penalty box to be enabled.

There are typically three situations that will cause a peer host to be put in the penalty box:

- If the transaction timer of a communication is expired, the peer host will be considered Down and will be put in the penalty box.
- If the transaction timer of a keep-alive communication is expired, the peer host will be considered Down and will be put in the penalty box.
- If after sending a keep-alive request or any other message to a peer host, the Call Agent receives one of the selected error codes, the peer host will be put in the penalty box. It is the error code that will indicate that the peer host cannot be used.

Note: When configuring the Call Agent it is possible to indicate the error codes that will trigger the peer host to be sent to the penalty box.(**SBC/Configuration/Blacklisting Error Codes**)

It is possible to configure how much time a peer host will remain in the penalty box, and the delay before which a peer host is considered down. This delay starts after the expiration of the transaction timer. It is also possible to disable the penalty box feature by using the special value 0 as the duration the peer host will remain in the penalty box.

5.3.1.12 Keep-Alive

The Keep-Alive monitoring parameter allows the unit to periodically send messages to a server to make sure the server can still be reached.

The Keep-Alive parameter is set individually for each Call Agent. SIP options are sent periodically for each Call Agent to their corresponding server. Any response received from the server means that it can be reached. No additional processing is performed on the response. If no response is received after the retransmission timer expires, the Sbc service considers the server as unreachable. In this case, any call attempt through the Call Agent is refused and the peer host will be sent to the Penalty Box. SIP options are still sent when the server cannot be reached and as soon as it can be reached again, new calls are allowed.

5.3.2 Basic SBC Configuration Tasks

5.3.2.1 Configuring a Call Agent

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click **Edit** located on the row of the Call Agent you wish to configure.
- 3) In the **Configure Call Agent** table, complete the fields as required and make sure the **Enable** check box is selected.

Note: **Monitoring Parameters** are not mandatory.

- 4) Complete the fields of the **Call Agent Configuration** as required.
- 5) Click **Save**.

Note: The changes are saved, but not all applied to the configuration.

- 6) Click **Apply** to apply all changes to the configuration.

Result

No will be displayed in the **Config.Modified** field, indicating that the configuration that was modified is now applied to the system. When the Mediatrix unit will use the selected Call Agent for a communication, the selected parameters will be applied.

5.3.2.2 Creating a Media Interface

Before you start

A Network Interface must be configured.

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Media Interface Configuration** table, click **+**.

Note: A new line of empty fields is added to the **Media Interface Configuration** table. An error message will be displayed indicating that the configuration of the row is invalid. This is normal as the Media Interface is not yet configured.

- 3) In the **Media Interface Configuration** table, complete the fields as required.

Note: The Network Interfaces displayed in the **Network** column, are created under **Network > Interfaces** tab.

- 4) Click **Save**.

Note: The changes are saved, but not all applied to the configuration.

- 5) Click **Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

The Media Interface will be available when configuring a Call Agent, in the **Media Interface** selection list of the **Configure Call Agent** page.

5.3.2.3 Creating a Signaling Interface

Before you start

A Network Interface must be configured. IPv6 is not supported, therefore Ipv6 configured Network interfaces cannot be used.

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Signaling Interface Configuration** table, click **+**.

Note: A line is added to the **Signaling Interface Configuration** table. An error message will be displayed indicating that the configuration of the row is invalid. This is normal as the Signaling Interface is not yet configured.

- 3) In the **Signaling Interface Configuration** table, complete the fields as required.

Note: The Network Interfaces displayed in the **Network** column, are created under **Network > Interfaces** page.

- 4) Click **Save**.

Note: The changes are saved, but not all applied to the configuration.

- 5) Click **Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

The Signaling Interface will be available when configuring a Call Agent, in the **Signaling Interface** selection list of the **Configure Call Agent** page.

5.3.2.4 Configuring the Call Agent Penalty Box

Steps

- 1) Go to **SBC/Configuration**.
- 2) Click **⚙** next to the Call Agent you wish to configure.

- 3) In the **Configure Call Agent** table, set the **Keep-Alive** field to 30.
- 4) Set the **Blacklisting Duration** to 60.
- 5) Click **Save**.

Result

Configure Call Agent		Value
Call Agent Parameters		
Name	Call_AgentName_ca	
Enable	☒	
Gateway	▼	
Signaling Interface	loop_s ▼	
Media Interface	loop_m ▼	
Peer Host	IP.address: port number	
Peer Network		
Force Transport	None ▼	
Monitoring Parameters		
Keep-Alive Interval	30	
Blacklisting Duration	60	
Blacklisting Delay		
Blacklisting Error Codes		

5.3.2.5 Setting the Keep-Alive Interval

Steps

- 1) Go to **SBC/Configuration**.
- 2) From the **Call Agent Configuration** table, click  next to the Call Agent you wish to configure.
- 3) In the **Keep-Alive Interval**, indicate the interval in seconds for sending SIP options to the Call Agent Peer host.

Note: 30 seconds is a good compromise between the speed at which errors are detected versus the resources used by the keep-alive signals.

Note: 0 indicates that the keep-alive feature is disabled.

- 4) Click **Save**.

5.4 Rulesets

5.4.1 Basic Ruleset Concepts

5.4.1.1 Rulesets

Rulesets define one or several rules used to filter, manipulate or route inbound or outbound requests.

There are two types of Rulesets:

- Call Agent Rulesets: they describe how inbound or outbound requests are handled by a specific Call Agent. They can also implement services or collect data.
- Routing Rulesets: they are used to globally route outbound requests, i.e. that they apply to all Call Agents.

When a request arrives at a Call Agent from a peer, the inbound rules of the Rulesets associated with the Call Agent are executed. Then, Routing Rulesets are executed until a Call Agent is selected for the destination. Last, the outbound rules of the Rulesets associated with the destination Call Agent are executed before sending the request to the peer.

Inbound rules of the Ruleset are executed in ascending Ruleset priority order. Outbound rules are executed in descending Ruleset priority order.

The Mediatrix unit is fundamentally rule driven. This means that almost all features can be activated based on certain conditions evaluated at run-time, based on parts of the signaling messages or media payload. All rules are constructed using the same pattern. They consist of a set of one or more conditions. If all conditions apply (logical conjunction), a set of one or more actions is executed. It is important to understand that rules are generally applied only on incoming or outbound requests. However, some rules have a scope that goes beyond these incoming or outbound requests. For example, header filters apply to all requests exchanged, including incoming requests.

Call Agents can have two origins:

- Factory: Read only Ruleset delivered with the application.
- Custom: User defined Ruleset.

A custom Ruleset has priority over a factory Ruleset. If a custom Ruleset is created with the same name as a factory Ruleset, it is the custom Ruleset that will be shown and used. Once the custom Ruleset is deleted, the factory Ruleset will be reactivated. Cloning, editing and saving a factory Ruleset will create a custom Ruleset without modifying the factory Ruleset.

Call Agent Rulesets have an *.crs extension and Routing Rulesets use the *.rrs extension. For more details on Ruleset conditions and descriptions, refer to the [DGW Configuration Guide - Reference Guide](#) document published on the [Media5 Documentation Portal](#).

Refer to the [DGE Configuration Guide - Ruleset Replacement Expressions](#) also published on the Media5 documentation portal.

IMPORTANT: Although it is possible to configure existing ruleset parameters via the CLI, it is not possible to create or edit a ruleset from the CLI: it must be either imported or directly created or edited in the DGW Web interface.

5.4.1.2 Ruleset Replacement Expressions

Ruleset replacement expressions are used when the value of a parameter, a command or an action is not known in advance, i.e. the value depends on the result of the SIP message processing.

A Ruleset replacement expression is a string that represents a SIP processing status. Replacement expressions always start with the dollar (“\$”) sign followed by an identifier. When the Ruleset uses a replacement expression, the replacement expression is replaced by the value of the SIP processing status representing the replacement expression.

For example,

- \$aU uses the User part of the **P-Asserted-Identity** header
- \$th uses the Host part of the **To** header
- sip:\$aU@\$th, used as the parameter of the Set R-URI action, uses the **P-Asserted-Identity** and **To** headers of the incoming request and puts them into the Request URI of the outgoing request.

Note: Special characters should be backslash-escaped, for example, as follows: \ # \\ or \$ # \\$

Note: It is important to know that if a mediation action (Section SIP Mediation) changes the content of a SIP message, the replacement expression will refer to the value after modification. E.g., if you apply the rule action “SetFrom(sip:new@from.com)”, \$fu will return new@from.com!

5.4.1.3 Ruleset Replacement Expression Exhaustive List

Macro	Replacements	Description
\$r	Request-URI (R-URI). The expression refers to current Request-URI which may be changed during the course of request processing	
	\$r.	Complete R-URI header
	\$ru	user@host[:port] part of R-URI
	\$rU	User part of the R-URI
	\$rd	R-URI domain (host:port)
	\$rh	Host part of the R-URI
	\$rp	Port number of the R-URI
	\$rP	R-URI Parameters
\$f	From header	
	\$f.	Complete From header field
	\$fu	user@host[:port] part of the From URI
	\$fU	User part of the From URI
	\$fd	From URI domain (host:port)
	\$fh	Host part of the From URI
	\$fp	Port number of the From URI
	\$fn	Display name of the From header field
	\$fP	Parameters of the From header field. Does not include the parameters of the URI.
	\$ft	The tag of the From header field
	\$fH	The name of the From header field, exactly as it is stated in the SIP request.
\$t	To header	
	\$t.	Complete To header
	\$tu	user@host[:port] part of the To URI
	\$tU	User part of the To URI
	\$td	To URI domain (host:port)
	\$th	Host part of the To URI
	\$tp	Port number of the To URI

Macro	Replacements	Description
	\$tn	Display name of the To header field
	\$tP	Parameters of the To header field. Does not include the parameters of the URI.
	\$tt	The tag of the To header
	\$tH	The name of the To header, exactly as it is stated in the SIP request.
\$a	P-Asserted-Identity (PAI)	
	\$a.	Complete PAI header.
	\$au	user@host[:port] part of the PAI URI
	\$aU	User part of the PAI URI
	\$ad	PAI URI Domain (host:port).
	\$ah	Host part of the PAI URI
	\$ap	Port number of the PAI URI
	\$aP	Parameters of the PAI header field. Does not include the parameters of the URI.
	\$at	The tag of the PAI
	\$aH	The name of the PAI header field, exactly as it is stated in the SIP request.
\$p	P-Preferred-Identity (PPI)	
	\$p.	Complete PPI header field.
	\$pu	user@host[:port] part of the PPI URI.
	\$pU	User part of the PPI URI.
	\$pd	PPI URI Domain (host:port).
	\$ph	Host part of the PPI URI.
	\$pp	Port number of the PPI URI.
	\$pP	Parameters of the PPI header field. Does not include the parameters of the URI.
	\$pt	The tag of the PPI header field.
	\$pH	The name of the PPI header, exactly as it is stated in the SIP request.
\$c	Call-ID	
	\$ci	Call-ID of the SIP request
\$s	Source party	

Macro	Replacements	Description
	\$si	Source IP address of the inbound SIP request
	\$sp	Source port number of the inbound SIP request
\$d	Expected destination party	
	\$di	Destination IP address of the outbound SIP request. This replacement expression is only available in outbound rules.
	\$dp	Destination port number of the outbound SIP request. This replacement expression is only available in outbound rules.
\$R	Interface of the inbound SIP request	
	\$Ri	IP address of the Signaling Interface on which the inbound SIP request was received
	\$Rp	Port number of the Signaling Interface on which the inbound SIP request was received
	\$Rf	ID of the Signaling Interface on which the inbound SIP request was received
	\$Rn	Name of the Signaling Interface on which the inbound SIP request was received
	\$RI	The configured address of the SignalingInterface.PublicIpAddr parameter on which the inbound SIP request was received
\$H	Arbitrary Headers. The replacement expressions in this group mention the name of an arbitrary header between parentheses. The core headers (From, To, Call-ID, Via, Route, Record-Route, Contact) cannot be replaced. Example: \$H(Server) will be replaced by the value of the Server header field.	
	\$H(headername)	Value of the 'headername' header
	\$HU(headername)	User part of the URI in the 'headername' header.
	\$Hd(headername)	URI Domain (host:port) of the 'headername' header.
	\$Hu(headername)	user@host[:port] part of the URI in the 'headername' header.
	\$Hh(headername)	Host part of the URI in the 'headername' header.
	\$Hp(headername)	Port number of the URI in the 'headername' header.

Macro	Replacements	Description
	\$Hn(headername)	Display name of the 'headername' header.
	\$HP(headername)	Parameters of the 'headername' header field. Does not include the parameters of the URI.
	\$HH(headername)	Header headername (as URI) headers
\$m	Request method	
	\$m	The method of the request.
\$V	Call parameter	
	\$V(gui.varname)	Value of the 'varname' call parameter.
\$B	Cnum and Rnum	
	\$B(cnum.rnum)	Value of the regular expression backreference. - Rnum is the index of the rule condition containing the regular expression, starting at 1. - Cnum is the index of the subexpression within the regular expression, starting at 1.
\$U	Register cache	
	\$Ua	Originating AoR from the registration cache. This replacement expression can only be used after the execution of a 'Restore contact from registrar' or a 'Retarget R-URI from cache' action.
	\$UA	Originating alias from the registration cache. This replacement expression can only be used after the execution of a 'Restore contact from registrar' or a 'Retarget R-URI from cache' action.
\$_	Operations on Values	
	\$_u(value)	Changes the value to uppercase.
	\$_l(value)	Changes the value to lowercase.
	\$_s(value)	Size of the value.
	\$_5(value)	MD5 sum of the value.
	\$_r(value)	Random number from 0 to 'value' - 1. Example: \$_r(5) gives 0, 1, 2, 3 or 4.
\$#	URL-encoded	

Macro	Replacements	Description
	\$#(value)	Encodes the value into a URL format with appropriate escaping for characters outside the ASCII character set.
\$attr	Global Attributes	
	\$attr(version)	Version number of the DGW firmware. The returned value matches with the %version% macro in DGW firmware.
	\$attr(profile)	Profile identification of the DGW firmware. The returned value matches with the %profile% macro in DGW firmware.
	\$attr(serial)	Serial number of the Mediatrix unit. The returned value matches with the %serial% macro in DGW firmware.
	\$attr(mac)	MAC address of the Mediatrix unit. The returned value matches with the %mac% macro in DGW firmware.
	\$attr(product)	Product name of the Mediatrix unit. The returned value matches with the %product% macro in DGW firmware.
	\$attr(productseries)	Product series name of the Mediatrix unit. The returned value matches with the %productseries% macro in DGW firmware.

5.4.2 Basic Ruleset Tasks

5.4.2.1 Creating a New Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets.

Note: To save time, consider [Cloning a Ruleset](#) (p.166).

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, enter a name in the empty field of either the **Call Agent Rulesets** or **Routing Rulesets** table.

- 3) Click .

Note: The name of the Ruleset will be added at the end of the table.

- 4) In the **Rulesets** page, click  located on the row of the Ruleset you have just created.
- 5) In the **Ruleset Edit** page, in either the **Outbound Rules** or **Inbound Rules**, click **Insert new rule**.
- 6) In the **Conditions** and **Actions** section, complete the fields as required.

Note: For more details on Actions and Conditions, refer to the [DGW Configuration Guide - Reference Guide](#) document published on the [Media5 Documentation Portal](#).

- 7) If necessary, click **Add condition** to add another condition.
- 8) If necessary, click **Add** to add another action.
- 9) Click **Save**.

Note: The new rule is saved but the modified configuration is not yet applied to the system.

Note: Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule](#) (p.171).

- 10) Go to **SBC / Configuration**.
- 11) Click **Apply**.

Note: The modified configuration is applied to the system.

Result

The new Ruleset is available to be associated with a Call Agent.

5.4.2.2 Cloning a Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, click  next to the Ruleset you wish to clone.
- 3) Click **OK**.

Note: The cloned Ruleset will be added at the end of the table. The name of the cloned Ruleset will include a numerical suffix to distinguish it from the original Ruleset.

- 4) In the **Rulesets** page, click  located on the row of the Ruleset you have just cloned.
- 5) Click **Edit** next to the rules you wish to modify.

- 6) In the **Conditions** and **Actions** section, modify the fields as required.

Note: For more details on Actions and Conditions, refer to the [Reference Guide](#) published on the Media5 documentation portal.

- 7) If necessary, click **Add condition** to add another condition.
- 8) If necessary, click **Add** to add another action.
- 9) Click **Save**.
- 10) Click **Change Name /description** to change the name and the description of the Ruleset.
- 11) Click **Save**.

Note: The new cloned rule is saved but the modified configuration is not yet applied to the system.

Note: Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule](#) (p.171).

- 12) Go to **SBC > Configuration**.
- 13) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

The new Ruleset is available to be associated with a Call Agent.

5.4.2.3 Modifying a Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset you wish to modify.
- 3) In the **Ruleset Edit** page, click **Edit** located on the row of the rule you wish to modify.
- 4) In the **Conditions** and **Actions** section, modify the fields as required.

Note: For more details on Actions and Conditions, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- 5) If necessary, click **Add condition** to add another condition.
- 6) If necessary, click **Add** to add another action.

- 7) Click **Save**.

Note: The modified rule is saved but the modified configuration is not yet applied to the system.

Note: Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule](#) (p.171).

- 8) Go to **SBC/Configuration**.
- 9) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

The Ruleset will be applied with the new changes.

5.4.2.4 Adding Rules to a Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset for which you wish to add a rule.
- 3) In the **Ruleset Edit** page,
 - click **Insert new rule** to add a rule at the top of the list of rules
 - click **Append new rule** to add a rule at the bottom of the list of rules.
- 4) In the **Conditions** and **Actions** sections, complete the fields as required.

Note: For more details on Actions and Conditions, refer to the [DGW Configuration Guide - Reference Guide](#) document published on the [Media5 Documentation Portal](#).

- 5) If necessary, click **Add condition** to add another condition.
- 6) If necessary, click **Add** to add another action.
- 7) Click **Save**.

Note: The new rule is added to the Ruleset and saved, but the modified configuration is not yet applied to the system.

- 8) Go to **SBC/Configuration**.
- 9) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

The rule will be executed the next time the Ruleset is used.

5.4.2.5 Changing the Name and Description of a Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets.

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset you wish to modify.
- 3) In the **Ruleset Edit** page, click **Change Name /description** located next to the name of the Ruleset.
- 4) In the **Ruleset Change Name/Description** page, modify the fields as required.
- 5) Click **Save**.

Note: The new name is saved but the modified configuration is not yet applied to the system.

- 6) Go to **SBC > Configuration**.
- 7) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

If you change the name of the Ruleset, you will need to re-associate the Ruleset to the Call Agent it is associated with otherwise, the configuration will be considered invalid.

5.4.2.6 Deleting a Ruleset

Information

This procedure applies to Call Agent and Routing Rulesets.

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Rulesets** page, click  next to the Ruleset you wish to delete.
- 3) Click **OK**.
- 4) Go to **SBCConfiguration**.
- 5) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

The Ruleset will no longer be available in the **Rulesets** page to be associated with a Ruleset. If the Ruleset was associated with a Call Agent, it will need to be removed manually from the list of Rulesets associated with the Call Agent otherwise, the configuration will be considered invalid.

5.4.2.7 Changing the Execution Priority Level of a Call Agent Ruleset

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click  next to the Call Agent for which you wish to modify the Ruleset priority level.
- 3) Use the arrows of the **Call Agent Rulesets** table to move a Ruleset up or down.
- 4) Click **Save**.
The changes will be applied to the configuration, but the modified configuration is not yet applied to the system.
- 5) Click **Apply** to apply the modified configuration to the system.

Result

Inbound rules of the Ruleset will be executed in ascending Ruleset priority order but Outbound rules will be executed in descending Ruleset priority order.

5.4.2.8 Changing the Execution Priority Level of a Routing Ruleset

Steps

- 1) Go to **SBC/Configuration**.
- 2) Use the arrows of the **Routing Rulesets** table to move a Ruleset up or down.
- 3) Click **Save**.

Note: The changes will be applied to the configuration, but the modified configuration is not yet applied to the system.

- 4) Click **Apply** to apply the modified configuration to the system.

Result

Inbound rules of the Ruleset will be executed in ascending Ruleset priority order but Outbound rules will be executed in descending Ruleset priority order.

5.4.2.9 Changing the Execution Priority Level of a Ruleset Rule

Information

This procedure applies to Call Agent and Routing Rulesets.

Steps

- 1) Go to **SBC/Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rules.
- 3) Use the **Up** and **Down** buttons to move the rules.
- 4) Go to **SBCConfiguration**.
- 5) Click **Apply**.

Note: The changes are saved to the configuration and the modified configuration is now applied to the system.

Result

Inbound rules of the Ruleset are executed in ascending Ruleset priority order but Outbound rules are executed in descending Ruleset priority order.

5.4.2.10 Changing the Execution Priority Level of a Rule Action

Information

This procedure applies to Call Agent and Routing Rulesets

Steps

- 1) Go to **SBC/Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rule actions.
- 3) Click **Edit** next to the rule for which you wish to change the actions order.
- 4) Click  or  to move actions.
- 5) Click **Save**.

Note: The new priority level is saved but the modified configuration is not yet applied to the system.

- 6) Go to **SBC/Configuration**.
- 7) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

When the Ruleset is used, the actions of a rule are always executed in the ascending priority order.

5.4.2.11 Changing the Execution Priority Level of a Rule Condition

Information

This procedure applies to Call Agent and Routing Rulesets

Steps

- 1) Go to **SBC/Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rule conditions.
- 3) Click **Edit** next to the rule for which you wish to change the conditions order.
- 4) Click **↓** or **↑** to move conditions.
- 5) Click **Save**.

Note: The new priority level is saved but the modified configuration is not yet applied to the system.

- 6) Go to **SBC/Configuration**.
- 7) Click **Apply**.

Note: The modified configuration is now applied to the system.

Result

When the Ruleset is used, the conditions of the rule are always executed in the ascending priority order.

5.4.2.12 Importing Rulesets

Before you start

Rulesets must be imported. The latest Ruleset package can be found on the <https://media5.secure.force.com/supportportal> (you will be required to supply a user name and password).

Information

This procedure is valid for Call Agent and Routing Rulesets.

Steps

- 1) Go to **Management/File**.

Note: Required Rulesets depend on the scenario being configured. Refer to the Call Agent and Routing Ruleset sections of the configuration notes for details on Rulesets needed to complete the configuration.

Note: Step 2 is only required when importing the first Ruleset and if you are not using a secure connexion to access the Management Interface (http://).

- 2) Click **Activate unsecure file importation from the Web browser**.
- 3) From the **Path** field, select sbc/rulesets/.
- 4) Click **Browse**, and navigate to the Ruleset you wish to import.

Note: Ruleset file extension must be *.crs for Call Agent Rulesets or *.rrs for Routing Rulesets.

- 5) Click **Import**.

Result

The imported Ruleset will appear in the **Internal files** table, with the selected path in front of the name. The Ruleset will be available in the tables of the **SBC/Rulesets** page.

Import File Through Web Browser	
Path	File
sbc/rulesets/	C:\Rulesets\your_ruleset

Browse ... Import

5.4.2.13 Associating Call Agent Rulesets to a Call Agent

Before you start

- The Call Agents must be configured.

- [Importing Rulesets](#) (p.173) must be completed.

Steps

- 1) Go to **SBC/Configuration**.

Note: Refer to the Call Agents section to identify which Rulesets are associated with the Call Agents used in this Use Case.

- 2) From the **Call Agent Configuration** table, click  located on the same row as the Call Agent to which you wish to associate a Ruleset.
- 3) In the **Call Agent Rulesets** table, click .
- 4) From the **Name** selection list, select a Ruleset.
- 5) To add other Rulesets, click .
- 6) Click **Save**.
- 7) In the **Configure Call Agent** page, click **Save**.
- 8) Click **Apply** to apply all changes to the configuration.

Result

Call Agent Rulesets			
Priority	Name	Parameters	
1	call_agent_ruleset_1		  
2	call_agent_ruleset_2		  
			

5.4.2.14 Associating Routing Rulesets to Your Configuration

Before you start

[Importing Rulesets](#) (p.173) must be completed for Routing Rulesets to be available.

Steps

- 1) Go to **SBC/Configuration**
- 2) In the **Routing Rulesets** table click  to add the first route.
- 3) From the **Name** selection list, select the Routing Ruleset you wish to apply to the configuration.

Note: Refer to the Routing Rulesets section to identify the Rulesets that apply to this Use Case.

- 4) Repeat steps 2 and 3 for each Routing Ruleset you wish to associate to your configuration.
- 5) If necessary, in the **Parameters** field enter the required parameters for each route.
- 6) Click **Save**.
- 7) Click **Apply** to apply all changes to the configuration.

Result

Routing Rulesets				
Priority	Name	Parameters		
1	routing_ruleset_1		^	↓
2	routing_ruleset_2		^	↓
			+	

5.5 Registration

5.5.1 Basic SBC Registration Concepts

5.5.1.1 Registration Agent

The Registration Agent is a feature that performs REGISTERS on behalf of other users.

In some use cases, using the Registration Agent may be necessary to have a separate entity perform the REGISTERS on behalf of users. For example:

- When users cannot register themselves.
- To separate internal and external networks in Demarcation Point scenarios

The Registration Agent is only involved with the registrations it initiates. If the Registration Agent is used, its REGISTERS are routed to the Mediatrix unit via the registration_ca Call Agent.

5.5.1.2 Registration Caching

Registration processing allows maintaining an endpoint reachable even from behind NATs.

When a call is routed by a Ruleset that includes the REGISTER throttling and Enable REGISTER caching actions, the SBC replaces the information of the Contact header with its own IP address before forwarding the call to an endpoint. Because a private IP address is used as the contact address in the Contact header field of the REGISTER messages, it becomes impossible to reach the user from the public Internet without going through the SBC since the contact's address is private.

The manipulated registration information is then registered in the registrar. When a Call is destined to the user, the call will be directed to the SBC. In order for the SBC to know which user is actually being contacted, the SBC keeps a local copy of the user's registration. The local copy includes the private IP address and the user's SIP URI as well as the public IP address included in the IP header that was assigned to the SIP message by the NAT.

If periodic request-response traffic does not cross the NAT behind which the user is located, the NAT address binding expires and the user becomes unreachable. Therefore, the SBC forces re-registration to keep NAT bindings alive.

5.5.1.3 Registration Throttling

Registration throttling protects SIP infrastructures against registration overloads.

Although registration overloads are often self-inflicted by the keep-alive functionality, it may also be caused by a router outage, broken client or Denial of Service attack. The SBC fends off such overloads by using high-performance in-memory registration cache that serves upstream registrations at high-rate, handles them locally, and propagates them down-stream at substantially reduced rate. That's the case if the registrations were to create new bindings, deleting existing ones or if they were to expire downstream. The propagated registration changes become effective on the SBC only if confirmed by the downstream server. If a registration expires without being refreshed the SBC issues a warning event.

5.5.1.4 Registration Cache Clearing

Clearing the registration cache will remove all inaccurate information that could remain if an equipment connecting to the SBC is restarted with new information such as a new IP address.

When the registration cache is cleared, all equipments connecting to the SBC need to re-register themselves before being able to receive SIP requests because without re-registration the SBC will not have the private contact address to know where to route the SIP.

5.5.2 Basic SBC Registration Tasks

5.5.2.1 Configuring a Registration Agent

Configure the registration agent used to issue the registrations.

Steps

- 1) Go to **SBC/Registration**.
- 2) In the **Registration Agent Configuration** table, click **+**.

Note: A new line of fields is added.

- 3) Complete the **User Name**, **Friendly Name**, and **Domain parameters** fields according to the service provider's requirements.
- 4) In the **Contact** field, enter credentials to register against the service provider.

Note: Format must be sip:user@public_IP Address or sip:public_IP Address or sips:user@public_IP_Address:sip listening port;uri-parameters of the unit.

- 5) If necessary, repeat [step 2](#) to [step 4](#) if you are using more than one service provider.
- 6) Click **Apply**.

Result

Registration Agent Configuration				
User Name	Friendly Name	Domain	Contact	Registration Type
USERNAME		IP.FQDN.of.registrar	sip:myCONTACT@%capubip(wa	Normal ▼

5.5.2.2 Finding a Specific AoR in the Registration Cache

Steps

- 1) Go to **SBC/Registration**
- 2) In the **Filter** table, enter the AoR.
- 3) Click **Search**.

Result

The **Registration Cache** table only displays the registration(s) related to the selected AoR.

5.5.2.3 Clearing the Registration Cache

Steps

- 1) Go to **SBC/Registration**.
- 2) Click **Clear Registration Cache** located under the **Registration Cache** table.

Result

All entries of the **Registration Cache** table will be erased and Registration Throttling will restart from scratch. The next REGISTERS will be immediately relayed to their destinations on their first occurrence.

5.6 SBC Advanced Parameters

5.6.1 SBC/Configuration Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters ,refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Tcp Connect Timeout

Refer to **Sbc.SignalingInterface.TcpConnectTimeout** .

Tcp Idle Timeout

Refer to **Sbc.SignalingInterface.TcpIdleTimeout**.

Registration Expiration

Refer to **Sbc.RegistrationAgent.ExpireValue**.

Registration Expiration

Refer to **Sbc.RegistrationAgent.RetryInterval**.

Min Severity

Refer to **Sbc.MinSeverity**.

5.6.2 SBC/Status Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by:

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

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) document published on the [Media5 Documentation Portal](#).

Tcp Connect Timeout

Refer to **Sbc.SignalingInterfaceStatus.TcpConnectTimeout**.

Tcp Idle Timeout

Refer to **Sbc.SignalingInterfaceStatus.TcpIdleTimeout**

Need Restart Info

Refer to **Sbc.NeedRestartInfo**.

6 POTS

6.1 Basic Concepts

6.1.1 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 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.

In call waiting, the caller ID service supplies information about a second incoming caller to a subscriber already busy with a phone call. However, caller ID on call waiting is not supported by all caller ID-capable telephone displays.

The following basic caller ID features are supported:

- Date and Time
- Calling Line Identity
- Calling Party Name
- Visual Indicator (MWI)

6.1.2 Caller ID Generation

Caller ID information is sent depending on the application and country-specific requirements: Caller ID generation using DTMF signalling and Caller ID generation using Frequency Shift Keying (FSK)

Note: The DGW Application does not support ASCII special characters higher than 127.

Caller ID generation can be done by:

- DTMF signalling performed during or before ringing, depending on the country settings or endpoint configuration. The Mediatrix unit provides the calling line identity according to the following standards:
 - Europe: ETSI 300 659-1 January 2001 (Annex B):
 - Access and Terminals (AT)
 - Analogue access to the Public Switched Telephone Network (PSTN)
 - Subscriber line protocol over the local loop for display (and related) services
 - Part 1: On-hook data transmission
 - Country-specific custom DTMF variations:
 - Telebras DTMF (Brasil and Argentina)
 - TDK DTMF (Denmark)
- Frequency Shift Keying (FSK). Different countries use different standards to send caller ID information. The Mediatrix unit is compatible with the following widely used standards:
 - ETSI 300 659-1
- Continuous phase binary FSK modulation is used for coding that is compatible with:
 - BELL 202
 - ITU-T V.23

Note: The displayed caller ID for all countries may be up to 20 digits for numbers and 50 digits for names. The DGW application does not support ASCII special characters higher than 127.

6.1.3 Caller ID Transmission

For most countries, the caller ID is transmitted after the first ring.

One notable exception is the UK, where Caller ID is sent after the dual tone alerting state tone on an inverted polarity line.

Other modes of transmission can be configured with the **Caller ID Transmission** parameter (under **POTS/Config/General Configuration**).

6.1.4 Flash Hook

Flash hook can be described as quickly depressing and releasing the plunger or the actual handset-cradle to create a signal indicating a change in the current telephone session.

The flash hook is used to trigger:

- call waiting
- second call

- call on hold
- conferences

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.

Note: As a best practice, the Flash button should be used to avoid terminating the call by accidentally pushing the plunger for too long.

6.1.5 Country Override Flash Hook Detection Range

This is the range in which the hook switch must remain pressed to perform a flash hook.

When selecting a country (under **Telephony/Misc/Country Selection**), each country has a default minimum and maximum time value within which pressing and releasing the plunger is actually considered a flash hook. However, these values can be overridden and customised with the **Country Override Flash Hook Detection Range** (under **POTS/FXS Configuration/Country Customisation**).

The range consists of :

- The minimal delay and maximal delay, in ms, separated by a "-".
- The minimal value allowed is 10 ms.
- The maximum value allowed is 1200 ms.
- The space character is not allowed.

6.1.6 FXO Force End-of-Call

The forced end-of-call service regroups all features permitting the unit to terminate a call. This can be required in a telephony network where the FXO loop current drops are not always detected.

The call termination can be triggered in three cases:

- On call failure: This feature is set by setting the **Force End of Call On Call Failure** parameter to **Enable**. When a call failure happens, the call is terminated after the timeout configured with the **Call Failure Timeout (sec)** parameter has elapsed and an error tone is played.
- On silence detection: A call is ended when silence is detected for a delay higher than the value configured by in the **Silence Detection Timeout (sec)** parameter (Refer to the [FXO Silence Detection](#) (p.182)). The mode is set with the **Force End Of Call On Silence Detection Mode** parameter.
- On tone detection: A call is ended when a selected tone is detected. The tone for this purpose depends on the detection mode specified by the **Force End Of Call On Tone Detection Mode** parameter which can be country specific (not available in all countries) or a custom tone. (Refer to [FXO Tone Detection](#) (p.182)).

All previously mentioned parameters are available under **POTS/FXO Configuration/ FXO Force End of Call**.

6.1.7 FXO Silence Detection

Silence detection allows the Mediatrix unit to close a line when no voice activity or silence is detected for a specified amount of time.

When silence is detected on the inbound and/or outbound media for an amount of time specified in the **Force End Of Call On Silence Detection Mode** parameter (under **POTS/FXO Configuration/FXO Force End of Call**), the call is terminated. This feature is useful to free resources in the event of an IP network failure that prevents the end of a call to be detected or when the end of call tone was not detected.

Note: The silence detection feature could inadvertently disconnect a communication when one party puts the other on hold more than 5 minutes (default value timeout). Using the hold tone feature prevents the detection of silence when the call is put on hold by the IP peer. Refer to the [DGW Configuration Guide - Tone Customisation](#) document published on the [Media5 Documentation Portal](#).

The current implementation of silence detection relies on the power of the media signal. A silence is detected if the power level of the media signal is lower than -60 dBm. This feature forcefully terminates a call that stayed silent for some time.

6.1.8 FXO Tone Detection

The FXO Tone Detection feature is used to resolve scenarios in which the far-end disconnection tone cannot be detected.

For a custom tone, the following parameters can be configured:

- **Tone Detection Custom Frequency**
- **Tone Detection Custom Cadence**
- **Detection Custom Repetition**

which are all located under **POTS/FXO Configuration/FXO Force End of Call**.

If a custom tone is defined, the ring pattern can have up to four on/off pairs in the format of on1,off1,on2,off2,on3,off3,on4,off4 where:

- on is a numerical value representing the time, in milliseconds, during which the tone can be detected
- off is a numerical value representing the time, in milliseconds, during which the tone cannot be detected
- the on and off values can range from 0 to 32,767 ms.
- Specifying more than 4 pairs will only use the first 4 pairs (eight first values).
- If less than 4 pairs are specified, 0 values will be added as necessary.

- The first zero (0) found in the string signals the end of the cadence (i.e. "200, 0, 300, 400" is the same as "200").
- If it starts with a value of zero (0) , the ring pattern is invalid.

In some cases, the detection of a tone with a complex cadence containing multiple frequencies is required, such as for the special information tone (SIT). However, since the detection of only one custom frequency can be configured in DGW, the custom frequency used to detect the complex cadence will need to be one of the frequencies found in the tone.

6.1.9 FXS Country Override Loop Current

When a remote end-user goes on-hook, the Mediatix unit signals the far end disconnect by performing a current loop drop (< 1 mA) on the analog line.

This current loop drop is typically used for disconnect supervision on analog lines. If the **Line Supervision Mode** parameter (under **POTS/FXS Configuration**) is set to **DropOnDisconnect** then the Mediatix unit signals the far end disconnect by performing a current loop drop on the analog line. By default, the Mediatix unit maintains a current drop for 1000 ms,, then a busy tone is generated to indicate the user to hang up. The current loop drop duration can be configured with the **Power Drop on Disconnect Duration** parameter (under **POTS/FXS Configuration**). (For more details, refer to the **FXS Line Supervision Mode** parameter in the [DGW Configuration Guide - Reference guide](#) published on the [Media5 Documentation Portal](#)).

When an FXS analog line goes off hook, it causes current to flow by closing the loop. The **Country Selection** parameter (**Telephony/Misc/Country**) allows the selection of predefined country settings for the tone profiles, ring patterns, and other parameters such as input and output gains. The value of the loop current for each country is by default 30 mA but can be overridden to a value ranging from 20 mA to 32 mA with the **Country Override Loop Current** parameter (under **POTS/FXS Configuration/Country Customisation**) provided the **Override Country Configuration** parameter is enabled (under **POTS/FXS Configuration/Country Customisation**).

Note: The actual measured current may be different from the one set, as it varies depending on the DC impedance. The default value is 30 mA. When a value higher than 32 mA is used, the unit will limit the current to 32 mA.

6.2 Basic FXS Tasks

6.2.1 Selecting the Detection/Generation Method of the Caller ID

Steps

- 1) Go to **POTS/Config**.
- 2) In the **General Configuration** table, complete the fields are required.

- 3) Click **Apply**.

6.2.2 Configuring FXS Parameters

Steps

- 1) Go to **POTS/FXS Configuration**.
- 2) In the **FXS Configuration** table, complete the fields as required.
- 3) Click **Apply**.

Result

FXS Configuration		
Line Supervision Mode:	DropOnDisconnect	
Disconnect Delay:	0	
Auto Cancel Timeout:	0	
Inband Ringback:	Disable	
Shutdown Behavior:	Disabled Tone	
Power Drop On Disconnect Duration:	1000	
Service Activation:	Flash Hook	
SIP Message Alerting:	Disable	

6.2.3 Overriding FXS Default Country Parameters

Steps

- 1) Go to **POTS/FXS Configuration**.
- 2) In the **Country Customisation** table, complete the fields as required.
- 3) Click **Apply**.

Result

Country Customisation		
Override Country Configuration:	Enable	
Country Override Loop Current:	30	
Country Override Flash Hook Detection Range:	100-1200	

6.3 Basic FXO Tasks

6.3.1 Configuring FXO Dialing Parameters

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Dialing Configuration** table, complete the fields as required.
- 3) Click **Apply**.

Result

FXO Dialing Configuration		
Pre Dial Delay (ms):	0	
Dial Tone Detection Mode:	CountryTone	
Dial Tone Detection Timeout (ms):		

6.3.2 Configuring FXO Answering Configuration

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Answering Configuration** table, for each endpoint, complete the fields as required.

Note: Available endpoints vary depending on the configuration of the unit,

- 3) Click **Apply**.

Result

FXO Answering Configuration				
ID	Wait Before Answering Delay (ms)	Answering On Caller Id Detection	Wait For Callee To Answer	
Slot4/FXO1	8000	Enable ▾	Disable ▾	
Slot4/FXO2	8000	Enable ▾	Disable ▾	
Slot4/FXO3	8000	Enable ▾	Disable ▾	
Slot4/FXO4	8000	Enable ▾	Disable ▾	

6.3.3 Configuring the FXO Incoming Call Behavior

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Incoming Call Behavior** table, for each endpoint, complete the fields as required.

Note: Available endpoints vary depending on the configuration of the unit,

- 3) Click **Apply**.

Result

For example

FXO Incoming Call Behavior		
ID	Not Allowed Behavior	
Slot4/FXO1	Play Congestion Tone ▾	
Slot4/FXO2	Do Not Answer ▾	
Slot4/FXO3	Play Congestion Tone ▾	
Slot4/FXO4	Play Congestion Tone ▾	

6.3.4 Configuring FXO Line Verification

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Line Verification** table, for each endpoint, complete the fields as required.
- 3) Click **Apply**.

Result

For example

FXO Line Verification	
Link State Verification:	Enable ▾
Link State Verification Timeout (ms):	5000

6.3.5 Configuring FXO Force End of Call

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Force End of Call** table, complete the fields as required.
- 3) Click **Apply**.

Result

For example

FXO Force End Of Call	
Force End Of Call On Call Failure:	Enable ▾
Call Failure Timeout (sec):	30
Force End of Call On Silence Detection Mode:	Disable ▾
Silence Detection Timeout (sec):	300
Force End Of Call On Tone Detection Mode:	Custom Tone ▾
Tone Detection Custom Frequency:	350
Tone Detection Custom Cadence:	
Detection Custom Repetition:	3 x

6.3.6 Configuring the Dial Tone Detection

Information

It allows the Mediatrix unit to wait for a dial tone before initiating the dialing sequence. If no dial tone is detected, the line is considered busy.

Steps

- 1) Go to **POTS/FXO Configuration**.

- 2) In the **FXO Dialing Configuration** table, from the **Dial Tone Detection Mode** drop box, select **CountryTone**.

Note: Not all PBX manufacturers produce the country dial tone on the extension line. If this is the case, make sure the **Dial Tone Detection Mode** is disabled, otherwise the Mediatrix unit will not output dialed digits.

Note: Not all PSTN switches produce the country dial tone on the PSTN line. If this is the case, make sure the **Dial Tone Detection Mode** is disabled, otherwise the Mediatrix unit will not output dialed digits.

- 3) Click **Apply**.

Result

FXO Dialing Configuration		
Pre Dial Delay (ms):	0	
Dial Tone Detection Mode:	CountryTone	
Dial Tone Detection Timeout (ms):		

6.3.7 Configuring the Answering Delay

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Answering Configuration** table, complete the fields as required.

Note: If the PBX does not pass the caller ID to the Mediatrix unit, you can reduce the **Wait Before Answering Delay** to **2500** to reduce the time before the Mediatrix unit goes off-hook upon ring detection.

- 3) Click **Apply**.

6.3.8 Configuring the Far End Disconnect Parameters

Information

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Force End of Call** table, from the **Force End Of Call On Tone Detection Mode** drop box, select **Custom Tone**.

- 3) Set the **Tone Detection Custom Frequency** field to **350**.

Note: Verify with your PBX supplier what tone (exact frequency and cadence) the PBX produces on the extension when the far end is disconnected.

- 4) Complete the other fields as required.
- 5) Click **Apply**.

Result

FXO Force End Of Call	
Force End Of Call On Call Failure:	Enable ▾
Call Failure Timeout (sec):	30
Force End Of Call On Silence Detection Mode:	Disable ▾
Silence Detection Timeout (sec):	300
Force End Of Call On Tone Detection Mode:	Custom Tone ▾
Tone Detection Custom Frequency:	350
Tone Detection Custom Cadence:	
Detection Custom Repetition:	3 x

6.3.9 Disabling Dial Tone Detection

Information

Disabling dial tone detection allows the Mediatrix unit to wait for a dial tone before initiating the dialing sequence. If no dial tone is detected or correctly recognised, the line is considered busy.

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Dialing Configuration** table, from the **Dial Tone Detection Mode** dropbox, select **Disable**.
- 3) Click **Apply**.

Result

FXO Dialing Configuration		
Pre Dial Delay (ms):	0	
Dial Tone Detection Mode:	Disable	
Dial Tone Detection Timeout (ms):	3000	

6.4 Advanced POTS Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

For FXS

- specify the Calling Party Name of the caller ID (CLIP) :
Pots.FxsCallerIdPrivateCallingPartyName
- to override a set of services that are activated during an emergency call:
Pots.FxsEmergencyCallOverride
- To set the period before the phone starts to ring in the event where the originator of an emergency call hangs-up before the emergency call center disconnects the call:
Pots.FxsEmergencyRingTimeout
- To customise a distinctive ringID: **Pots.FxsDistinctiveRingId**
- To customise a distinctive ring pattern: **Pots.FxsDistinctivePattern**

For FXO

- To override the FXO Custom Basic Parameters:
Pots.FxoCustomBasicParameters.OverrideDefaultCountryParameters and
Pots.FxoCustomBasicParameters.Impedance

6.4.1 FXS Distinctive Ring

The FXS endpoints support four distinctive ringing for basic incoming calls.

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

The following is an example of an Alert-Info via SIP INVITE:

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

The custom distinctive ring configuration allows the administrator to modify the ring pattern. These parameters can only be configured by the CLI or SNMP. Refer to the [Advanced POTS Parameters](#) . section.

The ring pattern can have up to three on/off pairs in the format of on1,off1,on2,off2,on3,off3 where:

- **on** is a numerical value representing the time, in milliseconds, during which ring tone will be active on the phone.
- **off** is a numerical values representing the time, in milliseconds, during which the phone will not ring.

For instance, **2000, 1000, 2000, 0** or **2000, 1000, 2000** is a cadence in which the frequency plays for 2 seconds, stops for 1 second, and plays for 2 more seconds.

Typically the ring pattern follows these rules:

- It can have up three pairs of "on,off". If less than 3 pairs are specified, **0** values will be added as necessary. Specifying more than six will only use the six first values.
- If it starts with a value of zero (0) , the ring pattern is invalid.
- The first zero (0) found in the string signals the end of the cadence (i.e. "200, 0, 300" is the same as "200").

6.5 Examples of FXO Tone Detection

6.5.1 Configuring the Detection of an 8 second 425 Hz Continuous Tone

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Force End of Call** table, from the **Force End Of Call On Tone Detection Mode** selection list, choose **Custom Tone**.
- 3) In the **Tone Detection Custom Frequency** field, enter 425.
- 4) In the **Tone Detection Custom Cadence** field, insert 8000,0 or 8000.
- 5) Click **Apply**.

Result

When a 425 Hz tone is played for 8 seconds, it will be detected.

FXO Force End Of Call		
Force End Of Call On Call Failure:	Disable	
Call Failure Timeout (sec):	30	
Force End of Call On Silence Detection Mode:	Disable	
Silence Detection Timeout (sec):	300	
Force End Of Call On Tone Detection Mode:	Custom Tone	
Tone Detection Custom Frequency:	425	
Tone Detection Custom Cadence:	8000,0	
Detection Custom Repetition:		

6.5.2 Configuring an On/Off British Reorder Tone

Steps

- 1) Go to **POTS/FXO Configuration**.
- 2) In the **FXO Force End of Call** table, from the **Force End Of Call On Tone Detection Mode** selection list, choose **Custom Tone**.
- 3) In the **Tone Detection Custom Frequency** field, enter 400.
- 4) In the **Tone Detection Custom Cadence** field, enter 400, 350, 225, 525 .
- 5) Click **Apply**.

Result

When a 400 Hz tone is played with a cadence of 0.4 seconds on, 0.35 seconds off, 0.225 seconds on, 0.525 seconds off, the tone will be detected.

FXO Force End Of Call		
Force End Of Call On Call Failure:	Disable	
Call Failure Timeout (sec):	30	
Force End of Call On Silence Detection Mode:	Disable	
Silence Detection Timeout (sec):	300	
Force End Of Call On Tone Detection Mode:	Custom Tone	
Tone Detection Custom Frequency:	400	
Tone Detection Custom Cadence:	400,350,225,525	
Detection Custom Repetition:		

6.5.3 Configuring the Detection of the Special Information Tone (SIT)

Steps

- 1) Go to **POTS/FXO Configuration**.

- 2) In the **FXO Force End of Call** table, from the **Force End Of Call On Tone Detection Mode** selection list, choose **Custom Tone**.
- 3) In the **Tone Detection Custom Frequency** field, enter 950.
- 4) In the **Tone Detection Custom Cadence** field, enter 330,660 .
- 5) Click **Apply**.

Result

When a SIT tone is played with a cadence of 950Hz/330ms, 1440Hz/330ms, 1800Hz/330ms, 950Hz/330ms, 1440Hz/330ms, 1800Hz/330ms etc. the tone will be detected.

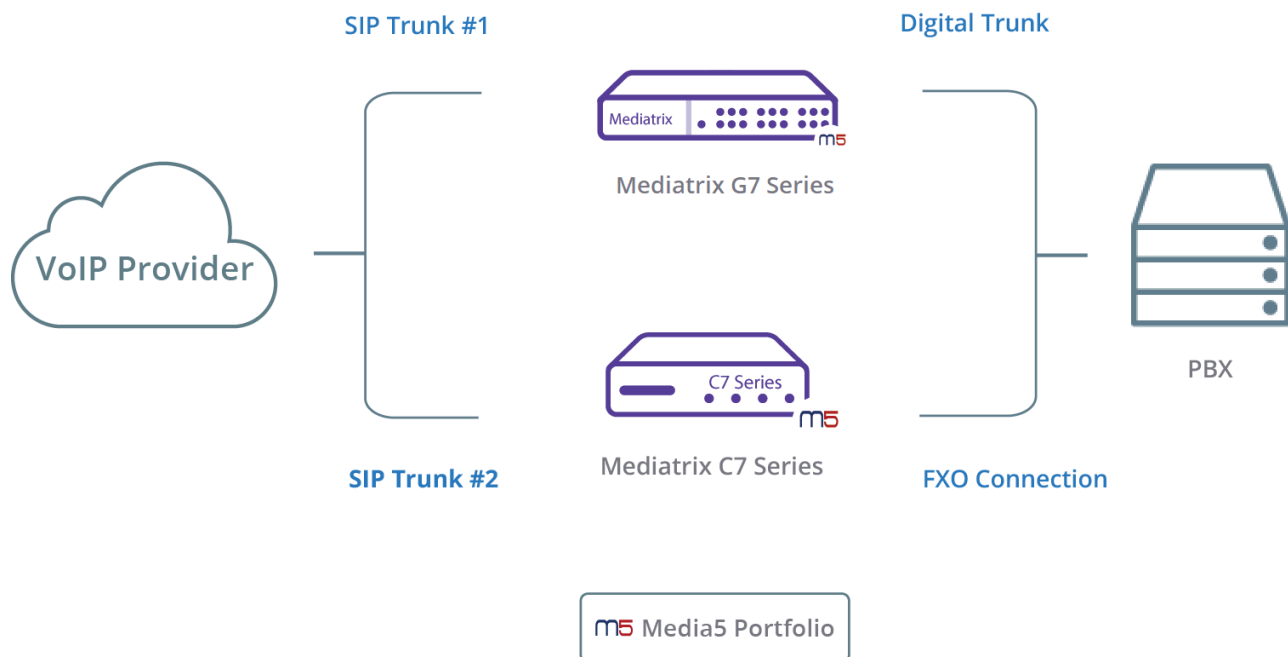
FXO Force End Of Call		
Force End Of Call On Call Failure:	Disable	
Call Failure Timeout (sec):	30	
Force End of Call On Silence Detection Mode:	Disable	
Silence Detection Timeout (sec):	300	
Force End Of Call On Tone Detection Mode:	Custom Tone	
Tone Detection Custom Frequency:	950	
Tone Detection Custom Cadence:	330,660	
Detection Custom Repetition:		

6.6 Cascade for Incoming Calls

A corporate PBX uses two VoIP gateways for inbound and outbound communication through a VoIP provider.

- Two Mediatrix devices connected to a SIP Trunk

For example: Cascade for incoming calls:



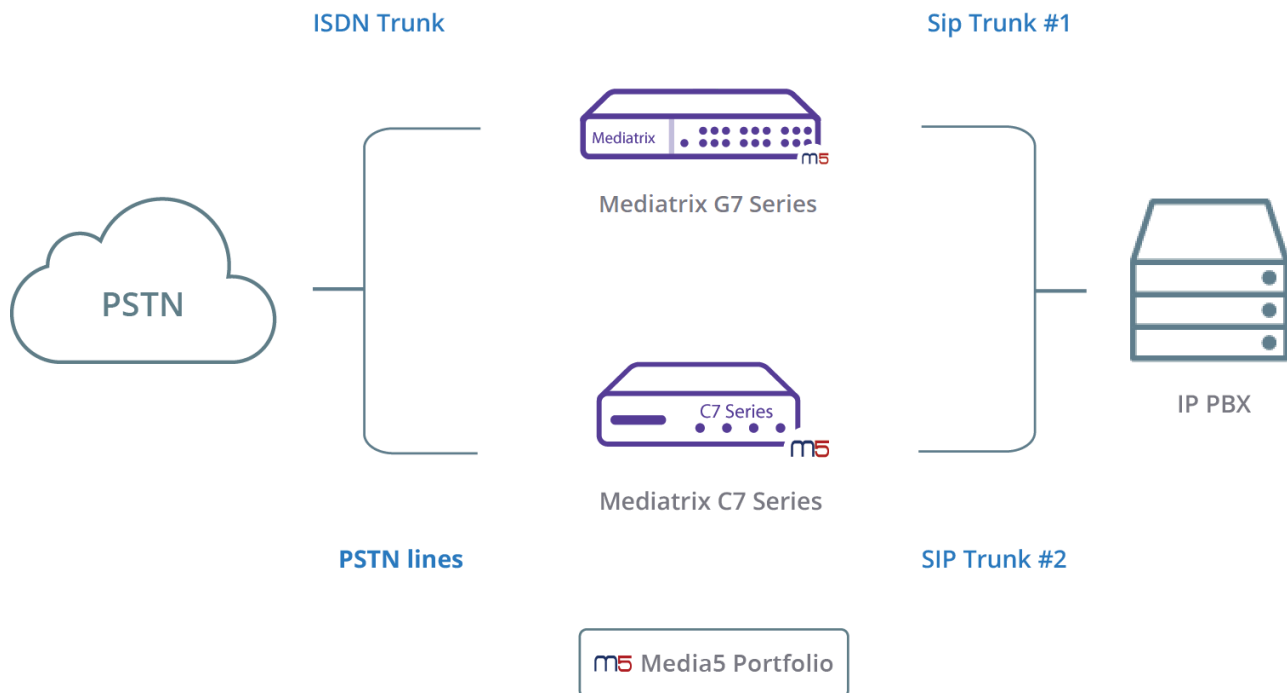
Note: When all channels of the primary Mediatrix unit are in use and there is a new incoming SIP call, by default, a Busy SIP message will be sent to the IP-PBX. If the analog/digital link is down, an error message will be sent. In both cases, the new incoming call will fail.

6.7 Cascade for Outgoing Calls

Corporate IP-PBX uses two VoIP gateways for inbound and outbound communication through the PSTN

- Two Mediatrix units in the LAN

For example:



Note: When all channels of the primary Mediatrix unit are in use and there is a new incoming SIP call, by default, a Busy SIP message will be sent to the IP-PBX. If the analog/digital link is down, an error message will be sent. In both cases, the new incoming call will fail.

7 ISDN

7.1 Cabling Information

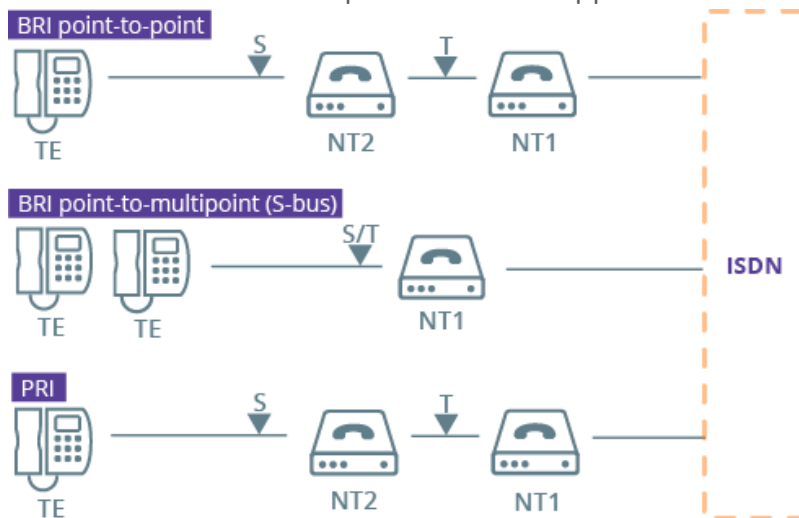
7.1.1 ISDN Reference Points

ISDN specifies a number of reference points that define logical interfaces between the various equipment types on an ISDN access line.

The Mediatrix unit supports the following ISDN reference points:

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

All other ISDN reference points are not supported.



7.1.2 BRI S/T Connection (RJ-48)



Caution: Always use standard telecommunication cables with a minimum of 26 AWG wire gauge.

BRI S/T connections use two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 3 and 6 are on one twisted pair and pins 4 and 5 are on a second pair according to common wiring standards which meet the TIA/EIA 568A and 568B requirements.



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



Pin#	TE mode	NT mode
1	Not Connected	Not Connected
2	Not Connected	Not Connected
3	Tx +	Rx +
4	Rx +	Tx +
5	Rx -	Tx -
6	Tx -	Rx -
7	Not connected	Not Connected
8	Not connected	Not Connected

7.1.3 PRI Connection (RJ-48)



Caution: Always use standard telecommunication cables with a minimum of 26 AWG wire gauge.

PRI connections use two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 1 and 2 are on one twisted pair and pins 4 and 5 are on a second pair according to common wiring standards which meet the TIA/EIA 568A and 568B requirements.

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



Pin #	NT Mode	TE Mode
1	Transmit #2 (+)	Receive #2 (+)
2	Transmit #1 (-)	Receive #1 (-)
3	Not connected	Not connected
4	Receive #2 (+)	Transmit #2 (+)
5	Receive #1 (-)	Transmit #1 (-)
6	Not connected	Not connected
7	Not connected	Not connected
8	Not connected	Not connected

7.2 Status

7.2.1 Basic ISDN Concepts

7.2.1.1 Preset Configuration

The ISDN Preset Configuration contains a set of values for the configuration of the parameters used by the ISDN connections.

The preset configuration files are located in the file system persistent memory. Depending on the Mediatrix unit you are using, the available ISDN Preset configuration files will differ or, it may also be possible that no preset configuration files are available depending on the Profile. Preset configuration files are provided by Media5 or can be user-defined, i.e. the current ISDN configuration was exported from a unit.

Using preset configuration files is especially useful for:

- units that do not use the default values provided by Media5 (for instance, using T1 instead of E1)
- using the same configuration on several units

IMPORTANT: user-defined presets are not kept in the event of a partial or factory reset. Only script files can be used as preset ISDN configuration files.

7.2.1.2 Integrated Services Digital Network (ISDN)

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

ISDN replaces the traditional telephone system so that one or two pairs of telephone wires can carry voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form. ISDN is a User-Network Interface (UNI) signalling protocol with a user and a network side.

- The user side is implemented in ISDN terminals (phones, terminal adapters, etc.)
- The network side is implemented in the exchange switches of the network operator.
- Both sides have different signaling states and messages.

The Mediatrix unit ISDN interfaces can be configured to work as user (TE) or network (NT) interfaces. Depending on your product, you can configure two types of ISDN interfaces:

- ISDN Basic Rate Interface (BRI)
- ISDN Primary Rate Interface (PRI)

7.2.1.2.1 Supported Signaling Protocols

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

IMPORTANT: In North America, the official standard is National ISDN2 (NI2). Virtually all 5ESS, DMS100, and GTD-5 switches have been upgraded to use that standard since the early 2000's. The "5ESS" and "DMS100" Signaling Properties settings are provided only for backwards compatibility only with older switches and PBXes, and might not support some functionalities such as Calling Name Delivery.

7.2.1.3 Auto configuration

The ISDN auto configuration is a process by which all ISDN interfaces try several configuration combination in order to obtain a physical link up and then a signaling link up (PRI interfaces only). The process is started using the `Isdn.AutoConfigure` command and can be stopped with

the `Isdn.CancelAutoConfigure` command. Starting the command will abruptly terminate all ongoing calls on the ISDN interfaces. Once the auto configuration process completes (successfully or not), a notification is sent reporting the result. If the operation is successful, the following parameters will be set with the values that provided the link up (overwriting the user configuration):

- Endpoint Type
- Clock Mode
- Port Pinout (PRI interfaces only)
- Line Coding (PRI interfaces only)
- Line Framing (PRI interfaces only)

7.2.1.3.1 ISDN Parameters Auto-Configured by Auto-Sensing

- PortPinout
- ClockMode
- LineFraming
- LineCoding
- EndpointType

7.2.2 Basic ISDN Tasks

7.2.2.1 Auto-Detecting and Auto-Configuring ISDN Interfaces

Information

Note: Some parameters cannot be auto configured. For example, the clock mode is configured according to the endpoint type, master for NT and slave for TE.

Steps

- 1) Go to **ISDN/Status**.
- 2) In the **Automatic Configuration** table, from the selection list, choose the interface you wish to auto configure or select all interfaces.
- 3) Click **Start Sensing**.

Note: Launching the Automatic Configuration may terminate abruptly all ongoing ISDN calls. The auto-configuration may take some time to complete and some of the current ISDN configuration settings might be replaced by new values.

Result

Under **ISDN/Status**, the **Physical Link** and **Signaling** fields of each interface should indicate **Up**.

Automatic Configuration	
Status:	--- All --- ▼ Start Sensing
Last Result:	None

Slot5/BRI1 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI2 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI3 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI4 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

7.2.2.2 Verifying the ISDN Status

Information

At any time, it is possible to check the status of the ISDN links.

Steps

- 1) Go to **ISDN/Status**
- 2) The **Physical Link** and **Signaling** status will be displayed for each interface.

Result

If the ISDN cables are properly connected and the basic interface settings are correct, the Physical Link should be **Up**.

Note: **Signaling** will also usually be "**Up**" on PRI links. However, in some cases (BRI, On-demand links), it is normal to be in the **Down** state, except for a brief period during call establishment.

Slot4/BRI4 [Configure]	
Physical Link: Up	
Signaling: Down	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot1/E1T1 [Configure]				
Line Type: T1				
Physical Link: Up				
Signaling: Up				
Bearer Group				
Channel 1: Idle	Channel 7: Idle	Channel 13: Idle	Channel 19: Idle	
Channel 2: Idle	Channel 8: Idle	Channel 14: Idle	Channel 20: Idle	
Channel 3: Idle	Channel 9: Idle	Channel 15: Idle	Channel 21: Idle	
Channel 4: Idle	Channel 10: Idle	Channel 16: Idle	Channel 22: Idle	
Channel 5: Idle	Channel 11: Idle	Channel 17: Idle	Channel 23: Idle	
Channel 6: Idle	Channel 12: Idle	Channel 18: Idle		

Slot2/E1T1 [Configure]				
Line Type: E1				
Physical Link: Up				
Signaling: Up				
Bearer Group				
Channel 1: Idle	Channel 9: Idle	Channel 17: Idle	Channel 25: Idle	
Channel 2: Idle	Channel 10: Idle	Channel 18: Idle	Channel 26: Idle	
Channel 3: Idle	Channel 11: Idle	Channel 19: Idle	Channel 27: Idle	
Channel 4: Idle	Channel 12: Idle	Channel 20: Idle	Channel 28: Idle	
Channel 5: Idle	Channel 13: Idle	Channel 21: Idle	Channel 29: Idle	
Channel 6: Idle	Channel 14: Idle	Channel 22: Idle	Channel 30: Idle	
Channel 7: Idle	Channel 15: Idle	Channel 23: Idle		
Channel 8: Idle	Channel 16: Idle	Channel 24: Idle		

7.2.3 Advanced ISDN Concepts

7.2.3.1 Definitions

media5corp.com

Term	Definitions
Originating Side	Where the call is initiated on the ISDN network. At the originating side

Term	Definitions
Destination Side	Where the call reaches its ISDN destination. The NT interface at the destination receives the call from another network, then sends a SETUP message over the ISDN link to one or more TE interfaces.
ISDN Interface	A physical ISDN port, either a BRI or PRI interface.
IsdnInterface	This is the 4th layer of the ISDN stack, referred in ITU-T Q.931 (05/98) as the Resource Management and Call Control entities.

7.2.3.2 Inband Tones Generation

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

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

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

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

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

On TE interfaces, as soon as the NT peer advertises that it plays inband tones through a Progress Indicator IE #8 or #1, the local inband tones generation is disabled for the rest of the call. Refer to the *UseImplicitInbandInfoEnable* interop parameter for special handling of Progress Indicator #1.

Whenever a tone is played inband locally or when the ISDN peer advertises that inband information is available, the CallManager is notified. The IP media path can then be opened earlier in the call, and can be closed with some delay after the call disconnection initiation. However, the configuration and associated behaviors of the higher-level entities are out of the scope of this document.

The following tables summarize the inband tones generation behaviour for both NT and TE endpoint types.

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

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

Note: When the signaling protocol is set to QSIG, the Signal IE does not exist so it has no effect on the inband tones generation. These inband tones are played if the inband tones generation is activated on the incoming side of the call.

7.2.3.3 Signal Handling

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

When the Signal IE handling is enabled on a given TE interface, the inband tones will be played towards the IP gateway when a Signal IE is received. On a NT interface, a Signal IE will be inserted in the ISDN messages sent to the TE peer when appropriate.

Note: If the signaling protocol is set to "NI-2" (National ISDN-2) on that interface, the Signal IE handling is forced to be enabled for a NT interface.

Note: When the signaling protocol is set to QSIG, the Signal IE is not used.

7.2.3.4 Interop Parameters

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

7.2.3.5 Channel Allocation Strategy

The ISDN interface supports 4 allocation strategy modes:

- ascending;
- descending;
- round-robin ascending;
- round-robin descending.

The Channel Allocation Strategy is configurable separately for each ISDN interface.

7.2.3.5.1 Ascending

In this mode, the `IsdnInterface` always allocates the free channel that has the lowest number.

7.2.3.5.2 Descending

The highest-numbered free channel is allocated.

7.2.3.5.3 Round-Robin Ascending

Starting from the enabled channel with the lowest number, the channels are selected increasingly at each allocation.

7.2.3.5.4 Round-Robin Descending

Same as round-robin ascending, except that it is exactly the opposite!

7.2.3.6 Ressource Management

7.2.3.6.1 Reservation of Channels for Incoming and Outgoing Calls

Channels can be reserved for incoming calls or for outgoing calls.

The **IncomingChannelRange** and **OutgoingChannelRange** parameters are defined for this purpose.

7.2.3.7 Supplementary Services

7.2.3.7.1 Supplementary Services Support

Three generic protocols are defined for the control of supplementary services, two of which are stimulus, the third being functional.

These protocols are:

- Keypad protocol;
- Feature key management protocol;
- Functional protocol.

The Functional protocol consists of two categories of procedures. The first category, called the separate message approach, uses separate message types to indicate a desired function. The HOLD and RETRIEVE set of messages are identified for this category.

The **FacilityServicesEnable** parameter is used to control the second category, called the common information element procedure, which uses the FACILITY information element.

When the facility services are disabled and the interface receives a FACILITY message, it answers it with a STATUS. When the facility services are enabled, the interface processes the FACILITY messages.

7.2.3.7.2 CLIP

In ISDN, the Calling Line Information Presentation (CLIP) is an optional service offered to the called party which provides the calling party's ISDN number. When the service is enabled, a Calling Party Number Information Element (CPN IE) containing the caller's IA5 digits is sent in the SETUP ISDN message.

CLIP is supplemented by privacy rules defined by [CLIR](#) (p.208) and [CLIR Override](#) (p.209). Refer to the diagrams in the [Interaction between CLIP, CLIR, and CLIR override](#) (p.210) section for details.

For all ISDN signaling protocols except QSIG, operation is as follows: on the originating side, the TE interface always sends the Calling Party Number IE (unless CLIP is disabled). It is up to the NT interface at the destination side to apply the appropriate privacy rules. If the originating side is NT, the Calling Party number is sent only if the **Calling Number** parameter is not set to 'Restricted' or if the **Override flag** parameter is set to 'Enabled'.

CLIP is enabled through the **ClipEnable** parameter, which can take the following values:

Disable	Calling Party Number IE is not sent.
Enable	Calling Party Number IE is sent in the SETUP message.
UserOnly	Calling Party Number IE is sent in the SETUP message only if the ISDN interface is configured as a TE.

7.2.3.7.3 CLIR

The Calling Line Information Restriction (CLIR) is a supplementary service offered to the calling party to restrict presentation of the calling party's ISDN number to the called party.

CLIR uses the Calling Party Number (CPN) IE's Presentation Indicator (PI) to disable presentation of the calling number to the called party. CLIR can be disabled by the CLIR override option, described later. Refer to the diagrams in the [Interaction between CLIP, CLIR, and CLIR override](#) (p.210) section for details.

For all ISDN signaling protocols except QSIG, operation is as follows: when the service is enabled on a TE originating interface, the Calling Party Number IE's Presentation Indicator field is set to "Restricted" upon transmission of an ISDN SETUP message from TE to NT. However, the TE must include the IA5 digits in the Calling Party Number.

When the service is enabled on a NT interface that receives a call, the Calling Party number IE Presentation Indicator is set to "Restricted" in the calling property returned to the call managing system.

For QSIG, when the service is enabled at the outgoing interface, the **Calling Party number IE Presentation Indicator** parameter is set to 'Restricted'. At the incoming side, this parameter has no effect. However, if the PI flag is set to "Restricted" in the received CPN IE, the calling party number is removed. See [ECMA-148](#) section 8.

CLIR is enabled through the **ClirEnable** parameter, which can take the following values:

Disable	There is no privacy restriction applied on the CLIP service.
Enable	<u>ISDN signaling protocols (except QSIG):</u> - TE interface that sends the SETUP message at the originating network side: The PI is set to "Restricted" in the CPN IE inserted in the SETUP message sent to the ISDN. However, the calling number is included in the CPN IE. - NT interface that receives the SETUP message at the originating network side: When receiving the SETUP message, the PI is forced to "Restricted" in the CPN IE received from the TE. The calling number itself is forwarded. <u>QSIG signaling protocol:</u> - Sending a SETUP message: The PI is set to "Restricted" in the CPN IE inserted in the SETUP message sent to the ISDN, unless the CLIR override option is set. However, even if PI is set to "Restricted", the calling number is included in the CPN IE. - Receiving a SETUP message: If PI is set in the received message, the calling party number is removed, unless the CLIR override option is set.

7.2.3.7.4 CLIR Override

CLIR override is an option that allows the calling party number to be presented to the destination party even when the Calling Party Number (CPN) IE's Presentation Indicator (PI) is set to "Restricted". This option is typically used for police or emergency services.

For all ISDN signaling protocols except QSIG, operation is as follows: if the CLIR Override is enabled on the NT interface at the originating side, the Calling Party Number IA5 digits is included in the Calling Party Number IEs even if the Presentation Indicator is set to "Restricted".

For QSIG, the Calling Line Information Restriction Override is a service offered at the destination interface. If the CLIR Override is not enabled and the Presentation Indicator is set to "Restricted" then the Calling Number is not presented. See [ECMA-148](#) section 8.

Refer to the diagrams in the [Interaction between CLIP, CLIR, and CLIR override](#) (p.210) section for details.

CLIR override is enabled through the **ClirOverrideEnable** parameter, which can take the following values:

Disable	The parameter has no effect.
Enable	<u>ISDN signaling protocols (except QSIG):</u> - The override option acts on the NT interface of the destination network side. It prevents the number to be removed from the CPN IE inserted in the SETUP message sent to the destination TE. <u>QSIG signaling protocol:</u> - The override option prevents the calling name to be removed from the CPN IE in a received SETUP message.

7.2.3.7.5 Interaction between CLIP, CLIR, and CLIR override

The following diagrams show how [CLIP](#) (p.208), [CLIR](#) (p.208) and [CLIR Override](#) (p.209) override work together to bring (or not) the calling party number from the call originator to the call destination. Refer to the [ISDN Signaling Protocols \(Except QSIG\)](#) (p.210) and [QSIG Signaling Protocol](#) (p.211) sections for the corresponding diagrams. Call flow must be read from the left (originating network side) to the right (destination network side).

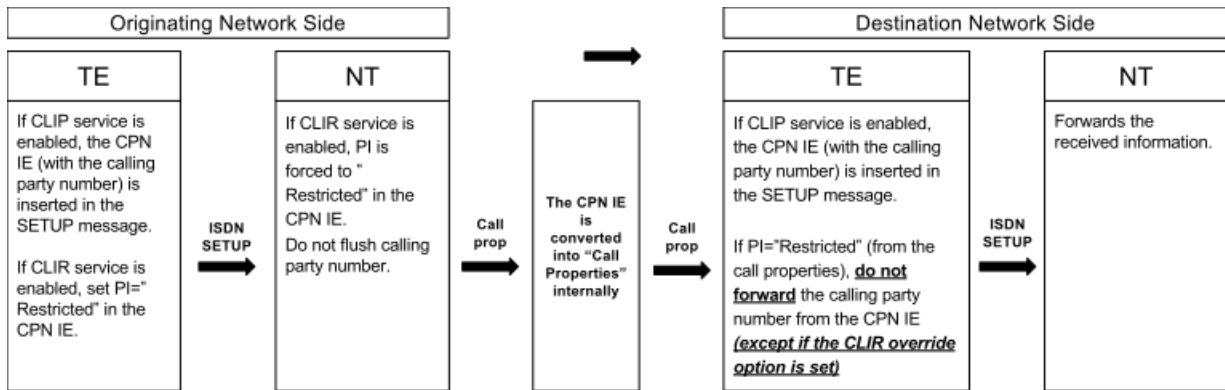
These diagrams also show on which interfaces the **ClipEnable**, **ClirEnable** and **ClirOverrideEnable** parameters have an effect. This is where they must be configured.

7.2.3.7.5.1 ISDN Signaling Protocols (Except QSIG)

The Mediatrix unit can play four different roles:

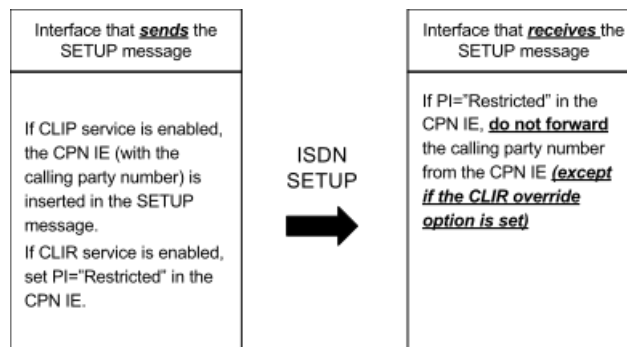
- TE interface at the Originating Network Side;
- NT interface at the Originating Network Side;
- TE interface at the Destination Network Side;
- NT interface at the Destination Network Side.

The following diagram illustrates an end-to-end call where all four roles are played by Mediatrix units:



7.2.3.7.5.2 QSIG Signaling Protocol

In QSIG, the ISDN interfaces have a peer-to-peer relationship. To describe how CLIP/CLIR/CLIR override work together, we only need to identify the interface that sends the SETUP message and the interface that receives it.



7.2.3.7.6 COLP

In ISDN, the Connected Line Identification Presentation is an optional service offered at the originating interface by the NT peer. When the service is enabled, a Connected Line Identification Presentation Element containing the connected number IA5 digits is sent under some conditions in the CONNECT ISDN message.

On the originating side, the TE interface always sends the Connected Party Number IE, it is up to the NT interface at the destination side to apply the appropriate privacy rules. If the originating side is NT, the Connected Party number is sent only if the Connected Number is not set to Restricted or if the Override flag is enabled.

For QSIG, the Connected Line Information Presentation is also an optional service offered at the outgoing and incoming interface. If available, the Connected Party Number IE containing the connected IA5 digits is included in the CONNECT ISDN message at the outgoing interface. However, the Connected Party Number is not presented at the incoming interface if the Connected Number is "Restricted" and the Override flag is not enabled see [ECMA-148](#), section 6.

The COLP can also be affected by the **uCP_ISDN_COLP_NUMBER** call property in the same way that the **CONP** (p.212) is affected by **uCP_ISDN_CONP_NAME** call property. See **CONP** (p.212) section for more information.

7.2.3.7.7 COLR

Generally, the Connected Line Identification Restriction is a service offered to the TE at the originating interface.

When the service is enabled on a TE originating interface, the Connected Party Number IE's Presentation Indicator field is set to "Restricted" upon transmission of an ISDN CONNECT message from TE to NT interface. However, the TE interface must include the IA5 digits in the Connected Party Number.

For QSIG, when the service is enabled at the outgoing interface, the **Connected Party number IE Presentation Indicator** parameter is set to 'Restricted'. At the incoming side, this parameter has no effect. See [ECMA-148](#) section 8.

7.2.3.7.8 COLR Override

In ISDN, the Connected Line Identification Restriction Override is a service offered at the originating interface by the NT peer.

If the CLIR Override is enabled on the NT interface at the originating interface, the Connected Party Number IA5 digits are included in the Connected Party Number IEs even if the Presentation Indicator is set to "Restricted".

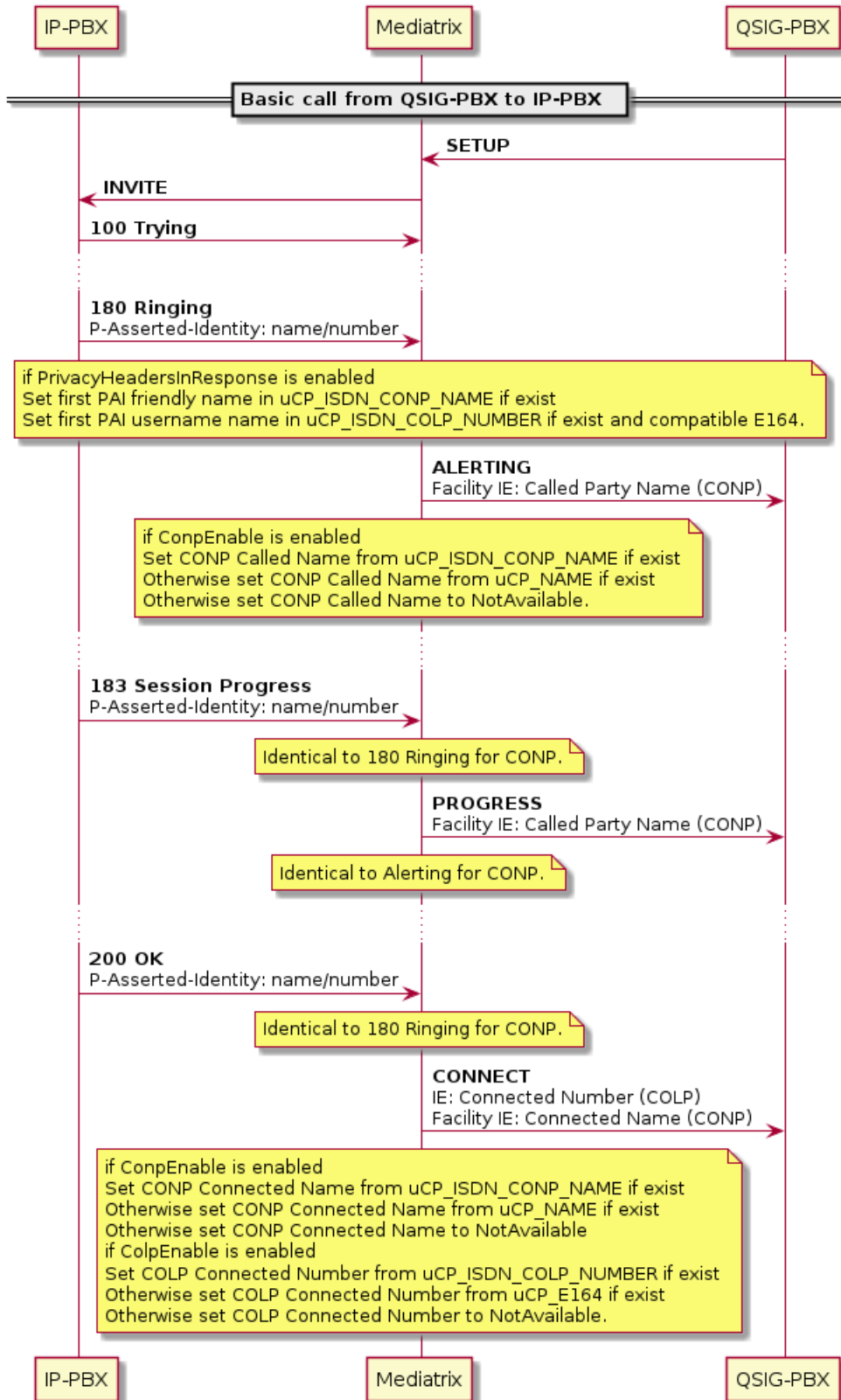
For QSIG, this parameter has no effect. See [ECMA-148](#) section 8.

7.2.3.7.9 CONP

The Connected Name identification Presentation (CONP) is a supplementary service which provides the name of the answering or alerting user to the calling user.

For ISDN-PBX to IP-PBX calls, if the **PrivacyHeadersInResponse** parameter is enabled, the **uCP_ISDN_CONP_NAME** call property will be set from the 180 Ringing, 183 Session Progressing, or 200 OK SIP message accordingly to the values of the P-Asserted-Identity SIP header. If the **ConpEnable** is enabled, the ISDN CONP called name and connected name will be set accordingly to the value of the **uCP_ISDN_CONP_NAME** call property respectively in the ISDN Alerting and Connect message.

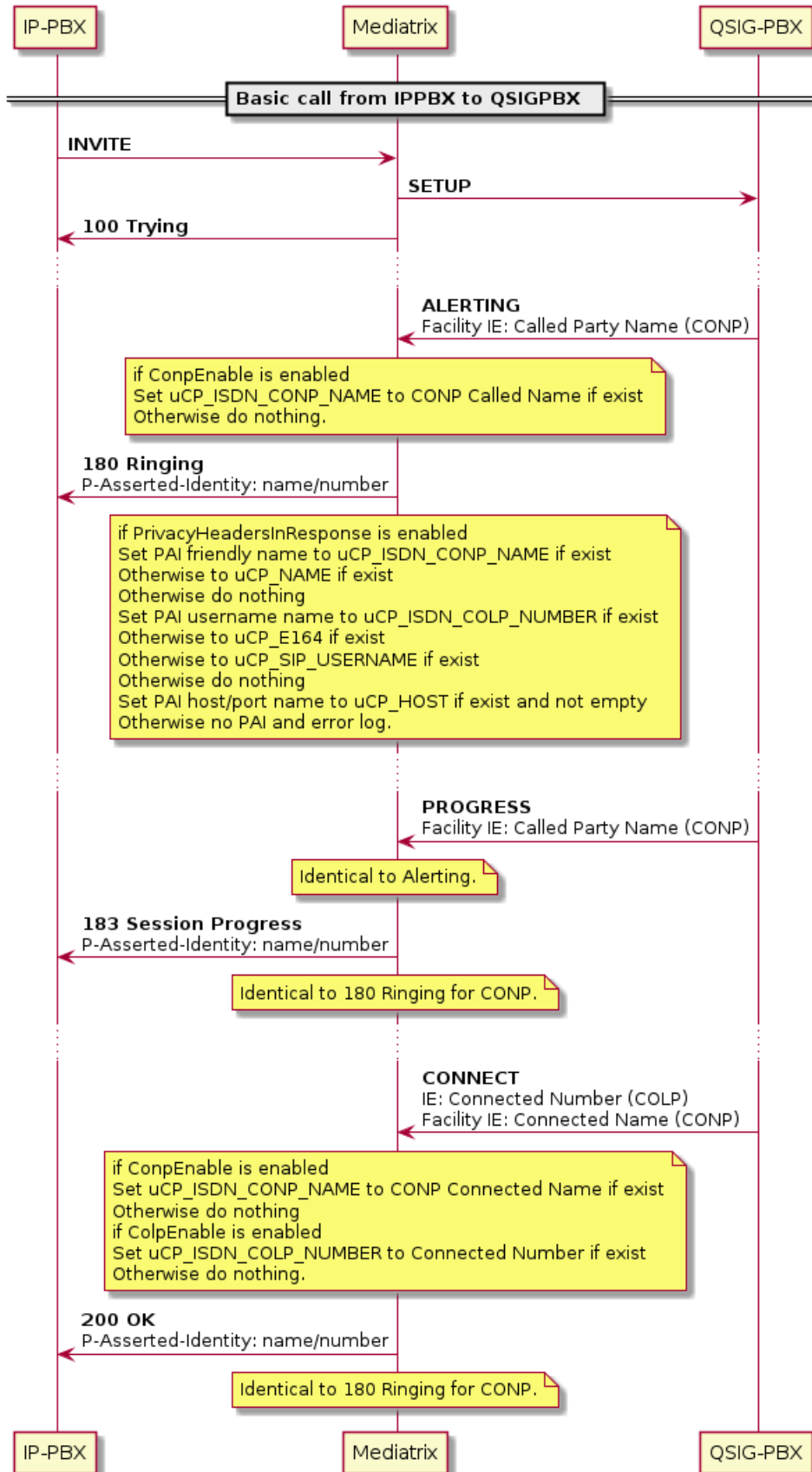
The following diagram shows a detailed call from ISDN-PBX to IP-PBX with the parameters involved on both the IP and ISDN sides.



For IP-PBX to ISDN-PBX calls, if the **ConpEnable** parameter is enabled, the **uCP_ISDN_CONP_NAME** call property will be set from the ISDN Alerting, ISDN Progress, or ISDN Connect from the value

of the Called or Connected Name Facility Information Element. If the **PrivacyHeadersInResponse** parameter is enabled, the P-Asserted-Identity SIP header friendly name will be set to the **uCP_ISDN_CONP_NAME** call property.

The following diagram shows a detailed call from IP-PBX to ISDN-PBX with the parameters involved on both the IP and ISDN sides.



If the number of characters in the connected/called party name exceeds 50, the gateway will truncate the excess characters.

7.2.3.7.10 Facility Message Waiting Delay

Upon reception of a SETUP from the remote peer, the interface can optionally wait for a configurable amount of time for a FACILITY message before processing the call. As soon as it receives a FACILITY message or the delay expires, it goes on with normal call processing. The delay is configured via the **MaximumFacilityWaitingDelay** parameter.

7.2.3.7.11 MSN (Multiple Subscriber Number)

The Multiple Subscriber Number is a service allowing the TE to configure up to three numbers. This service is available only for a BRI interface configured in TE Point To Multipoint. When this service is enabled in the TE, the Called Party Number (Called E.164) received from IE is matched with these numbers. If the Called Party Number is found, the call can be processed. In the case where the E.164 is not matched, the call is silently discarded.

7.2.3.7.12 Notify

The NOTIFY is an ISDN service independent of the HOLD and RETRIEVE. It serves only to notify an ISDN endpoint when the remote peer, usually a SIP endpoint, holds or resumes a call. So a NOTIFY REMOTE HOLD message is sent to the ISDN endpoint when the remote peer puts the call on hold, and a NOTIFY REMOTE RETRIEVAL message is sent when the remote peer resumes the call.

If the ISDN **SignalingChannelOutgoingNotifyEnable** parameter is disabled, no NOTIFY message is sent.

The BRI phone can use this message to inform the user of the new call state, by displaying the remote hold or retrieval message on its LCD screen for example. Note that the BRI phone keeps the voice path opened, so the hold tone or MOH can be heard.

7.2.3.7.13 Calling Party Name

Calling Party Name can be received and sent through three different methods:

- Facility information element;
- Display information element;
- User-User information element.

When receiving an incoming call, the Calling Party Name value comes from the provided IE, in this order:

- Display
- Facility

- User-User

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

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

Protocol	CallingNameDelivery			
	eFacility	eDisplay	eUserUser	eSignalingProtoco
DSS1	IE User-User	IE User-User	IE User-User	IE User-User
Dms100	IE Facility	IE Display	IE Display	IE Display
NI-2	IE Facility	IE Facility	IE Facility	IE Facility
5ESS	IE Facility	IE Facility	IE User-User	IE Facility
QSIG	IE Facility	IE Facility	IE Facility	IE Facility

7.2.3.7.14 Call Rerouting

The Call Rerouting supplementary service allows to reroute an incoming public ISDN call (originated from PSTN) within or beyond the private ISDN network (such a PBX) as specified in the ETS30020701, section 10.5. The Rerouting data are received and relayed through a FACILITY message containing a Facility Information Element. The Rerouting data are encoded in a CallRerouting invoke component as specified in the ETS30020701, section 7.

In a Mediatrix typical CallRerouting scenario, when the CallRerouting supplementary service is enabled (the **Isdn.SignalingChannelFacilityServicesEnable** parameter is enabled and the **Isdn.SignalingChannelCallReroutingBehavior** parameter is set to "RelayReroute" or "ProcessLocally") and a Facility Information Element containing a CallRerouting invoke component is received via a FACILITY message on a TE endpoint (from the private network), the ISDN service parses the CallRerouting data and forward it to the CallManager via a specific CallMessage.

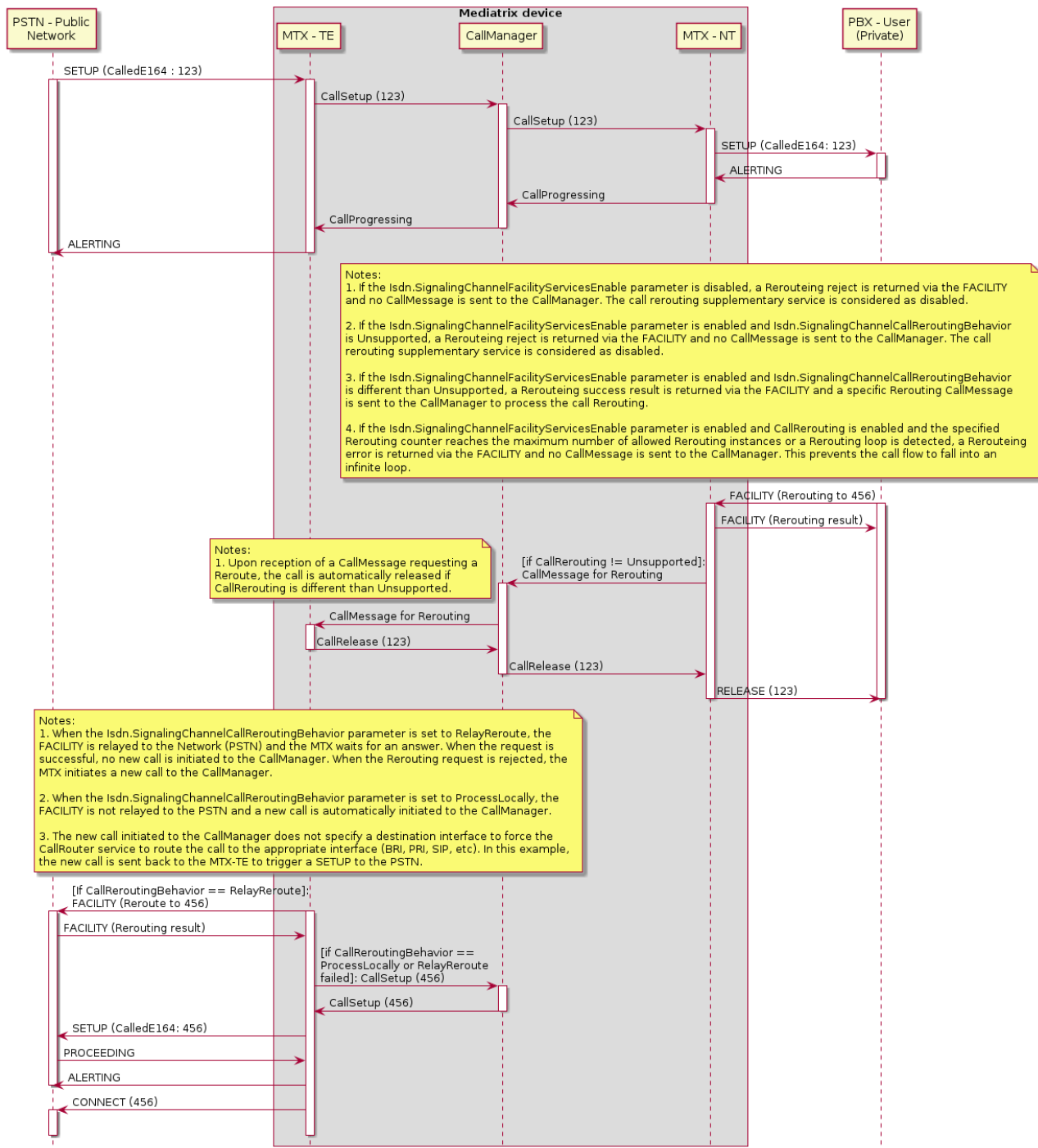
To prevent infinite CallRerouting loops, the ISDN service inspects the reroutingCounter value and returns an error if a loop is detected or if the maximal reroutingCounter value allowed by the ETS300 207 01 is reached (>5). When the CallRerouting service is not supported (**Isdn.SignalingChannelFacilityServicesEnable** parameter is disabled or **Isdn.SignalingChannelCallReroutingBehavior** set to "Unsupported"), the CallRerouting request is automatically rejected.

Upon reception of a CallMessage specifying a Rerouting request, the ISDN service inspects the CallRerouting properties set and according to the **Isdn.SignalingChannelCallReroutingBehavior** parameter, the services takes an action. If the parameter is set to "RelayReroute", a Facility Information Element containing a CallRerouting invoke component is transmitted to the ISDN peer (public network side) via a FACILITY message. The ISDN service waits for an answer from the peer.

If the parameter is set to "ProcessLocally" or a negative CallRerouting answer is received (a negative answer received would mean that the public network side (PSTN) is unable to complete the call Rerouting request), the Isdn service initiates a new call to process locally the call Rerouting request. The new call is requested to the CallManager without specifying a destination interface to force the CallRouter service to select the appropriate route. If the new call is routed to an ISDN interface, the ISDN service sends a SETUP containing a DivertingLegInformation2 invoke component in the Facility IE as specified in the ETS 300 207 01, section 10.2 and section 10.4. The data related to the call diversion set in the DivertingLegInformation2 are transferred from the CallRerouting properties.

Note: Upon reception of the CallMessage requesting a Rerouteing, the ISDN service automatically releases the current call whatever if the **Isdn.SignalingChannelCallReroutingBehavior** parameter is set to "RelayReroute" or "ProcessLocally".

An illustration of a typical ISDN Call Rerouting scenario (Call Forward Unconditionnal) in a Mediatrix device would be as the following sequence diagram:



7.2.3.7.15 Malicious Call Identification

Malicious Call Identification (MCID) is a supplementary service that enables the service provider to identify the source of malicious calls. A user who receives a malicious call from another network can notify the PSTN of the malicious nature of the call, allowing the offnet system to take action, such as notifying legal authorities.

To invoke the MCID supplementary service, the called user shall send a mCIDRequest invoke component carried by a Facility information element in a FACILITY message.

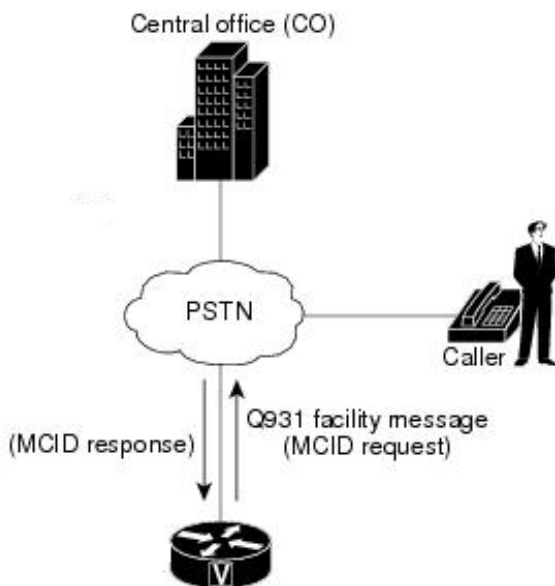
To indicate that the service has been accepted, the network shall send:

- if accepted, a mCIDRequest return result component, or
- if rejected, a mCIDRequest return error component carried by a Facility information element in a FACILITY message

Note: For customer needs, the mCIDRequest invoke can be sent from both Network and User sides. This behavior does not follow the signaling flow in EN 300 130-1 Annex A which stipulates that the mCIDRequest invoke is only sent from the User side to Network side.

To enable the MCID supplementary service, the **Isdn.SignalingChannel.FacilityServicesEnable** and **Isdn.SignalingChannel.McidEnable** parameters must both be set to Enable. Further more, the MCID feature is only available for DSS1 signaling.

An illustration of a typical ISDN MCID scenario in a Mediatrix device:



On the reception of a SIP INFO message containing the **P-Call-Info: malicious** proprietary header, the associated ISDN call will send an ISDN FACILITY message indicating that this call is tagged as malicious.

7.2.3.7.16 InformationFollowing Operation

The "informationFollowing" operation is supported for NI2 signaling only.

When a SETUP message is received containing an "informationFollowing" operation, the unit immediately sends a PROCEEDING message. The unit then waits normally for a FACILITY

message containing the calling party name, for a maximum time configured with the **MaximumFacilityWaitingDelay** parameter.

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

Note that the "informationFollowing" operation is mutually exclusive with the configuration parameter **CallProceedingDelay**, which configures a delay before sending the PROCEEDING message. If the PROCEEDING message is sent due to the "informationFollowing" operation, the **CallProceedingDelay** parameter is ignored.

7.2.3.7.17 Advice of Charge

To enable the Advice of Charge (AOC) support on the ISDN interface you must enable the FACILITY services and at least one of the following AOC support: AOC-E (End of Call) or AOC-D (During the Call).

Note: Since the AOC from ISDN interface to SIP is currently not supported, enabling the AOC on an ISDN interface configured as TE (user side) is only meaningful when using hairpinning.

7.2.3.8 Default Values for Call Properties

Each ISDN interface can be configured with default values for the following parameters in the Calling Party Number IE and the Called Party Number IE.

These default values apply only to outgoing ISDN calls:

Information Element (IE)	Parameter	Configuration Parameter
Calling Party Number	Type of Number (TON)	DefaultCallingTon
Calling Party Number	Numbering Plan Indication (NPI)	DefaultCallingNpi
Calling Party Number	Presentation Indicator (PI)	DefaultCallingPi
Calling Party Number	Screening Indicator (SI)	DefaultCallingSi
Called Party Number	Type of Number (TON)	DefaultCalledTon
Called Party Number	Numbering Plan Indication (NPI)	DefaultCalledNpi

These parameters provide default values that are inserted in the Calling Party Number IE and the Called Party Number IE when these values are not already provided by the call properties.

Another way to control these values is by using the "Properties Manipulation" feature of the Call Router. This method has precedence over the parameters described here.

The following paragraphs provide additional information on how these parameters work:

- TON and NPI: If the value is not available from the Call Properties, the corresponding value from **DefaultCallingTon**, **DefaultCalledTon**, **DefaultCallingNpi** or **DefaultCalledNpi** parameter is used directly.
- PI: If PI is not available from the Call Properties, its value is determined by the following two steps.
 - First, it is set to the default value defined by "DefaultCallingPi".
 - Second, it can be overridden by the CLIP and CLIR services: the value can be set to "Restricted" by the CLIR service and the value can be set to "NotAvailable" if there is no number to forward.
- SI: Like the other parameters, the **DefaultCallingSi** parameter is ignored if the SI value is provided by the Call Properties. If SI is not provided by the call properties, it is set to the value provided by **DefaultCallingSi** except for one special case: when the **DefaultCallingSi** parameter is set to "Context Dependent", the unit applies internal rules to set SI to the value that makes most sense according to context. These internal rules are as follows:
 - For all signaling protocols except QSIG:
 - If interface is configured as NT (network side), SI is set to "NetworkProvided"
 - If interface is configured as TE (user side), SI is set to "UserProvidedNotScreened"
 - For QSIG signaling protocol:
 - If the calling party number string is not empty, SI is set to "UserProvidedVerifiedAndPassed"
 - If the calling party number string is empty, SI is set to "NetworkProvided"

7.2.4 Advanced ISDN Tasks

7.2.4.1 Exporting a Preset Configuration File

Before you start

If you are using a user-defined preset configuration file, do not forget to upload it through the file management system.

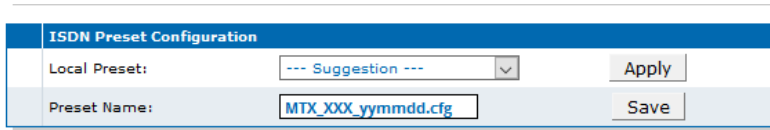
Steps

- 1) Go to **ISDN/Status**.
- 2) In the **ISDN Preset Configuration** table, in the **Preset Name** field, enter the name for the exported preset configuration file.

Note: We strongly recommend indicating the type of unit and date of export as the name of the preset configuration file. For example: MTXC740_20230215.

- 3) Click **Save**.

Result



The preset configuration file will be displayed under **Management/File**, in the **Internal files** table.

7.3 Primary Rate Interface

7.3.1 PRI (E1/T1) Configuration

7.3.1.1 Important Information for North America

Mediatrrix units are configured to default for E1, which is used in most countries in Europe, Middle-East, Africa and Oceania. For the T1 interface used in North America, some settings **MUST** be changed.

Setting	T1 (North America)	E1 (Default)
Line Coding	B8ZS	HDB3
Line Framing	ESF (usually), or SF(D4)	CRC4 (usually), or NO-CRC4
Signaling Protocol	NI2 (usually)	DSS1 (usually)
Preferred Encoding Scheme	u-Law	a-Law
Fallback Encoding Scheme	a-Law	u-Law
Channel Range	1-23	1-30

7.3.1.2 Supported Signaling Protocols

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

IMPORTANT: In North America, the official standard is National ISDN2 (NI2). Virtually all 5ESS, DMS100, and GTD-5 switches have been upgraded to use that standard since the early 2000's. The "5ESS" and "DMS100" Signaling Properties settings are provided only for backwards compatibility only with older switches and PBXes, and might not support some functionalities such as Calling Name Delivery.

7.3.1.3 Important PRI Settings

Endpoint Type, Clock Mode, and Port Pinout

These settings should normally be auto-detected (Step 1)

- In TE (Terminal Equipment) mode, the unit is normally in slave mode and will automatically update its clock from the other (telco) side.
- In NT (Network Termination) mode, the unit is normally in master mode and will provide the clock to the other side.
- For more information on clock reference when using multiple interfaces, refer to the [Mediatrrix Gateways and ISDN Clock Synchronisation](#) and [Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).

Signaling Protocol

Refer to the [Supported Signaling Protocols](#) (p.199) section.

Fallback Encoding Scheme

Only valid when receiving a SETUP message. The user sending the SETUP message does not indicate an alternative bearer capability.

Channel Range

This is typically used for fractional T1 or E1 service.

- Channels start at 1 and make abstraction of the synchronisation and signaling timeslots.
- Channels outside of the range defined for this field are ignored. For example:
 - Fractional T1 512K: Channel Range 1-8 (corresponds to B channels 1-8, D channel 24)
 - Fractional E1 on ramp 10: Channel Range 1-10 (corresponds to timeslot 0 + B channels 1-10 + D channel 16)
 - Fractional E1 on ramp 10: Channel Range 1-20 (corresponds to timeslot 0 + B channels 1-15 + D channel 16 + B channels 17-21)

Channels Reserved for Incoming Calls and Channels Reserved for Outgoing Calls

- Bearer channels are by default usable for both incoming and outgoing calls. Use this range to reserve channels for incoming or outgoing calls.
- Channels outside of the range defined by **ChannelRange** parameter are ignored.
- Channels reserved in both **IncomingChannelRange** and **OutgoingChannelRange** parameters are considered usable for both incoming and outgoing calls.

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

Calling Name Max Length

The value for calls from SIP to ISDN is set to 34 by default, but ranges from 0 to 82. Some telephone companies do not allow customers to pass Calling Name and will drop calls if it is not set to zero.

Interface Configuration

Call properties set in the Call Router have precedence over the default values of the table. For more details on the Call Router, refer to the [Call Router user guide](#) published on the [Media5 Documentation Portal](#).

7.3.1.4 Using a Preset Configuration File

Before you start

If you are using a user-defined preset configuration file, do not forget to upload it through the file management system, under **Management/File**.

Steps

- 1) Go to **ISDN/Status**.
- 2) In the **ISDN Preset Configuration** table from the **Local Preset** list, choose the preset configuration file you wish to import.

Note: In North America, the PRI_NorthAmerica-NI2.cfg contains the recommended settings for a connexion with most of the telephone operators.

- 3) Click **Apply**.

Result

The preset configuration file will be uploaded to the unit and applied.

Note: In most cases, the unit will be restarted. Please wait a few minutes for the operation to complete, then log-in again into the Web interface of the unit.

ISDN Preset Configuration	
Local Preset:	PRI_NorthAmerica-NI2.cfg Apply
Preset Name:	Save

7.3.1.5 Associating a PRI Port to a Line Type and Protocol

Steps

- 1) Go to **System/Hardware**.
- 2) In the **PRI Ports Configuration** table, from the **Line Type** selection list, select either E1 or T1.
- 3) From the **Signaling** selection list, associate a type of signaling to the PRI port.

- 4) Click **Apply**.
- 5) Restart the unit.

Result

The selected line type will appear under **ISDN/Primary Rate Interface**. This is an example of a PRI port association.

PRI Ports Configuration			
Port	Line Type	Signaling	
Slot1/E1T1	E1 ▼	Isdn ▼	
Slot3/E1T1	E1 ▼	Isdn ▼	

7.3.1.6 Configuring the E1T1 Interface (PRI)

Before you start

Endpoint Type, Clock Mode, and Port Pinout: These settings should normally be auto-detected , therefore, always use [Auto-Detecting and Auto-Configuring ISDN Interfaces](#) (p.200) procedure first to automatically detect and to automatically configure your PRI interface. The manual configuration of the PRI interface should be used for fine tuning of the configuration.

Information

Note: Before you start, refer to the [Important Information for North America](#) (p.223) section

Steps

- 1) Go to **ISDN/Primary Rate Interface**.

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

- 2) From the **Select Interface** drop box, select the E1/T1 interface you wish to modify.

Note: Depending on the Mediatrix model, there may be several interfaces.

- 3) Modify the parameters as required.
- 4) Click **Apply**.

Result

7.3.2 Advanced Primary Rate Interface (PRI) Tasks

7.3.2.1 Modifying Port Pinout

Steps

- 1) Go to **ISDN/Primary Rate Interface**.

Note: Not all PRI and/or BRI platforms support Port Pinout.

- 2) In the **Interface Configuration** table, set the **Port Pinout** to reflect your configuration.

Result

Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	NT ▼
Clock Mode:	Master ▼
Port Pinout:	NT ▼
Monitor Link State:	Auto ▼
Line Coding:	TE
	NT

7.4 Basic Rate Interface (BRI)

7.4.1 ADvanced BRI Tasks

7.4.1.1 Configuring the BRI Interface

Before you start

Always use the Auto-sensing feature to automatically detect and to automatically configure your PRI interface. Use the [Auto-Detecting and Auto-Configuring ISDN Interfaces](#) (p.200) procedure first. The manual configuration of the BRI interface should be used for fine tuning of the configuration.

Information

It is important to take into consideration the following information:

- **Endpoint Type:** Values used for the Mediatrix unit must be opposite to the value used for the PBX. For instance, if the PBX is set to TE, then the Mediatrix unit must be set to NT. When the BRI interface **Signaling Protocol** is set to QSIG, the endpoint type is only used in the second layer (LAPD) since it is a concept that does not exist in QSIG. NOTE: To use a specific interface as the clock reference, this parameter must be set to TE. For more information on Clock Synchronisation, refer to the [Technical Bulletin - Mediatrix Gateways and ISDN Synchronisation](#) and [Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).
- **Preferred Encoding Scheme:** Only G.711 u-Law and G.711 a-Law codecs are allowed. G.711 u-Law may not be supported by DSS1 NT and TE endpoints. It is recommended to use G.711 a-Law as preferred encoding protocol.
- **Fallback Encoding Scheme:** Only G.711 u-Law and G.711 a-Law codecs are supported. Only valid when receiving a SETUP message. The user sending the SETUP message does not indicate alternative bearer capability.
- **Clock Mode:** "Auto" should be the value to use. In a BRI configuration, setting the clock mode to slave for a NT endpoint can be set for interop usage, while setting the clock mode to master for a TE endpoint is invalid (slave mode is automatically applied in this case). For more information on Clock Synchronisation, refer to the [Technical Bulletin - Mediatrix Gateways and ISDN Synchronisation](#) and [Technical Bulletin - Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).
- **Calling Name Max Length:** The value for calls from SIP to ISDN ranges from 0 to 82.
- **Exclusive B-Channel Selection:** When the parameter is enabled only the requested B channel is accepted when a call is initiated; if the requested B channel is not available, the call is cleared.
- **Monitor Link State Parameter:** When enabled with the **Ignore OPTIONS on no usable endpoints** also enabled under the **SIP/Interop** page, this will influence how the SIP options are answered.
- **Connection Type:** depends on the equipment to which the Mediatrix unit port is connected to and it must be the same for all interconnected pieces of equipment.
- **Signaling Protocol:** Must match the connected ISDN equipment or network.
- **TEI Negotiation :** Only applies on Point to Multipoint connections.
- Call properties set in the Call Router have precedence over the default values of the **Interface Configuration** table. For more details on the Call Router, refer to the [DGW Configuration Guide - Call Router user guide](#) published on the [Media5 Documentation Portal](#).
- In strings, the space character is ignored and duplicating causes is not allowed.
- Some ISDN switches may require that the Sending Complete information element be included in the outgoing SETUP message to indicate that the entire number is included and there are no further destination digits to be sent.
- An ISDN telephone may send INFORMATION messages that contain a "Keypad Facility". You can thus trigger a supplementary service (Hold, Conference, etc.) by sending a keypad facility. Since the keypads can be received via several INFORMATION messages, they are accumulated until they match or reset if the keypad reception timeout (second) has elapsed since the last keypad has been received. The keypad reception timeout can only be modified via SNMP. If the

keypad reception timeout is set to 0, it disables the timeout, thus assuming that all keypads will be received in a single INFORMATION message

Steps

- 1) Use the [Auto-Detecting and Auto-Configuring ISDN Interfaces](#) (p.200) procedure first.
- 2) Go to **ISDN/Basic Rate Interface**.
- 3) From the **Select Interface** drop-box, select the BRI interface you wish to modify.

Note: Depending on the Mediatrix model, there may be several interfaces. To configure more than one interface at a time, use the **Apply To The Following Interfaces** table.

- 4) Make all required changes to the displayed parameters.
- 5) Click **Apply**.

7.4.1.2 Setting the Clock Mode

Steps

- 1) Go to **ISDN/Basic Rate Interface**.
- 2) In the **Select Endpoint** dropdown menu, select the endpoint you want to configure.
- 3) In the **Interface Configuration** table, set the **Clock Mode**.

Result

Interface Configuration	
Endpoint Type:	TE ▼
Clock Mode:	Auto ▼
Monitor Link State:	Auto Master Slave
Connection Type:	int ▼

7.5 Interop

7.5.1 Advanced Interop Concepts

7.5.1.1 Interop Parameters

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

7.5.2 Advanced Interop Tasks

7.5.2.1 Configuring Interop Parameters

Information

Interop parameters can be configured for PRI and BRI interfaces.

Steps

- 1) Go to **ISDN/Interop**.
- 2) From the **Select Interface** drop down, choose the interface for which you wish to configure the interop parameters.

Note: To select more than one interface at a time, if available on the unit, use the **Apply To The Following Interfaces** table.

- 3) In the **Interface Configuration** table, complete the fields as required.

- 4) Click **Apply**.

7.6 Timer

7.6.1 Basic Timer Concepts

7.6.1.1 ISDN Clock Mode

ISDN is a synchronous network, meaning that all endpoints on the network need to synchronize on the same clock signal. Typically, one endpoint acts as the clock MASTER, generating the clock signal, and the other endpoints act as clock SLAVE, synchronizing on the clock signal received from the MASTER.

By default, a NT type endpoint acts as clock MASTER, and a TE type endpoint acts as clock SLAVE. This default behaviour can be changed by using the web interface of the Mediatrix units. The clock mode of the ISDN endpoints can be set to either clock MASTER or clock SLAVE.

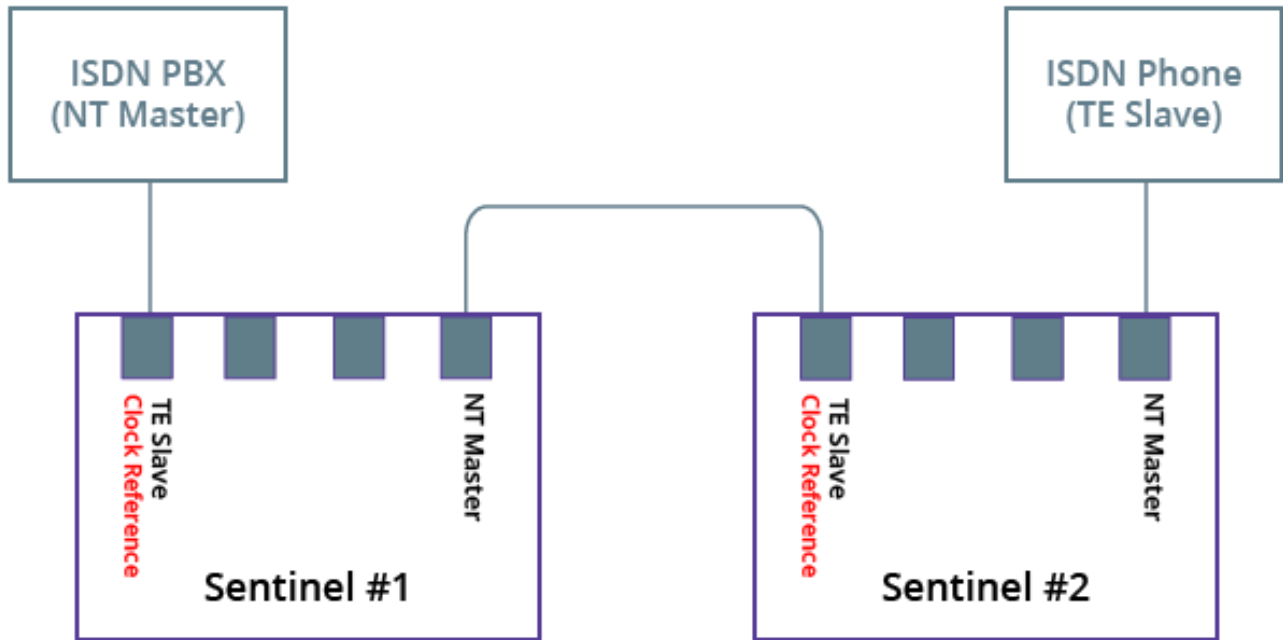
The following is a description of the endpoints behaviour with regards to clock signal synchronization:

- In transmission, all endpoints, regardless of their type, send a clock signal along with the data they send.
- In reception, all endpoints, regardless of endpoint type, use the clock they receive from the other end to synchronize the received data.
- In transmission, a clock SLAVE adjusts the clock it sends, based on the clock received from the other end in reception.
- In transmission, a clock MASTER sends an absolute clock signal that does not depend on the clock received from the other end.

7.6.1.2 ISDN Clock Reference

On Mediatrix units with multiple ISDN endpoints, it is possible to select which endpoint should be used as the clock reference. When an endpoint is designated as clock reference, the other endpoints on the Mediatrix unit use this endpoint's clock as a synchronization source for generating their own clock.

In the following example, the clock signal generated by the ISDN PBX is received on the Mediatrix C740 #1's TE Slave endpoint and taken as a reference for this unit. Therefore the clock signal generated by this unit's NT Master endpoint is synchronized on this signal. The Mediatrix C740 #2's TE Slave endpoint receives this signal and uses it as a reference for this unit, meaning that the clock signal generated by this unit's NT Master endpoint towards the ISDN phone is synchronized on this signal, therefore on the PBX's signal.



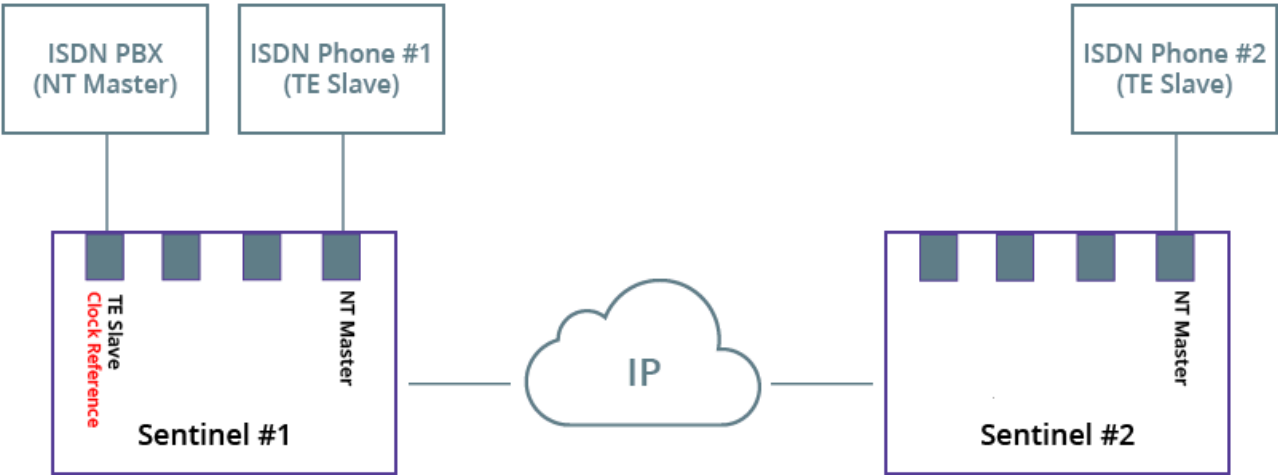
7.6.1.3 Current Clock Reference

The Mediatrix unit selects the interface that is effectively used as clock reference in the following way:

- Only a clock SLAVE interface can be used as clock reference.
- If there is a configured preferred clock reference interface, this interface becomes the clock reference as soon as it is UP (and running in SLAVE mode).
- If the preferred clock reference interface is DOWN or if there is no configured preferred clock reference interface, the first clock SLAVE interface to become UP becomes the clock reference.
- If no clock SLAVE interface is UP, there is no clock reference and the unit uses its own internally-generated clock signal.

7.6.1.4 IP Connection Between ISDN Networks

When using Mediatrix units to connect different ISDN networks through IP, each ISDN network runs on its own clock because there is no way to share the clock signal between the networks. Therefore, VoIP calls between different ISDN networks always experience periodical frame slips, which result in periodical packet losses, or measured bit error rates.



7.6.1.5 Mediatrix Unit Clock Synchronization

An ISDN network will be reliable when all endpoint clocks are synchronized correctly. When endpoints are not synchronized, they each run on their own internally-generated clock signals (free-running). The following are acceptable clock signal deviations from the reference specified clock frequency in ppm (parts-per-million).

Recommendation	Interface	Acceptable deviation
ITU-T I.430	Basic Rate (BRI)	100 ppm
ITU-T I.431	Primary Rate (PRI)	50 ppm

Mediatrix units are tested and certified against these specifications, and are guaranteed to follow the specified clock signal accuracy.

When endpoints are not synchronized, the clock signals are obviously not running at the exact same frequency, because of normal hardware deviations. The clock signals therefore gradually drift away from each other and a periodical frame slip happens

With respect to the specified accepted deviations, the worst case frame slip rates are calculated as follows:

Interface	Acceptable deviation	Worst case difference between endpoints	Frame slip rate
Basic Rate (BRI)	100 ppm for each endpoint on a link	200 ppm	2E-4 (one slip every 5000 frames)
Primary Rate (PRI)	50 ppm for each endpoint on a link	100 ppm	1E-4 (one slip every 10000 frames)

7.6.1.6 Direct ISDN Connection Between Endpoints

It is important to configure each endpoint appropriately so the clock signal is synchronized correctly with the rest of the network. The following table shows the different endpoint clock mode combinations and the associated behaviour.

Endpoint 1 \ Endpoint 2	Master	Slave
Master	- Endpoints are not synchronized. - Connection experiences frame slips and potentially loses data.	Endpoints are synchronized.
Slave	Endpoints are synchronised.	Connection MAY be established but is unreliable due to synchronization loop.

7.6.1.7 TDM Sync Feature

The TDM Sync feature provides a means to synchronise the operation of T1/E1/BRI circuits spanning across multiple units and to specify which port of a unit should be used as the reference.

All ISDN ports must be synchronised. When using one device, it is possible to specify a "source" port for the clock on which the other ports can be synchronised on. With several devices, the ports of the different units can also be synchronised. Therefore, it is very helpful to have a special TDM Sync port, with the clock, which can be shared between the devices.

Bad synchronisation can cause, for example:

- Choppy video communications
- Failure of fax transmissions
- Lost of audio frames

The Sync signal transferred between units is an 8 KHz Frame Sync Pulse.

7.7 Services

7.7.1 Basic ISDN Services Concepts

7.7.1.1 Analog/Digital Link Down Call Flow

Time	200.10.10.254	192.168.0.10	Comment
55.630048	INVITE SDP (g711U g729 g711A CN)		SIP From: <sip:18005554444@192.168.0.10 To:<sip:18883330001@192.168.0.10
55.658573	503 Service Unavailable		SIP Status
55.676320	ACK		SIP Request

7.7.2 Basic ISDN Services Tasks

7.7.2.1 Enabling ISDN Supplementary Services

Steps

- 1) Go to **ISDN/Services**.
- 2) From the **Select Interface** drop-down, select the interface for which you wish to enable ISDN optional services.
- 3) In the **Services Configuration** table, enable the required ISDN options.

Note: To activate the ISDN hold feature, the **Default Hook Flash Processing** must be set to **Using Signaling Protocol** (Under**Telephony/Services**).

Note: For the Date/Time IE to be sent, the SNTP server must be configured (Under **Network/Host**).

Note: The AOC features are not available in the NI2 and QSIG signaling protocols. Refer to [Configuring the E1T1 Interface \(PRI\)](#) (p.226) to configure the signaling protocol.

Note: To enable AOC support on the ISDN interface, the **Facility Services** parameter and **AOC-E (End-of-Call)** or **AOC-D (During the Call)** parameter must be set to **Enable**. Since the AOC from ISDN

interface to SIP is currently not supported, enabling the AOC on an ISDN interface configured as TE (user side) is only meaningful when using hair-pinning.

Note: The **Call Rerouting Behavior** parameter is not available in the NI2 and QSIG signaling protocols. Refer to [Configuring the E1T1 Interface \(PRI\)](#) (p.226) to configure the signaling protocol.

- 4) Click **Apply**.

7.7.2.2 Enabling the Network Traffic Control (NTC) Service

Steps

- 1) Go to **System/Services**.

Note: Starting the NTC service enables Traffic Shaping even if bandwidth limitation is disabled.

Note: The NTC service sends packets on the physical link according to their respective priorities. The lower the value, the higher the priority. Packets with lower priority are dropped first.

- 2) In the **User Service** table, click  located on the same line as Network Traffic Control (NTC).

Result

The Network Traffic control (NTC) line will turn to blue, and the **Status** field will indicate **Started**.

7.8 Other Advanced ISDN Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

Interop Play Local Ringback When No MediaStream

Configure the **isdn.InteropPlayLocalRingbackWhenNoMediaStream** parameter to set how to play the local ringback when there is no stream. For more details, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

7.8.1 Definitions

Term	Description
BRI	Basic Rate Interface
E1	European PRI digital signal carrier. 32 channels (30 voice channels + synchronization and signaling)
ISDN	Integrated Services Digital Network
NT	Network Termination. The endpoint on the telephone switch side.
PRI	Primary Rate Interface
T1	North-American PRI digital signal carrier. 24 channels (23 voice + 1 signaling)
TE	Terminal Equipment, the endpoint on the customer side

7.8.2 BRI Configuration

7.8.2.1 Important BRI Settings



Caution: The Mediatrix unit BRI ports can be used as a S or T reference point, but not as U reference points (2-wire). Never connect a U SCN line or a U TE into the Mediatrix unit BRI ports. If you are using an S-BUS, you can simultaneously connect only one unit in NT mode and up to 7 units in TE mode.

Endpoint Type

- Values used for the Mediatrix unit must be opposite to the value used for the PBX. For instance, if the PBX is set to TE, then the Mediatrix unit must be set to NT.
- When the BRI interface **Signaling Protocol** is set to QSIG, the endpoint type is only used in the second layer (LAPD) since it is a concept that does not exist in QSIG.
- To use a specific interface as the clock reference, this parameter must be set to TE.

Clock Mode

- **Auto** should be the value to use.
- In a BRI configuration, setting the clock mode to slave for a NT endpoint can be set for interop usage, while setting the clock mode to master for a TE endpoint is invalid (slave mode is automatically applied in this case). For more information on Clock Synchronisation, refer to the

[Technical Bulletin -Mediatrix Gateways and ISDN Synchronisation](#) and [Technical Bulletin - Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).

Monitor Link State Parameter

When enabled with the **Ignore OPTIONS on no usable endpoints** also enabled under the **SIP/Interop** page, this will influence how the SIP options are answered.

Connection Type

Depends on the equipment to which the Mediatrix unit port is connected to and it must be the same for all interconnected pieces of equipment.

Signaling Protocol

Must match the connected ISDN equipment or network.

Preferred Encoding Scheme

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

Fallback Encoding Scheme

Only valid when receiving a SETUP message. The user sending the SETUP message does not indicate alternative bearer capability.

Calling Name Max Length

The value for calls from SIP to ISDN ranges from 0 to 82.

Exclusive B-Channel Selection

When the parameter is enabled only the requested B channel is accepted when a call is initiated ; if the requested B channel is not available, the call is cleared.

Hook-Flash Keypad

- Set the actual keypad string that is to be considered as a hook-flash in the Hook-Flash Keypad field.
- An ISDN telephone may send INFORMATION messages that contain a "Keypad Facility". You can thus trigger a supplementary service (Hold, Conference, etc.) by sending a keypad facility.
- Since the keypads can be received via several INFORMATION messages, they are accumulated until they match or reset if the keypad reception timeout (second) has elapsed since the last keypad has been received. The keypad reception timeout can only be modified via SNMP. If the keypad reception timeout is set to 0, it disables the timeout, thus assuming that all keypads will be received in a single INFORMATION message.
- Setting this parameter to an empty string disables the hook-flash detection.
- The permitted keypad must be made up of IA5 characters. See ITU-T Recommendation T.50.

Accepted Progress Causes and Accepted Status Causes

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

TEI Negotiation

Only applies on Point to Multipoint connections.

Interface Configuration

Call properties set in the Call Router have precedence over the default values of the **Interface Configuration** table. For more details on the Call Router, refer to the [DGW Configuration Guide - Call Router user guide](#) published on the [Media5 Documentation Portal](#).

7.8.2.2 Configuring the BRI Interface

Before you start

Always use the Auto-sensing feature to automatically detect and to automatically configure your PRI interface. Use the [Auto-Detecting and Auto-Configuring ISDN Interfaces](#) (p.200) procedure first. The manual configuration of the BRI interface should be used for fine tuning of the configuration.

Information

It is important to take into consideration the following information:

- **Endpoint Type:** Values used for the Mediatrix unit must be opposite to the value used for the PBX. For instance, if the PBX is set to TE, then the Mediatrix unit must be set to NT. When the BRI interface **Signaling Protocol** is set to QSIG, the endpoint type is only used in the second layer (LAPD) since it is a concept that does not exist in QSIG. NOTE: To use a specific interface as the clock reference, this parameter must be set to TE. For more information on Clock Synchronisation, refer to the [Technical Bulletin - Mediatrix Gateways and ISDN Synchronisation](#) and [Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).
- **Preferred Encoding Scheme:** Only G.711 u-Law and G.711 a-Law codecs are allowed. G.711 u-Law may not be supported by DSS1 NT and TE endpoints. It is recommended to use G.711 a-Law as preferred encoding protocol.
- **Fallback Encoding Scheme:** Only G.711 u-Law and G.711 a-Law codecs are supported. Only valid when receiving a SETUP message. The user sending the SETUP message does not indicate alternative bearer capability.
- **Clock Mode:** "Auto" should be the value to use. In a BRI configuration, setting the clock mode to slave for a NT endpoint can be set for interop usage, while setting the clock mode to master for a TE endpoint is invalid (slave mode is automatically applied in this case). For more information on Clock Synchronisation, refer to the [Technical Bulletin - Mediatrix Gateways and ISDN Synchronisation](#) and [Technical Bulletin - Synchronising Unit Operation \(TDM Sync\)](#) published on the [Media5 Documentation Portal](#).
- **Calling Name Max Length:** The value for calls from SIP to ISDN ranges from 0 to 82.
- **Exclusive B-Channel Selection:** When the parameter is enabled only the requested B channel is accepted when a call is initiated; if the requested B channel is not available, the call is cleared.
- **Monitor Link State Parameter:** When enabled with the **Ignore OPTIONS on no usable endpoints** also enabled under the **SIP/Interop** page, this will influence how the SIP options are answered.
- **Connection Type:** depends on the equipment to which the Mediatrix unit port is connected to and it must be the same for all interconnected pieces of equipment.
- **Signaling Protocol:** Must match the connected ISDN equipment or network.

- **TEI Negotiation** : Only applies on Point to Multipoint connections.
- Call properties set in the Call Router have precedence over the default values of the **Interface Configuration** table. For more details on the Call Router, refer to the [DGW Configuration Guide - Call Router user guide](#) published on the [Media5 Documentation Portal](#).
- In strings, the space character is ignored and duplicating causes is not allowed.
- Some ISDN switches may require that the Sending Complete information element be included in the outgoing SETUP message to indicate that the entire number is included and there are no further destination digits to be sent.
- An ISDN telephone may send INFORMATION messages that contain a “Keypad Facility”. You can thus trigger a supplementary service (Hold, Conference, etc.) by sending a keypad facility. Since the keypads can be received via several INFORMATION messages, they are accumulated until they match or reset if the keypad reception timeout (second) has elapsed since the last keypad has been received. The keypad reception timeout can only be modified via SNMP. If the keypad reception timeout is set to 0, it disables the timeout, thus assuming that all keypads will be received in a single INFORMATION message

Steps

- 1) Use the [Auto-Detecting and Auto-Configuring ISDN Interfaces](#) (p.200) procedure first.
- 2) Go to **ISDN/Basic Rate Interface**.
- 3) From the **Select Interface** drop-box, select the BRI interface you wish to modify.

Note: Depending on the Mediatrix model, there may be several interfaces. To configure more than one interface at a time, use the **Apply To The Following Interfaces** table.

- 4) Make all required changes to the displayed parameters.
- 5) Click **Apply**.

7.8.3 Auto-Detecting and Auto-Configuring ISDN Interfaces

Information

Note: Some parameters cannot be auto configured. For example, the clock mode is configured according to the endpoint type, master for NT and slave for TE.

Steps

- 1) Go to **ISDN/Status**.
- 2) In the **Automatic Configuration** table, from the selection list, choose the interface you wish to auto configure or select all interfaces.
- 3) Click **Start Sensing**.

Note: Launching the Automatic Configuration may terminate abruptly all ongoing ISDN calls. The auto-configuration may take some time to complete and some of the current ISDN configuration settings might be replaced by new values.

Result

Under **ISDN/Status**, the **Physical Link** and **Signaling** fields of each interface should indicate **Up**.

Automatic Configuration	
Status:	--- All --- ▼ Start Sensing
Last Result:	None

Slot5/BRI1 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI2 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI3 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

Slot5/BRI4 [Configure]	
Physical Link: Up	
Signaling: Up	
Bearer Group	
Channel 1: Idle	Channel 2: Idle

7.8.4 Advanced Tasks

7.8.4.1 Enabling ISDN Supplementary Services

Steps

- 1) Go to **ISDN/Services**.
- 2) From the **Select Interface** drop-down, select the interface for which you wish to enable ISDN optional services.

- 3) In the **Services Configuration** table, enable the required ISDN options.

Note: To activate the ISDN hold feature, the **Default Hook Flash Processing** must be set to **Using Signaling Protocol** (Under **Telephony/Services**).

Note: For the Date/Time IE to be sent, the SNTP server must be configured (Under **Network/Host**).

Note: The AOC features are not available in the NI2 and QSIG signaling protocols. Refer to [Configuring the E1T1 Interface \(PRI\)](#) (p.226) to configure the signaling protocol.

Note: To enable AOC support on the ISDN interface, the **Facility Services** parameter and **AOC-E (End-of-Call)** or **AOC-D (During the Call)** parameter must be set to **Enable**. Since the AOC from ISDN interface to SIP is currently not supported, enabling the AOC on an ISDN interface configured as TE (user side) is only meaningful when using hair-pinning.

Note: The **Call Rerouting Behavior** parameter is not available in the NI2 and QSIG signaling protocols. Refer to [Configuring the E1T1 Interface \(PRI\)](#) (p.226) to configure the signaling protocol.

- 4) Click **Apply**.

7.8.4.2 Configuring Interop Parameters

Information

Interop parameters can be configured for PRI and BRI interfaces.

Steps

- 1) Go to **ISDN/Interop**.
- 2) From the **Select Interface** drop down, choose the interface for which you wish to configure the interop parameters.

Note: To select more than one interface at a time, if available on the unit, use the **Apply To The Following Interfaces** table.

- 3) In the **Interface Configuration** table, complete the fields as required.
- 4) Click **Apply**.

7.8.4.3 Modifying Port Pinout

Steps

- 1) Go to **ISDN/Primary Rate Interface**.

Note: Not all PRI and/or BRI platforms support Port Pinout.

- 2) In the **Interface Configuration** table, set the **Port Pinout** to reflect your configuration.

Result

Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	NT ▼
Clock Mode:	Master ▼
Port Pinout:	NT ▼
Monitor Link State:	Auto ▼
Line Coding:	TE ▼
	NT ▼

7.8.4.4 Exporting a Preset Configuration File

Before you start

If you are using a user-defined preset configuration file, do not forget to upload it through the file management system.

Steps

- 1) Go to **ISDN/Status**.
- 2) In the **ISDN Preset Configuration** table, in the **Preset Name** field, enter the name for the exported preset configuration file.

Note: We strongly recommend indicating the type of unit and date of export as the name of the preset configuration file. For example: MTXC740_20230215.

- 3) Click **Save**.

Result

ISDN Preset Configuration	
Local Preset:	--- Suggestion --- ▼ Apply
Preset Name:	MTX_XXX_yymmdd.cfg Save

The preset configuration file will be displayed under **Management/File**, in the **Internal files** table.

7.8.4.5 Other Advanced ISDN Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

Interop Play Local Ringback When No MediaStream

Configure the **isdn.InteropPlayLocalRingbackWhenNoMediaStream** parameter to set how to play the local ringback when there is no stream. For more details, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

7.8.5 Cabling Information

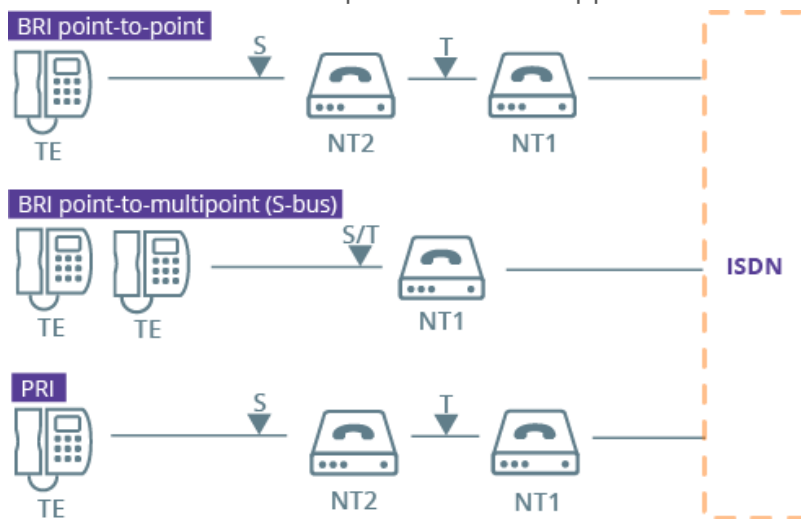
7.8.5.1 ISDN Reference Points

ISDN specifies a number of reference points that define logical interfaces between the various equipment types on an ISDN access line.

The Mediatrix unit supports the following ISDN reference points:

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

All other ISDN reference points are not supported.



7.8.5.2 BRI S/T Connection (RJ-48)



Caution: Always use standard telecommunication cables with a minimum of 26 AWG wire gauge.

BRI S/T connections use two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 3 and 6 are on one twisted pair and pins 4 and 5 are on a second pair according to common wiring standards which meet the TIA/EIA 568A and 568B requirements.



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



Pin#	TE mode	NT mode
1	Not Connected	Not Connected
2	Not Connected	Not Connected
3	Tx +	Rx +
4	Rx +	Tx +
5	Rx -	Tx -
6	Tx -	Rx -
7	Not connected	Not Connected
8	Not connected	Not Connected

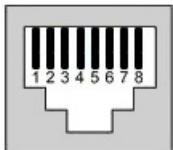
7.8.5.3 PRI Connection (RJ-48)



Caution: Always use standard telecommunication cables with a minimum of 26 AWG wire gauge.

PRI connections use two pairs of wires: one pair for transmission and the second pair for reception. It is wired so that pins 1 and 2 are on one twisted pair and pins 4 and 5 are on a second pair according to common wiring standards which meet the TIA/EIA 568A and 568B requirements.

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



Pin #	NT Mode	TE Mode
1	Transmit #2 (+)	Receive #2 (+)
2	Transmit #1 (-)	Receive #1 (-)
3	Not connected	Not connected
4	Receive #2 (+)	Transmit #2 (+)
5	Receive #1 (-)	Transmit #1 (-)
6	Not connected	Not connected
7	Not connected	Not connected
8	Not connected	Not connected

8 R2 CAS

8.1 Status

8.1.1 Basic R2 Concepts

8.1.1.1 R2 Auto-Configuration

The R2 Auto-configuration feature allows the detection and the configuration of a specific or of all R2 interfaces so that the R2 link goes up and becomes usable with a minimal user interaction.

When launching an auto-configuration process, it stops automatically when all selected interfaces have been tested. For each interface, the auto-configuration process is considered successful when the link becomes up or a failure when all combinations have been tried without having a link up.

During R2 Auto-Configuration, the following parameters are updated:

- PortPinout : TE / NT
- ClockMode : MASTER / SLAVE
- LineCoding : AMI / HDB3
- LineFraming : CRC4 / NOCRC4

8.1.1.2 R2 Preset Configurations

It is possible to save a set of configurations as presets for future R2 connections.

These preset files are located in the file system's persistent memory. They differ depending on the Mediatrix unit you are using. Using preset files is especially useful for units that do not use the default values provided by Media5.

Note: Only script files can be used as R2 Preset configuration.

It is also possible to export the current R2 configuration in a preset.

Note: User-defined preset files are not kept in the event of a factory reset.

Installed configuration scripts/images are listed in the DGW Web interface, under **Management/File**.

8.1.2 R2 Basic Tasks

8.1.2.1 Auto-Configuring R2 Interfaces

Information

Launching the auto-configuration may terminate abruptly all ongoing R2 calls.

Steps

- 1) Go to **R2/Status**.
- 2) In the **Automatic Configuration** table, from the selection list, choose the interfaces to auto-configure.
- 3) Click **Start Sensing**.

Result

Auto-configuration on all R2 interfaces may take some time to complete. Some of the current R2 settings might be replaced by new values.

Automatic Configuration	
Status:	--- All --- ▼ Start Sensing
Last Result:	None

8.1.2.2 Using an R2 Preset Configuration

Information

Remember that the Preset configuration must first be imported in the file management system under **Management/File**.

Steps

- 1) Go to **R2/Status**.
- 2) In the **R2 Preset Configuration** table, from the **Suggestion** list, choose the Preset to apply.
- 3) Click **Apply**.

Result

The values of the parameters included in the R2 Preset configuration will be applied to the Mediatrix unit.

R2 Preset Configuration		
Local Preset:	--- Suggestion ---	Apply
Preset Name:		Save

8.1.2.3 Saving an R2 Preset Configuration

Information

It is a best practice to export the R2 configuration before performing a factory reset or a partial reset, as user-defined presets are deleted.

Steps

- 1) Go to **R2/Status**.
- 2) In the **Preset Name** field, enter the name of the R2 configuration you wish to save.
- 3) Click **Save**.

Result

The R2 configuration will be exported and available under **Management/File**. The file will also be available under the **Suggestion** list.

R2 Preset Configuration		
Local Preset:	--- Suggestion ---	Apply
Preset Name:		Save

8.2 R2 Configuration

8.2.1 Basic R2 Configuration Concepts

8.2.1.1 Channel Associated Signaling (CAS)

The Channel Associated Signaling (CAS) is a method of signalling where each traffic channel has a dedicated signaling channel.

In other words, the signalling for a particular traffic circuit is permanently associated with that circuit. Channel-associated call-control is still widely used today, mostly in South America, Africa, Australia, and in Europe. The Mediatrix unit uses the MFC/R2 CAS protocol. This is a compelled sequence multi-frequency code signaling. MFC/R2 can be used on international as well as national connections. In MFC/R2 signaling, the equipment units at the exchanges that send and receive digits, and the

signaling between these units, are usually referred to as register and interregister signalling. The terms forwards and backwards are heavily used in descriptions of MFC/R2.

- Forwards is the direction from the calling party to the called party.
- Backwards is the direction from the called party to the calling party.

8.2.1.2 Line Signals for the Digital Version of MFC/R2

The MFC/R2 digital line signals (defined in ITU-T Q.421) are the ABCD bits of CAS in timeslot 16 of an E1.

They represent the states of the line, and are similar to the states of an analog line. In general, only bits A and B are used. In most systems, bits C and D are set to fixed values and never change. There are some national variants where bit C or D may be used for metering pulses.

8.2.1.3 Interregister Signals

The interregister, or interswitch, signals in MFC/R2 signaling (defined in ITU-T Q.441) are encoded as the presence of 2, and only 2, out of 6 specific tones, spaced at 120 Hz intervals.

Two sets of tones are defined:

- one for forward signals
- one for backward signals

There are 15 combinations of 2 out of 6 tones i.e.:

- 10 signals for the digits 0 to 9
- additional signals available for supervisory purposes

MFC/R2 uses a separate set of frequencies for the forward and backwards directions. The interregister signals are sent in-band. They may pass transparently through several nodes in the network between the two terminating switches. The signals are arranged in groups. When a call begins, the calling end uses group I signals, and the called end uses group A. The called end may tell the calling end to switch to using group II and group B signals, or to switch back to group A. In some countries, there are also groups III and C, used for caller number transfer. Groups III and C do not exist in the ITU specifications. MFC/R2 uses a system called compelled signaling. To ensure the sending end never sends signals too fast, each signal from the sending end results in an acknowledgement from the receiving end. The sending end is instructed signal by signal what it should send next – a dialed digit, a digit of caller ID, etc.

For more details refer to the <https://www.itu.int/rec/T-REC-Q.400-Q.490-198811-I>

8.2.2 Basic R2 Configuration Tasks

8.2.2.1 Configuring R2 CAS Parameters

Steps

- 1) Go to **R2/R2 Config**.
- 2) **Note:** The number of available interfaces depends on the Mediatrix unit model.
- 3) In the **Interface Configuration** configure the fields as required.

Result

Interface Configuration	
Clock Mode:	Slave ▼
Port Pinout:	Auto ▼
Monitor Link State:	Enable ▼
Line Coding:	HDB3 ▼
Line Framing:	CRC4 ▼
Channel Range:	1-30
Channel Allocation Strategy:	Ascending ▼
Maximum Active Calls:	0
Encoding Scheme:	G.711 a-Law ▼
Line Signaling Protocol:	Q.421 2 Bits Signaling ▼
Incoming Digit Signaling:	MFC/R2 ▼
Outgoing Digit Signaling:	MFC/R2 ▼
Country Selection:	BrazilR2 ▼
Digit Attenuation:	0

8.3 Advanced R2 Tasks

8.3.1 Overriding Country Default R2 Signaling Variants

Steps

- 1) Go to **R2/Signaling**.
- 2) From the **Select Interface** selection list, choose an interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **Country** table, from the **Override Default Country Settings** selection list, choose **Enable**.
- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection** field. To get the appropriate values of the selected country, you must reset the table values first.

- 5) When prompted to, restart required services.
- 6) In the **R2 Signaling Variants**, complete the fields as required.
- 7) Click **Apply**.
- 8) Again, when prompted to, restart required services.

Result

Country	
Country Selection:	BrazilR2
Override Default Country Settings:	Enable ▾

R2 Signaling Variants	
Parameters	Value
Bits CD:	1
ANI Length:	0
DNIS Length:	0
ANI Request:	Enable ▾
Send ANI request after nth DNIS Digits:	0
Collect Call Blocked:	Enable ▾
ANI Category:	Nat Subscriber NoPrio ▾
Line Free Category:	Line Free Charge ▾
ANI Restricted:	Enable ▾
Incoming Decline Method:	Release ▾

8.3.2 Overriding Country Default R2 Timers Variants

Before you start

Modifying the default values of the Timers Variants should be performed by qualified technicians unless you are an expert in R2 CAS protocol.

Steps

- 1) Go to **R2/Timers**.
- 2) From the **Select Interface** selection list, choose an interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **Country** table, from the **Override Default Country Settings** selection list, choose **Enable**.

- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) When prompted to, restart required services.
- 6) In the **R2 Timers Variants**, complete the fields as required.

Note: Changing a timeout value could require to adjust other timeout values in R2 Timers Variants and R2 Digit Timers Variants. Refer to the parameter description for more details.

- 7) Click **Apply**.
- 8) Again, when prompted to, restart required services.

Result

Country		
Country Selection:	BrazilR2	
Override Default Country Settings:	Enable Disable	

R2 Timers Variants		
Parameters	Value	
Seizure Ack Timeout:	2000	
Fault Seizure Ack Timeout:	60000	
Double Seizure Timeout:	100	
Double Answer Timeout:	1500	
Answer Timeout:	0	
ReAnswer Timeout:	1000	
Release Guard Timeout:	100	
InterCall Guard Timeout:	100	
Congestion Tone Guard Timeout:	1000	
Unblocking Timeout:	100	
Address Complete Timeout:	8000	
Wait Answer Timeout:	60000	
Digit Complete Timeout:	4000	
Wait GroupB Response Complete Timeout:	3000	
Wait Immediate Response Complete Timeout:	1000	
Play Tone Guard Timeout:	70	
Accept Call Timeout:	2000	
Clear Forward Guard Timeout:	1500	
Clear Backward Guard Timeout:	1500	
Fault On Answered Guard Timeout:	250	
Fault On Clear Backward Guard Timeout:	250	
Fault On Seize Ack Guard Timeout:	250	
Fault On Seize Guard Timeout:	250	
Decline Guard Timeout:	1500	
No Digit Timeout:	0	

8.3.3 Overriding Country Default R2 Digit Timers Variants

Before you start

Modifying the default values of the Digit Timers Variants should be performed by qualified technicians unless you are an expert in R2 CAS protocol.

Steps

- 1) Go to **R2/Digit Timers**. media5corp.com

- 2) From the **Select Interface** selection list, choose an interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **Country** table, from the **Override Default Country Settings** selection list, choose **Enable**.

- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **R2 Digit Timers Variants**, complete the fields as required.

Note: Changing a timeout value could require to adjust other timeout values in R2 Timers Variants and R2 Digit Timers Variants. Refer to the parameter description for more details.

- 6) Click **Apply**.

Result

For example:

Country		
Country Selection:	BrazilR2	
Override Default Country Settings:	Enable	

R2 Digit Timers Variants		
Parameters	Value	
MFC Pulse Inter Digit Timeout:	100	
MFC Pulse Min On Timeout:	150	
MFC Max Sequence Timeout:	10000	
MFC Max On Timeout:	5000	
MFC Max Off Timeout:	5000	
MF Congestion Tone Duration:	0	

8.3.4 Overriding Country Default Link Timers Variants

Steps

- 1) Go to **R2/Link Timers**.

- 2) From the **Select Interface** selection list, choose an interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **Country** table, from the **Override Default Country Settings** selection list, choose **Enable**.
- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **R2 Link Timers Variants**, complete the fields as required.
- 6) Click **Apply**.

Result

Country	
Country Selection:	BrazilR2
Override Default Country Settings:	Enable v

R2 Link Timers Variants	
Parameters	Value
Link Activation Timeout:	1000
Link Activation Retry Timeout:	3000

8.3.5 Overriding Country Default Tone Variants

Steps

- 1) Go to **R2/Tones**.
 - 2) From the **Select Interface** selection list, choose an interface.
- Note:** The number of available interfaces depends on the Mediatrix unit model.
- 3) In the **Country** table, from the **Override Default Country Settings** selection list, choose **Enable**.
 - 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) When prompted to, restart required services.

- 6) In the **R2 Tones Backward Groups** and **R2 Tones Forward Groups**, complete the fields as required.

Note: For more details on Forward tones/groups and Backward tones/groups, refer to the [Interregister Signals](#) (p.251) section.

- 7) Click **Apply**.
- 8) Again, when prompted to, restart required services.

Result

Country		
Country Selection:	BrazilR2	
Override Default Country Settings:	Enable ▾	

R2 Tones Forward Groups	Value	
End of DNIS Tone:	I15 ▾	
End of ANI Tone:	I15 ▾	
Restricted ANI Tone:	I12 ▾	

R2 Tones Backward Groups	Value	
Send Next DNIS Digit Tone:	A15 ▾	
Send Previous DNIS Digit Tone:	A15 ▾	
Switch to Group II Tone:	A15 ▾	
Network Congestion Tone:	A15 ▾	
Send Calling Party Category Tone:	A15 ▾	
Immediate Accept Tone:	A15 ▾	
Send DNIS Digit N-2 Tone:	A15 ▾	
Send DNIS Digit N-3 Tone:	A15 ▾	
Repeat all DNIS Tone:	A15 ▾	
Send Next ANI Digit Tone:	A15 ▾	
Send Calling Party Category Tone switch to Group C:	A15 ▾	
Send Special Information Tone:	B15 ▾	
User Busy Tone:	B15 ▾	
Network Congestion Tone:	B15 ▾	
Unassigned Number Tone:	B15 ▾	
Line Free with Charge Tone:	B15 ▾	
Line Free with Charge Tone (Supplementary):	B15 ▾	
Line Free without Charge Tone:	B15 ▾	
Line Out of Order Tone:	B15 ▾	
Changed Number Tone:	B15 ▾	
Send Next ANI Digit Tone:	C15 ▾	
Repeat all DNIS Tone switch to Group A:	C15 ▾	
Send Next DNIS Digit Tone switch to Group A:	C15 ▾	
Network Congestion Tone:	C15 ▾	
Send Previous DNIS Digit Tone switch to Group A:	C15 ▾	
Switch to Group II Tone:	C15 ▾	

9 E and M CAS

9.1 Status

9.1.1 Basic E and M Concepts

9.1.1.1 E&M Auto-Configuration

The E&M Auto-configuration feature allows the detection and the configuration of all, or a specific, E&M interfaces so that the E&M link goes up and becomes usable with a minimal user interaction.

When launching an auto-configuration process, it stops automatically when all selected interfaces have been tested. For each interface, the auto-configuration process is considered a success when the link becomes up or a failure when all combinations have been tried without having a link up.

During E&M Auto-Configuration, the following parameters are updated:

- PortPinout : TE / NT
- ClockMode : MASTER / SLAVE
- LineCoding : B8ZS / AMI
- LineFraming : SF / ESF

9.1.1.2 E&M Preset Configurations

It is possible to save a set of configuration as presets for future E&M connections.

Using preset files is especially useful for units that do not use the default values provided by Media5. These preset configuration files are located in the file system's persistent memory listed in the DGW Web interface, under **Management/File** and they differ depending on the Mediatrix unit you are using.

Note: Only script files can be used as R2 Preset configuration.

It is also possible to export the current E&M configuration in a Preset Configuration file.

Note: User-defined presets are not kept in the event of a factory reset.

Installed configuration scripts/images are listed in the DGW Web interface, under **Management/File**

9.1.2 Basic E and M Tasks

9.1.2.1 Auto-Configuring E&M

Information

Launching auto-configuration may terminate abruptly all ongoing E&M calls.

Steps

- 1) Go to **E&M/Status**.
- 2) In the **Automatic Configuration** table, from the selection list, choose the interface to auto-configure.

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

- 3) Click **Start Sensing**.

Result

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

Automatic Configuration	
Status:	Slot1/E1T1 ▾ Start Sensing
Last Result:	None

9.1.2.2 Saving an E&M Preset Configuration

Steps

- 1) Go to **E&M/Status**.
- 2) In the **E&M Preset Configuration** table, in the **Preset Name** field, indicate the name of the Preset.
- 3) Click **Save**.

Result

The current E&M configuration is exported. to the File management system. The preset configuration will be available in the **Suggestion** selection list.

E&M Preset Configuration	
Local Preset:	--- Suggestion --- ▼ Apply
Preset Name:	Eam_Preset_Config_Name Save

9.1.2.3 Using an E&M Preset Configuration

Steps

- 1) Go to **E&M/Status**.
- 2) In the **E&M Preset Configuration** table, from the **Local Preset** selection list, choose the configuration file to apply.
- 3) Click **Apply**.

Result

The selected configuration is applied

E&M Preset Configuration	
Local Preset:	--- Suggestion --- ▼ Apply
Preset Name:	Save

9.2 E and M Config

9.2.1 Basic E and M Config Concepts

9.2.1.1 Channel Associated Signaling (CAS)

When using CAS signaling, each traffic channel has a dedicated signaling channel. In other words, the signaling for a particular traffic circuit is permanently associated with that circuit.

E&M (earth & magneto, or ear & mouth) is a type of CAS signalling that defines line signaling and register signaling. It is also called Signalling System R1 and is mainly used in North America. E&M was originally developed to allow PABXs in different geographic locations to communicate over an analog private circuit. Some digital interfaces such as CAS also use versions of E&M signaling.

The terms forwards and backwards are heavily used in descriptions of E&M.

- Forwards is the direction from the calling party to the called party.
- Backwards is the direction from the called party to the calling party.

9.2.2 Basic E and M Config Tasks

9.2.2.1 Configuring E&M CAS Parameters

Steps

- 1) Go to **E&M/E&M Configuration**.
- 2) From the **Select Interface** selection list, choose an E&M interface.

Note: The number of available interfaces depends on the Mediatrix unit model.
- 3) In the **Interface Configuration** table, configure the fields as required.
- 4) Click **Apply**

Result

Interface Configuration		
Clock Mode:	Slave	▼
Port Pinout:	Auto	▼
Monitor Link State:	Enable	▼
Line Coding:	B8ZS	▼
Line Framing:	ESF	▼
Channel Range:	1-24	
Channel Allocation Strategy:	Ascending	▼
Maximum Active Calls:	0	
Encoding Scheme:	G.711 a-Law	▼
E&M Signaling Type Selection:	Wink Start	▼
Digit Attenuation:	0	

9.3 Advanced E and M Configuration Tasks

9.3.1 Overriding Country Default E&M Signaling Variants

Information

Overriding the default settings is considered an advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

Steps

- 1) Go to **E&M/Signaling**.
- 2) From the **Select Interface** selection list, choose an E & M interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **E&M Signaling Type** table, from the **Override Default Signaling Settings** selection list, choose **Enable**.
- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **E&M Signaling Variants** table, complete the fields as required.

- 6) Click **Apply**.

Result

This is an example of configuration.

E&M Signaling Type	
E&M Signaling Type Selection:	Wink Start
Override Default Signaling Settings:	Enable ▾

E&M Signaling Variants	
Parameters	Value
Bits BCD:	8
ANI Length:	0
DNIS Length:	0
Incoming Register Signaling:	DTMF ▾
Outgoing Register Signaling:	DTMF ▾
Incoming Dial Map:	%dnis%t
Outgoing Dial Map:	%dnis%t
Wait Wink:	Enable ▾
Wait Wink Ack:	Disable ▾
Send Wink:	Enable ▾
Send Wink Ack:	Disable ▾

9.3.2 Overriding Country Default E&M Timers Variants

Information

Overriding the default settings is considered an advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

Steps

- 1) Go to **E&M/Timers**.
- 2) From the **Select Interface** selection list, choose an E & M interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **E&M Signaling Type** table, from the **Override Default Signaling Settings** selection list, choose **Enable**.

- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **E&M Timers Variants**, complete the fields as required.
- 6) Click **Apply**.

Result

This is an example of configuration.

E&M Signaling Type		
E&M Signaling Type Selection:	Wink Start	
Override Default Signaling Settings:	Enable Reset	

E&M Timers Variants		
Parameters	Value	
Backward Wait Pre Wink Timeout:	50	
Backward Send Wink Timeout:	200	
Backward Wait First Digit Timeout:	10000	
Backward Clear Backward Timeout:	2000	
Backward Digit Complete Timeout:	4000	
Forward Wait Wink Timeout:	5000	
Forward Wait Max Wink On Timeout:	5000	
Forward Wait Pre Dial Timeout:	140	
Forward Wait Answer Timeout:	180000	
Forward Clear Forward Timeout:	2000	
Release Guard Timeout:	200	

9.3.3 Overriding Country Default E&M Digit Timers Variants

Information

Overriding the default settings is considered an advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

Steps

- 1) Go to **E&M/Digit Timers**.

- 2) From the **Select Interface** selection list, choose an E & M interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **E&M Signaling Type** table, from the **Override Default Signaling Settings** selection list, choose **Enable**.
- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **E&M Digit Timers Variants**, complete the fields as required.
- 6) Click **Apply**.

Result

This is an example of configuration

E&M Signaling Type	
E&M Signaling Type Selection:	Wink Start
Override Default Signaling Settings:	Enable ▼

E&M Digit Timers Variants	
Parameters	Value
KP On Timeout:	100
KP Off Timeout:	68

9.3.4 Overriding Country Default E&M Link Timers Variants

Information

Overriding the default settings is considered an advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

Steps

- 1) Go to **E&M/Link Timers**.
- 2) From the **Select Interface** selection list, choose an E & M interface.

Note: The number of available interfaces depends on the Mediatrix unit model.

- 3) In the **E&M Signaling Type** table, from the **Override Default Signaling Settings** selection list, choose **Enable**.

- 4) Click **Reset to Default** to update the values with the selected country.

Note: Once the **Override Default Country Settings** is enabled, the indicated values in the table are not from the specified country in the **Country Selection**. To get the appropriate values of the selected country, you must reset the table values first.

- 5) In the **E&M Link Timers Variants**, complete the fields as required.
- 6) Click **Apply**.

Result

This is an example of configuration.

E&M Signaling Type	
E&M Signaling Type Selection:	Wink Start
Override Default Signaling Settings:	Enable v

E&M Link Timers Variants	
Parameters	Value
Link Activation Timeout:	1000
Link Activation Retry Timeout:	3000

9.4 Advanced E&M CAS Parameters

The PRI statistics are available in the **Hardware.StatsInfo** table. To reset the statistics, you must set "ResetStats" in the **Hardware.StatsInfo.ResetStats** parameter.

10 SIP

10.1 Gateways

10.1.1 Basic Gateway Concepts

10.1.1.1 SIP Gateways

In the scope of this document and Mediatrix products in general, a "SIP gateway" is a software entity of the DGW application that ties the SIP communications to different network interfaces and listening ports. Not to be confused with a "VoIP gateway" which usually represents the whole gateway device.

A SIP gateway can be used to:

- Redirect ISDN calls to different SIP servers depending on the call.
- Hunt calls across several gateways.
- Terminate communication sessions between two or multiple parties.

There are two types of SIP gateways: trunk gateway and endpoint gateway. For more details on their difference, refer to [Trunk Gateway vs Endpoint Gateway](#) (p.271)

10.1.1.2 Important Information to Know before Using SIP Gateways

Limitations

- Adding a SIP gateway triggers a warning message if the total number of registrations configured reached the defined limit. Refer to [Number of Registrations](#) (p.283).
- The Mediatrix unit supports a maximum of 10 gateways.

IMPORTANT: Downgrading from a version supporting 10 gateways (introduced in DGW v.46.0) to an older version with a limit of 5, will erase gateways in excess of 5. After downgrade, the configuration will require verification.

Naming

Gateway names only support alphanumeric characters, "-", and "_".

Network Interfaces

- When a gateway is associated with a Network interface for signaling, it applies to all transport types (UDP, TCP, etc.).

- The LAN interface may be used by a SIP gateway to be bound on the LAN. However, there is no SIP to SIP routing between the LAN and the Uplink interface..

Port Use

If two or more SIP gateways use the same port, only the first SIP gateway starts correctly. The others are in error and not started. The SIP gateway is also in error and not started if the port is already used.

10.1.1.3 Trunk Gateway vs Endpoint Gateway

IMPORTANT: Gateways on a unit must be of the same type, i.e.. you cannot have trunk and endpoint gateways on the same unit. Using 2 types of gateways on the same unit may cause SIP messages to be misrouted.

Trunk Gateways	Endpoint Gateways
Operates like a traditional SIP gateway	Operation is inspired from the IMS (IP Multimedia Subsystem) model.
No concept of being connected to a SIP server at the SIP level.	- Establishes SIP connections to a SIP server based on the success of SIP registration. - SIP dialogs for a given SIP user can only be established once the user is registered to the server.
Accepts incoming SIP requests from peers on a listening port.	The gateway has no listening port. It accepts incoming SIP requests only from the server on which it is registered.
When the destination is an FQDN, each SIP transaction is possibly sent to a different IP address, depending on the DNS query result. The gateway assumes that all SIP servers identified by a single FQDN have a synchronised state.	The Endpoint Gateway is designed to operate with a destination specified by an FQDN. The addresses obtained from the DNS resolution of this FQDN are used as potential "SIP connection" addresses, in ordered priorities. The endpoint gateway first attempts to register to the highest priority server. If the SIP connection (registration) fails, the next priority server is tried, and so on. A failback scheme periodically attempts to switch to the server with the highest priority available. Failover/fallback to another server requires the SIP user to register on that server prior to establishing SIP communication.
Supports UDP, TCP, and TLS transport: - TLS connections are persistent - UDP and TCP connections are not persistent	Supports UDP, TCP, and TLS transport - Separate persistent connections are established for each user. - For UDP transport, the gateway simulates persistent connections.
SIP dialogs are established independently of each other (in some conditions, the selection of the destination server may depend on the keep alive parameters configured under SIP/Servers).	SIP dialogs for a given SIP user can only be established once the user is registered to the server.

Trunk Gateways	Endpoint Gateways
The call router shows a single SIP source/destination for the gateway.	The call router and gateway status tables show an instance of the gateway for each user of the gateway.
Supports endpoint, gateway, user, and unit registrations.	Supports endpoint registrations only.
Supports NAPTR DNS queries.	NAPTR DNS queries are not supported.

10.1.2 Basic Gateway Tasks

10.1.2.1 Creating a SIP Gateway on the LAN Network Interface

Information

IMPORTANT: The LAN interface may be used by a SIP gateway to be bound on the LAN. However, there is no routing between the LAN and the Uplink interface.

Steps

- 1) Go to **SIP/Gateways**.
- 2) In the **Gateway Configuration** table, in the **Name** field, enter the name of the new gateway (ex. gateway_lan).
- 3) Click **+**.
- 4) From the **Type** selection list, select the type of gateway used.

Note: In most scenarios, it is the Trunk gateway type that is used. For more details refer to [Trunk Gateway vs Endpoint Gateway](#) (p.271).

- 5) From the **Signaling Network** selection list, select **Lan1**
- 6) In the **Port** and **Secure Port** fields, enter the gateway listening port to use (ex. 5060) .

Note: The default value is 0, which means it will use Port 5060 and Secure Port 5061 . To have multiple gateways in the same Signaling Network, use different ports, for example Port 5062 and Secure Port 5063.

- 7) Click **Apply**.
- 8) Click **restart required services** located at the top of the page.

Result

The new gateway will be available under the **SIP/Servers** page.

10.1.2.2 Creating a SIP Gateway on the Uplink Network Interface

Steps

- 1) Go to **SIP/Gateways**.
- 2) In the **Gateway Configuration** table, in the **Name** field, enter the name of the new gateway. (ex. gateway_uplink)
- 3) Click **+**.
- 4) From the **Type** selection list, select the type of gateway used.

Note: In most scenarios, it is the Trunk gateway type that is used. For more details refer to [Trunk Gateway vs Endpoint Gateway](#) (p.271).

- 5) From the **Signaling Network** selection list, select **Uplink**.
- 6) In the **Port** and **Secure Port** fields, enter the gateway listening port to use (ex. 5060) .

Note: In the Port and Secure Port fields, enter the gateway listening ports to use. Default is 0, which means it will use Port 5060 and Secure Port 5061. To have multiple gateways in the same Signaling Network, use different ports, for example Port 5062 and Secure Port 5063).

- 7) Click **Apply**.
- 8) Click **restart required services** located at the top of the page.

Result

The new gateway will be available under the **SIP/Servers** page.

10.1.2.3 Modifying a SIP Gateway

Steps

- 1) Go to **SIP/Gateways**.
- 2) In the **Gateway Configuration** table, modify the fields of the gateway.
- 3) Click **Apply**.
- 4) Click **restart required services**.

Result

The changes will appear in the **Gateway Status** table.

10.1.2.4 Deleting a SIP Gateway

Steps

- 1) Go to **SIP/Gateways**.

- 2) In the **Gateway Configuration** table, click - next to the gateway to delete.
- 3) Click **Apply**.
- 4) Click **restart required services**, located at the top of the page.

Result

The Gateway will be removed from the **Gateway Status** table along with its configured parameters (e.g. servers, registrations), and any reference to this gateway would be invalid (e.g. from the Call Router or the Sbc service). Furthermore, error notifications and syslogs will be issued to indicate the inconsistencies found.

10.1.3 SIP Gateway Advanced Parameters

All SIP gateway parameters are configurable via the DGW Web Interface.

10.2 SIP Servers

10.2.1 Basic SIP Server Concepts

10.2.1.1 SIP Servers

SIP servers manage all SIP calls in the network, therefore they are the main component of an IP PBX system.

Depending on the environment and the needs of the SIP-based IP-PBX phone system, there are four types of SIP servers that can be used with the Mediatrix units.

- Registrar host: receives REGISTER requests and places the information in the location service for the domain it handles
- Messaging host: receives MWI SUBSCRIBE requests and places the information in the location service for the domain it handles.
- Proxy host: An entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. It is the final destination of the SIP requests.
- Outbound proxy host: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. It is an intermediate step before reaching the proxy host.

10.2.1.2 Important Information to Know Before Using SIP Servers

Servers

- The registrar and proxy SIP hosts must have one of the following formats:
 - IP address
 - IP address: port number, for example:192.168.0.5:5060
 - IP address: 0 where "0" indicates the default port 5060 or 5061 in secure mode.
 - FQDN
- If any of the SIP server parameters corresponds to a domain name that is bound to a SRV record, the corresponding port must be set to 0 for the unit to perform SRV type DNS requests (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather only use Type A requests because it does not need to be specified which port to use.
- All SIP servers identified by a single FQDN are considered by a trunk gateway as having a synchronised state.
- When the destination of a SIP server is an FQDN, each SIP transaction is possibly sent to a different IP address, depending on the DNS query result.
- The outbound SIP proxy server is enabled only if the IP address is valid (i.e., not 0.0.0.0:0). Setting the address to 0.0.0.0:0 or leaving the field empty disables the outbound proxy server.
- The outbound proxy address is never included in the SIP packets, it is only used as a physical network destination for the packets.

10.2.2 Basic SIP Server Tasks

10.2.2.1 Configuring the Default Registrar Host

Information

In some instances, the configuration of the default servers may already be completed.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Default Servers** table, in the **Registrar Host** field, indicate the server IP address or FQDN to use for all gateways.

Note: For example, 192.168.0.5:5060

- 3) In the **Proxy Host** field indicate the server IP address or FQDN to use for all gateways.
- 4) Click **Apply**.
- 5) Click **restart required services**, located at the top of the page.

Result

All gateways will use this registrar host, unless a gateway has been configured to specifically use another one in the **Registrar Servers** table, under **SIP/Servers**. Refer to [Assigning a Specific Registrar Host to a Gateway](#) (p.279).

Default Servers	
Registrar Host:	sip.registrarserver.com
Proxy Host:	sip.proxyserver.com
Messaging Server Host:	
Outbound Proxy Host:	

10.2.2.2 Configuring the Default Messaging Server Host

Information

In some instances, the configuration of the default servers may already be completed.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Default Servers** table, in the **Messaging Server Host** field, indicate the static IP address or domain name and port number.

Note: For example, 192.168.0.5:5060

- 3) In the **Proxy Host** field indicate the server IP address or FQDN to use for all gateways.
- 4) Click **Apply**.
- 5) Click **restart required services**, located at the top of the page.

Result

All gateways will use this messaging server host, unless a gateway has been configured to use another one in the **Messaging Servers** table under **SIP/Servers**. Refer to [Assigning a Specific Messaging Server Host to a Gateway](#) (p.279).

Default Servers		
Registrar Host:		
Proxy Host:	sip.proxyserver.com	
Messaging Server Host:	IP address or domainname:port number	
Outbound Proxy Host:		

10.2.2.3 Configuring the Default Proxy Host

Information

In some instances, the configuration of the default servers may already be completed.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Proxy Host** field indicate the server IP address or FQDN to use for all gateways.

Note: For example, 192.168.0.5:5060

- 3) Click **Apply**.
- 4) Click **restart required services**, located at the top of the page.

Result

All gateways will use this proxy host, unless a gateway has been configured to use another one in the **Proxy Servers** table, under **SIP/Servers**. Refer to [Assigning a Specific Proxy Host to a Gateway](#) (p.280).

Default Servers		
Registrar Host:		
Proxy Host:	sip.proxyserver.com	
Messaging Server Host:		
Outbound Proxy Host:		

10.2.2.4 Configuring the Default Outbound Proxy Host

Information

In some instances, the configuration of the default servers may already be completed.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Default Servers** table, in the **Proxy Host** field indicate the server IP address or FQDN to use for all gateways.
- 3) In the **Outbound Proxy Host** field, indicate the server IP address or FQDN to use for this gateway.
- 4) Click **Apply**.

- 5) Click **restart required services**, located at the top of the page.

Result

All gateways will use this outbound proxy host, unless the gateway has been configured to use another one in the **Proxy Servers** table, under **SIP/Servers**. Refer to [Assigning a Specific Outbound Proxy Host to a Gateway](#) (p.281).

Default Servers		
Registrar Host:		
Proxy Host:	sip.proxyserver.com	
Messaging Server Host:		
Outbound Proxy Host:	sip.outboundproxyserver.com	

10.2.2.5 Assigning a Specific Registrar Host to a Gateway

Before you start

You can assign a specific Registrar Server to the default gateway, or to a gateway you have created.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Registrar Servers** table, from the **Gateway Specific** drop down located on the same row as **local**, select **Yes**.
- 3) In the **Registrar Host** field, indicate the server IP address or FQDN.
- 4) Click **Apply**.

Result

The gateway(s) for which **Yes** was selected will now use the specified IP address or FQDN instead of the address or FQDN indicated in the **Registrar Host** field of the **Default Servers** table, under **SIP/Servers**.

Registrar Servers		
Gateway	Gateway Specific	Registrar Host
gateway_1_gw	Yes	IP address/FQDN
gateway_2_gw	Yes	IP address/FQDN

10.2.2.6 Assigning a Specific Messaging Server Host to a Gateway

Before you start

You can assign a specific Messaging Server to the default gateway, or to a gateway you have created.

Steps

- 1) Go to **SIP/Servers**.

- 2) In the **Messaging Servers** table, from the **Gateway Specific** drop down select **Yes** to assign a specific messaging server to the gateway.
- 3) In the **Messaging Server Host** field, indicate the IP address: Port number to use.
- 4) Click **Apply**.
- 5) Click **restart required services** located at the top of the page.

Result

The gateway(s) for which **Yes** has been selected, will now use the specified IP address: port number instead of the IP address: port number indicated in the **Messaging Server Host** field of the **Default Servers** table, under **SIP/Servers**.

Messaging Servers			
Gateway	Gateway Specific	Messaging Server Host	
gateway_1_gw	Yes ▾	IP address/: port number	
gateway_2_gw	Yes ▾	IP address/: port number	

10.2.2.7 Assigning a Specific Proxy Host to a Gateway

Before you start

You can assign a specific Registrar Server to the default gateway, or to a gateway you have created.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Proxy Servers** table, from the **Gateway Specific** drop down list located next to the gateway you wish to assign a specific Proxy SIP server, select **Yes**.
- 3) In the **Proxy Host** field, indicate the server IP address or FQDN.
- 4) Click **Apply**.

Result

The gateway(s) for which **Yes** was selected will use the specified IP address or FQDN instead of the default IP address or FQDN indicated in the **Proxy Host** field of the **Default Servers** table, under **SIP/Servers**.

Proxy Servers				
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host	
gateway_1_gw	Yes ▾	IP address/FQDN		
gateway_2_gw	Yes ▾	IP address/FQDN		

10.2.2.8 Assigning a Specific Outbound Proxy Host to a Gateway

Before you start

You can assign a specific Registrar Server to the default gateway, or to a gateway you have created.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Registrar Servers** table, from the **Gateway Specific** drop down located on the same row as **local**, select **Yes**.
- 3) In the **Outbound Proxy Host** field, indicate the server IP address or FQDN.
- 4) Click **Apply**.

Result

The gateway(s) for which **Yes** was selected will use the specified IP address or FQDN instead of the address indicated in the **Outbound Proxy Host** field of the **Default Servers** table, under **SIP/Servers**.

Proxy Servers				
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host	
gateway_1_gw	Yes ▾	IP address/FQDN	IP address/FQDN	
gateway_2_gw	Yes ▾	IP address/FQDN	IP address/FQDN	

10.2.3 SIP Server Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the Configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following advanced parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Setting the default Outbound Proxy Router Type

[SipEp.defaultProxyOutboundType](#)

Setting Gateway-Specific Outbound Proxy Router Type

[SipEp.gwSpecificProxy.OutboundType](#)

10.3 Registrations

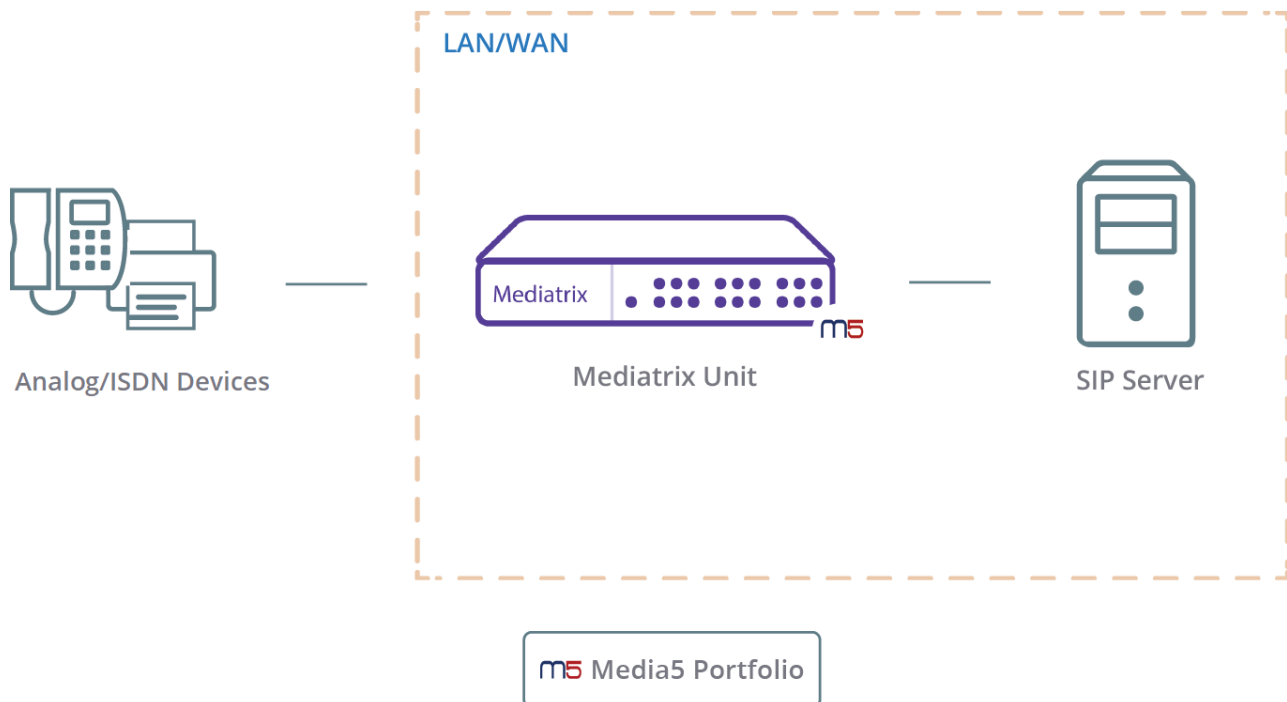
10.3.1 Basic Registration Concepts

10.3.1.1 Registration

The DGW firmware handles multiple registration modes, either per endpoint, per gateway, or for the whole unit. Simultaneous registrations are supported for each endpoint or to multiple SIP gateways (a maximum of 5 is supported).

Each endpoint may have its own registration information. You can set information for each endpoint such as its telephone number and friendly name.

Unit registration is used to register a contact not directly related to endpoints. This is generally used to indicate to a registrar the IP location of the Mediatrix unit when it is used as a gateway. In SIP, a registration is valid for a period of time defined by the registrar. Once a unit is registered, the SIP protocol requires the User Agent to refresh this registration before the registration expires. Typically, this re-registration must be completed before the ongoing registration expires, so that the User Agent's registration state does not change (i.e., remains 'registered').



10.3.1.2 Registering to all SIP Gateways vs to a specific SIP Gateway

Each endpoint can register to a specific SIP Gateway or register to all configured SIP Gateways simultaneously. DGW handles each registration separately, allowing the registration of individual endpoints to different SIP Gateways.

You can define a specific gateway to register to each endpoint of the Mediatrix unit. For instance, you could set all endpoints of the Mediatrix unit to register to all SIP Gateways simultaneously and set a specific endpoint to register to just one of the SIP Gateways. Using one or more specific parameter usually requires to enable an override parameter and set the specific configuration to apply. Refer to [Advanced SIP Registration Parameters](#) (p.285) section.

10.3.1.3 Number of Registrations

The total number of registrations is the sum of all the endpoint and gateway pairs.

For most Mediatrix devices, the total number of registrations is limited to 64. However, for the Mediatrix G7 Series, the Mediatrix S7 Series, the Sentinel 400, and the Sentinel 100, the limit is 500. If a custom DGW profile is used, the limit can be different depending on what value was defined in the profile. For example, when using a Sentinel 400, up to 500 registrations are possible, but if the profile specifies 200, then the unit will only be able to manage up to 200 registrations.

The Mediatrix unit supports a maximum of 10 gateways. An endpoint configured with **All** gateways generates as many registrations as the number of gateways. In a setup with 3 gateways, one endpoint configured with **All** as the gateway name counts for 3 in the total number of registrations. The registrations are enabled gateway by gateway until the limit is reached. Endpoint registrations are used first, then unit registrations. The remaining registrations are not registered and do not appear in the **Status** table. If the number of registrations exceeds the defined limit, a warning is displayed on the Web interface (as well as in the CLI and SNMP interfaces) and a syslog notify (Level Error) is sent. Adding a gateway or an endpoint triggers a warning message if the total number of registrations configured reached the defined limit

10.3.1.4 Registration Number Example

In this example, three gateways (Default, gw1, and gw2) are used with the Mediatrix unit, as displayed in the **Gateway Configuration** table.

The default ports (0 = 5060 for plain SIP and 0 = 5061 for secure SIP) can be used for two gateways, as long as they are attached to different signaling networks (in the **Gateway Configuration** table, default/Uplink and gw1/Lan1 use the same ports 0 and 0). If you wish to define another gateway for the same signaling network, a different port should be used than the default ones (**Gateway Configuration** table, gw2 is attached to the Uplink signaling network, as is the default gateway. For this scope, gw2 is only functional if it uses different ports than the default gateway). When a **Gateway Name** for a **User Name** is set to **All**, this means that 3 registrations are used.

Gateway Configuration						
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port
default	Trunk	Uplink		--- Suggestion ---	0	0
gw1	Trunk	Lan1		--- Suggestion ---	0	0
gw2	Trunk	Uplink		--- Suggestion ---	5062	5063

Endpoints Registration				
Endpoint	User Name	Friendly Name	Register	Gateway Name
Slot2/E1T1	ur1	ur1	Enable	all
Slot3/E1T1	ur2	ur2	Enable	gw2

Unit Registration		
Index	User Name	Gateway Name
1	te1	all
2	te2	all
3	te3	gw1
4	te4	default

User Name	Gateway Name	Number of Registrations
ur1	All	3
ur2	gw2	1
te1	all	3
te2	all	3
te3	gw1	1
te4	default	1
TOTAL NUMBER OF REGISTRATIONS		12

10.3.2 SIP Registration Basic Tasks

The following technical bulletins describe the basic tasks related to registration. Keep in mind that these documents are for units configured with the default values of the parameters.

The following documents are published on the [Media5 Documentation Portal](#):

- [Technical Bulletin - Basic SIP Endpoint Registration](#)
- [Technical Bulletin - Basic SIP Gateway Registration](#)
- [Technical Bulletin - Basic SIP Unit Registration](#)
- [Technical Bulletin - Basic SIP Username Registration](#)

10.3.3 Advanced SIP Registration Parameters

Although the services can be configured in great part in the DGW Web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on these advanced parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Non specific registration parameters

- Registration Delay Value: **SipEp.InteropRegistrationDelayValue**
- Behaviour on Initial-Registration Reception: **SipEp.BehaviorOnInitialRegistrationReception**
- Unregistered Unit Behavior: **SipEp.DefaultUnitRegistrationUnregisteredBehavior**
- Default Registration Retry Time Value: **SipEp.DefaultRegistrationRetryTime**
- Default Unregistered Endpoint Behaviour: **SipEp.DefaultRegistrationUnregisteredBehavior**

User Agent registration parameters

- Preferred Language: **SipEp.UserAgent.AcceptLanguage**
- Contact Domain: **SipEp.UserAgent.ContactDomain**
- SIP User Agent Header: **SipEp.InteropSendUaHeaderEnable**

Endpoint specific registration parameters

- Specific Unregistered Endpoint Behaviour: **SipEp.GwSpecificRegistration.UnregisteredBehavior**

Gateway specific registration parameters

- Specific Unregistered Endpoint Behaviour: **SipEp.GwSpecificRegistration.UnregisteredBehavior**
- Gateway Specific Registration Retry Time: **SipEp.GwSpecificRegistrationRetryTime**
- Expiration Value in Registration: **SipEp.GwSpecificRegistration.ExpirationValue**
- Registration Refresh: **SipEp.GwSpecificRegistrationRefreshTime**
- Registration Expiration: **SipEp.GwSpecificRegistration.ProposedExpirationValue**
- Enable Configuration: **SipEp.GwSpecificRegistration.EnableConfig**

10.4 SIP Authentication

10.4.1 Basic SIP Authentication Concepts

10.4.1.1 SIP Authentication

SIP authentication is a security feature that allows a SIP server to validate the authenticity of the sender, and to accept only the requests when they have the proper credentials.

To authenticate a SIP request, the server issues an authentication challenge to which the SIP client must respond with the proper username/password credentials. The Mediatrix unit can be configured with the authentication information needed to respond to the authentication challenges issued by SIP servers.

The authentication information is configured in the **Authentication** table. Each entry of the table has a **Criteria** and a **Realm**, if it is enabled, that define when it is appropriate to use this entry.

There are 4 criteria categories:

- **endpoint-specific:** Applies only to challenges received for SIP requests related to a specific endpoint. For instance, the registration associated with the endpoint in the user agent table or the INVITE sent to initiate a call from the endpoint.
- **gateway-specific:** Applies only to challenges received for SIP requests on a specific SIP gateway.
- **user-name specific:** Applies only to challenges for a context that uses a specific user name.
- **global to the whole unit:** Applies to all challenges received for SIP dialogs. The defined user names and passwords will apply to all the endpoints of the unit.

IMPORTANT: If authentication credentials are required for several realms, create a separate table entry for each realm.

The **Authentication** table may have between 20 and 100 rows. If you have less than 20 rows, the Mediatrix unit automatically adds new rows up to the minimum of 20.

When a challenge occurs (either 401 Unauthorized or 407 Proxy Authentication Required), the first entry in the **Authentication** table having a criteria that matches the challenge is used to reply to the challenge. The username and password of a criteria can be configured in the Web interface in the **SIP/Authentication/ Authentication** table. The entries of the **Authentication** table are tried from the first row to the last row. To have a match, the realm in the **Authentication** table entry must match the realm in the challenge or the **Validate Realm** field of the entry must be set to **Disable**. For each entry matching certain criteria (described below), the challenge is replied with the entry's user name and password. If authentication fails, the SIP server may issue another authentication challenge, provided it has been configured to do so. (Because of the increased risks of hacking, servers usually give only a single chance). In that case, the next entry in the table having a matching criteria is used to reply to this new challenge. This can be repeated until no more matching entry is

found. If no entry matches the criteria, the authentication fails. To match the authentication request, the entry must also meet one of the following criteria:

- The challenge needs to be for a SIP request related to the endpoint specified in the **Endpoint** column if the corresponding **Criteria** column is set to **Endpoint**.
- The challenge needs to be for a SIP request performed on the SIP gateway specified in the **Gateway** column if the corresponding **Criteria** column is set to **Gateway**.
- The challenge needs to be for a context that uses the user name specified in the **User Name** field if the corresponding **Criteria** column is set to **username**. The user name associated with a context is:
 - the user name of the FROM if the context sent the original SIP request, or
 - the user name of the request URI if the context received the original SIP request
- The challenge applies to a unit if the corresponding **Criteria** column is set to **Unit**.

10.4.1.2 Authentication Table Entries - Order is Important

The priority of an entry in the **Authentication** table is important. The most specific authentication credential must be set before the more generic ones, otherwise the challenges will be responded with the generic credentials rather than the specific ones. If authentication fails with the credentials found in the **Authentication** table, the SIP server may issue another authentication challenge. In that case, the next entry in the table having a matching criteria is used to reply to this new challenge. This can be repeated until no more matching entry is found.

For example

✦ Authentication

Authentication									
Priority	Criteria	Endpoint	Gateway	Username	Criteria	Validate	Realm	Realm	User Name
1	Endpoint	Slot4/FXS1				Disable			User1
2	Endpoint	Slot4/FXS3				Disable			User3
3	Gateway		gateway_1			Disable			gw1
4	Gateway		gateway_2			Disable			gw2
5	Unit					Disable			Unit1

- Three gateways are defined in the **Gateway** table (under **SIP/Gateways**)
 - gateway_1
 - gateway_2
 - gateway_3

- The unit has 4 endpoints:
 - **Slot4/FXS1**
 - **Slot4/FXS2**
 - **Slot4/FXS3**
 - **Slot4/FXS4**
- The SIP requests related to **Slot4/FXS1**, **Slot4/FXS3**, and **Slot4/FXS4** are sent via **gateway_2**
- The SIP requests related to **Slot4/FXS2** are sent via **gateway_3**

Table 3: Scenario 1

Step	Description
1	Endpoint Slot4/FXS3 needs to register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria that matches endpoint Slot4/FXS1 , but because the REGISTER was issued for Slot4/FXS3 , the match fails.
6	Entry #2 of the Authentication table has a Criteria that matches endpoint Slot4/FXS3 and because the REGISTER was issued for Slot4/FXS3 , the match succeeds, and the credentials of this entry are used to respond to the challenge.
7	If the credentials configured in entry #2 are good, the SIP server accepts to handle the REGISTER request.

Table 4: Scenario 2

Step	Description
1	Endpoint Slot4/FXS4 must register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria to match endpoint Slot4/FXS1 but because the REGISTER was issued for Slot4/FXS4 , the match fails.
6	Entry #2 of the Authentication table has a Criteria to match endpoint Slot4/FXS3 but because the REGISTER was issued for Slot4/FXS4 , the match fails.
7	Entry #3 of the Authentication table has a Criteria to match gateway gateway_1 but because the REGISTER was issued via gateway_2 , the match fails.
8	Entry #4 of the Authentication table has a Criteria to match gateway_2 and because the REGISTER was issued via gateway_2 , the match succeeds, and the credentials of this entry are used to respond to the challenge.
9	If the credentials configured in entry #4 are good, the SIP server accepts to handle the REGISTER request.

Table 5: Scenario 3

Step	Description
1	Endpoint Slot4/FXS2 must register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria to match endpoint Slot4/FXS1 , but because the REGISTER was issued for Slot4/FXS2 , the match fails.
6	Entry #2 of the Authentication table has a Criteria to match endpoint Slot4/FXS3 , but because the REGISTER was issued for Slot4/FXS2 , the match fails.
7	Entry #3 of the Authentication table has a Criteria to match gateway gateway_1 , but because the REGISTER was issued via gateway_3 , the match fails.
8	Entry #4 of the Authentication table has a criteria to match gateway gateway_2 , but because the REGISTER was issued via gateway_3 , the match fails.
9	Entry #5 of the Authentication table has a criteria to match the whole unit, so the match succeeds, and the credentials of this entry are used to respond to the challenge.
10	If the credentials configured in entry #5 are good, the SIP server accepts to handle the REGISTER request.

10.4.1.3 Important Information To Know before Using Sip Authentication

Access Rights

The **SIP /Authentication** page is not accessible if you have the User or Observer access right.

Naming

The SIP username (i.e. the one in the username criteria) is checked against SIP username syntax of RFC3261.

Authentication

The **Authentication** table (under **SIP /Authentication**) may have between 20 and 100 rows. If you have less than 20 rows, the Mediatrix unit automatically adds new rows up to the minimum of 20.

Authentication Order

The order of the tried entries in the **SIP/Authentication** table is from the first row to the last row. The row sequence is important. Refer to [Authentication Table Entries - Order is Important](#) (p.287) .

Endpoint Authentication

- Several usernames/passwords can be defined for a single Endpoint.
- Endpoint Authentication can be defined for all types of endpoints i.e. E1T1/FXS/FXO/BRI/PRI.

10.4.2 Basic SIP Authentication Tasks

10.4.2.1 Defining Authentication Credentials for a Gateway

Before you start

- Administrator access rights are required to access this page.
- The **Mediatrix** unit can support up to 5 gateways.

Steps

- 1) Go to **SIP/Authentication**.
- 2) Click  located on the first row.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 3) In the **Authentication** table, from the **Criteria** selection list, select **Gateway**.
- 4) From the **Gateway** selection list, select a gateway.
- 5) Enter a password and username for the gateway.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply**.

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to the gateway specified in the **Gateway** column. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Gateway		Gateway_Name_gw		Disable		username	*****

10.4.2.2 Defining Authentication Credentials for an Endpoint

Before you start

You will not be able to access this page if you have a User or Observer access right.

Information

If different usernames/passwords are needed for different realms, use multiple table entries.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click **+** to add a new row at the bottom of the table.

- 2) Click **Edit** located on the first row.
- 3) From the **Criteria** selection list, select **Endpoint**.
- 4) From the **Endpoint** selection list, select an endpoint.
- 5) Enter a password and username for the endpoint.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to the endpoint specified in the **Endpoint** column. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	Endpoint_Name			Disable		Username	*****

10.4.2.3 Defining Authentication Credentials for the Unit

Before you start

- You will not be able to access this page if you have a User or Observer access right.

- The challenge applies to a unit if the corresponding **Criteria** column is set to **Unit**.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 2) Click **Edit** located on the first row.
- 3) From the **Criteria** selection list, select **Unit**.
- 4) Enter a password and username for the unit.

Note: You can optionally enable realm validation, if needed.

- 5) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to any gateway or endpoint of the unit. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Unit				Disable		Username	*****

10.4.2.4 Defining Authentication Credentials for a Username

Before you start

You will not be able to access this page if you have a User or Observer access right.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 2) Click  located on the first row.
- 3) From the **Criteria** selection list, select **User Name**.
- 4) In the **Username Criteria**, enter the name of a username.
- 5) Enter a password and username for the username.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to a specific username. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Username			UserName1	Enable		UserName	*****

10.4.2.5 Selecting the Priority Level of an Authentication

Steps

- 1) Go to **SIP/Authentication**.
- 2) Use the arrows to move an authentication entry up or down the table.

Note: Search is performed from the first entry of the table down to the last.

- 3) Click **Apply** or **Apply and Refresh Registration**

Result

The Authentication table will be searched in the selected order to find which credentials to use.

10.5 Transport

10.5.1 Basic SIP Transport Concepts

10.5.1.1 SIP Transport Types

You can globally set the transport type for SIP all the endpoints of the Mediatrix unit to either UDP (User Datagram Protocol), TCP (Transmission Control Protocol), or TLS (Transport Layer Security).

Please note that RFC 3261 states the implementations must be able to handle messages up to the maximum datagram packet size. For UDP, this size is 65,535 bytes, including IP and UDP headers. However, the maximum datagram packet size the Mediatrix unit supports for a SIP request or response is 5120 bytes excluding the IP and UDP headers. This should be enough, as a packet is rarely bigger than 2500 bytes.

10.5.1.2 Important Information to Know Before Configuring SIP Transport

- For SIP signaling, UDP and TCP are mutually exclusive with TLS. Activating TLS automatically disables these unsecure protocols.
- The TLS Persistent Connections Status table is not displayed if the TLS transport is not activated.
- Secure transport (TLS) requires to:
 - Synchronise the time in the unit (Refer to [Selecting the Unit's Time Zone](#) (p.95)).
 - Install the security certificates used to authenticate the server to which you will connect. Refer to [Technical Bulletin - Using Trusted CA and Host Certificates](#) published on the [Media5 Documentation Portal](#).
 - Configure the unit so that a “transport=tls” parameter is added to the Contact header of your SIP requests. (**SIP/Transport/General Configuration** table, **Add SIP Transport in Contact Header**).

If secure media (SRTP) is used, it is highly recommended to also use secure SIP signaling (TLS), otherwise the security of the media could be easily compromised by an attacker looking at the SIP signaling.

10.5.2 Basic SIP Transport Tasks

10.5.2.1 Preparing the Unit to Use TLS for SIP

Information

These steps should be performed first when using Transport Layer Security (TLS) as they are mandatory for all TLS based applications (TR-069, SIP over TLS, 802.1X, HTTPS file transfer, etc.)

Steps

- 1) Make sure the unit is able to retrieve current Time/Date information from a NTP server, either from a NTP server learnt from DHCP or static NTP servers.
- 2) Make sure the time zone of your unit is adjusted properly. Refer to [Selecting the Unit's Time Zone](#) (p.95)

Note: This step is mandatory for the unit to have the proper date/time, otherwise the TLS communication cannot be validated.

- 3) Upload all the trusted CA certificates required for server validation. Refer to [Technical Bulletin -Using Trusted CA and Host Certificates](#) published on the [Media5 Documentation Portal](#).

- 4) If the respective pop-up message appears, click **restart required services**.

10.5.2.2 Enabling TLS Transport for SIP

Before you start

A TLS certificate must be installed on the Mediatrix unit.

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **TLS** to **Enable**.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. Once TLS is **enabled**, all configured gateways will use TLS, and all other protocols will be disabled.

- 3) Click **Apply**.

10.5.2.3 Enabling UDP Transport for SIP

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **UDP** to **Enable**.

IMPORTANT: The unit does not support a mix of both TLS and non-TLS links. If TLS is enabled and you want to enable UDP, you must first disable TLS. This will apply to all gateways.

- 3) Click **Apply**.

10.5.2.4 Enabling TCP Transport for SIP

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **TCP** to **Enable**.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. If TLS is enabled and you want to enable TCP, you must first disable TLS. This will apply to all gateways.

- 3) Click **Apply**.

10.5.2.5 Configuring SIP Transport Parameters

Before you start

Some servers implementation may require to explicit the transport type in the SIP Contact header. If that's the case, see the following steps.

Steps

- 1) Go to **SIP/Transport**.
- 2) Enable one or both of the **Add SIP Transport in Registration** or **Add SIP Transport in Contact Header** parameters, depending on what is required.
- 3) **Apply**.

Result

In the following example, the transport parameter is added in the Contact header of the REGISTER request and includes the supported transport (UDP, TCP or TLS) for that gateway.

General Configuration		
Add SIP Transport in Registration:	Enable ▾	
Add SIP Transport in Contact Header:	Enable ▾	
Persistent Base Port:	16000	
Failback Interval:	15	
TLS Certificate Trust Level:	Locally Trusted ▾	
TCP Connect Timeout:	127	
Add rport:	Disable ▾	

10.5.3 Advanced SIP Transport Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by either :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- To set transport TLS Cipher Suite settings: refer to the [DGW Configuration Guide - Transport Layer Security](#) document published on the Media5 documentation portal.

- To set whether or not the unit uses the symmetric source port feature when Sending SIP traffic over UDP: **SipEp.InteropSymmetricUdpSourcePortEnable**.
- To set TLS authentication: refer to the [DGW Configuration Guide - Transport Layer Security](#) document published on the Media5 documentation portal.
- To set whether or not to force a DNS NAPTR request: **SipEp.InteropForceDnsNaptrInTls**.
- To set the proper SIP failover conditions: **SipEp.defaultSipFailoverConditions** and **SipEp.GwSpecificFailover.SipFailoverConditions**.
- To select the SIP gateway on which failover conditions will be applied: **SipEp.gwSpecificFailover.EnableConfig**.
- To set the failover conditions on a specific gateway: **SipEp.gwSpecificFailover.SipFailoverConditions**.
- To set the persistent port interval: **SipEp.TransportPersistentPortInterval**.

10.6 Interop

10.6.1 Basic SIP Interop Concepts

10.6.1.1 Interoperability

Interoperability is the ability of computer systems or software to exchange information and to be able to use the information that has been exchanged.

For example, when deploying a SIP trunk, information must be exchanged between the SIP trunking service provider or ITSP offering the SIP trunk service, the IP-PBX, and the Mediatrix device located on the edge of the network. If the information cannot be understood, processed and exchanged by every component, customers will experience interoperability issues that can translate into:

- Device and user registration issues
- Problems when trying to transfer calls
- Increased vulnerability to VoIP cyber attacks
- Messaging delays or failure

10.6.2 Basic SIP Interop Tasks

10.6.2.1 Setting the SIP INVITE for T.38 Fax Error Behavior

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **Behavior on T.38 INVITE Not Accepted** table, set the behavior of each SIP error code.

- 3) Click **Apply**.

Result

When an error is received as a response to an INVITE for T.38 fax, the selected behavior will be applied.

Behavior on T.38 INVITE Not Accepted		
SIP Error Code	Behavior	
406	Re-INVITE For Clear Channel Only	▼
415	Re-Establish Audio	▼
488	Drop Call	▼
606	Re-INVITE For Clear Channel Only	▼

10.6.2.2 Configuring SIP Interoperability

Before you start

Before configuring SDP interoperability, you must first read the online help available for each field and parameter as important information on limitations, instructions, exclusions, and proscriptions are mentioned. Click **Show Help** located at the top right of the screen.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **SIP Interop** table, set each parameter as required.
- 3) Click **Apply**.

Result

SIP Interop	
Secure Header:	Disable
Default Username Value:	Anonymous
OPTIONS Method Support:	Always 200 OK
Ignore OPTIONS on no Usable Endpoints:	Disable
SIP URI User Parameter Value:	
Behavior on Machine Detection:	Re-INVITE on Fax T38 Only
Registration Contact Matching:	Strict
Transmission Timeout:	32
Collect Call Proprietary Header:	Ignore

10.6.2.3 Configuring SDP Interoperability

Before you start

Before configuring SDP interoperability, you must first read the online help available for each field and parameter as important information on limitations, instructions, exclusions, and proscriptions are mentioned. Click **Show Help** located at the top right of the screen.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **SDP Interop** table, set each parameter as required.
- 3) Click **Apply**.

Result

SDP Interop	
Offer Answer Model:	
Answer Codec Negotiation:	All Common - Local Priority ▼
Enforce Offer Answer Model:	Enable ▼
Allow Less Media In Response:	Disable ▼
Allow Media Reactivation in Answer:	Disable ▼
Multiple Active Media:	
Allow Audio and Image Negotiation:	Disable ▼
Allow Multiple Active Media In Answer:	Enable ▼
Other:	
On Hold SDP Stream Direction in Answer:	RecvOnly ▼

10.6.2.4 Selecting the Security Level to Validate TLS Server Certificates

Before you start

- At least one certificate must be returned by the peer even if no validation is made.
- **No Validation** and **Trusted Certificate** certificate validation should only be used for lab purposes.
- The Host name must absolutely be known by the DNS server the unit is contacting.
- The certificate authority (CA) must be added to the Cert service.

Information

For more details on Transport Layer Security (TLS), refer to the [DGW Configuration Guide -Transport Layer Security](#) published on the [Media5 Documentation Portal](#). This configuration is mandatory for certificate validation.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **TLS Interop** table, set **Certificate Validation** parameter as required.

Note: This parameter has no effect on the TLS client authentication when the unit is acting as a TLS server. Refer to the **Interop.TlsClientAuthenticationEnable** parameter in the [Reference Guide](#) published on the Media5 documentation portal.

- 3) Click **Apply**.

Result

TLS Interop	
Certificate Validation:	Host Name v

10.6.2.5 Configuring the Behavior of the T.38 INVITE Not Accepted

This task allows you to set the unit's behaviour after receiving an error to a SIP INVITE for T.38 fax.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **Behavior on T.38 INVITE Not Accepted** table, from the **Behavior** selection list, set the required behavior for each **SIP Error Code**.
- 3) Click **Apply**.

Result

Behavior on T.38 INVITE Not Accepted		
SIP Error Code	Behavior	
406	Re-INVITE For Clear Channel Only v	
415	Drop Call	
488	Re-INVITE For Clear Channel Only	
	Re-Establish Audio	
	Use Previous Media Negotiation	
606	Re-INVITE For Clear Channel Only v	

10.6.2.6 Configuring Miscellaneous Interoperability Parameters

Before you start

Before configuring SDP interoperability, you must first read the online help available for each field and parameter as important information on limitations, instructions, exclusions, and proscriptions are mentioned. Click **Show Help** located at the top right of the screen.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **Misc Interop** table, set each parameter as required.
- 3) Click **Apply**.

Result

Misc Interop	
Map Plus To TON International:	Enable ▼
Ignore Plus In Username:	Disable ▼
Escape Pound (#) In SIP URI Username:	Enable ▼
Escape Format:	Lower Hexadecimal ▼

10.6.2.7 Selecting the SIP TLS Server Certificate Security Level

Information

The security level used to validate the TLS server certificate has no effect on the TLS client authentication when the unit is acting as a TLS server. Refer to the [SipEp.InteropTlsClientAuthenticationEnable](#) parameter.

Only the setting for SIP over TLS transport is available over the Web GUI. For others, like file transfer or TR-069, settings are available with the script. And the levels of support are different. SIP over TLS security level has one more level (Trusted Certificate level) which other services do not have.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **TLS Interop** table, select the security level used to validate certificates.

10.6.3 Troubleshooting SIP Interoperability

Problem	Solution
Media negotiation problems because the Mediatrix unit sends a BYE after receiving a 200 OK.	Set the Enforce Offer Answer Model value to Disable and the Allow Less Media In Response value to Enable .
No ringing is heard for outgoing calls	The Early RTP feature was enabled (SipEp.InteropListenForEarlyRtpEnable) although the server does not support early RTP (or early media).

10.6.4 Advanced Interoperability Interface Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Direction Attributes

- Defining the direction attribute when putting a call on hold:
SipEp.InteropOnHoldSdpStreamDirection
- Defining if the direction attribute is present: **SipEp.InteropSdpDirectionAttributeEnable**
- Enable/Disable SDP Detect Peer Direction Attribute Support:
SipEp.InteropSdpDetectPeerDirectionAttributeSupportEnable
- Defining the SDP direction attribute level: **SipEp.InteropSdpDirectionAttributeLevel**
- Defining the behaviour with the “sendonly” direction attribute:
SipEp.InteropOnHoldAnswerSdpStreamDirection

On hold

- Defining the on hold SDP connection address: **SipEp.InteropOnHoldSdpConnectionAddress**

Headers

- Max-Forwards Header: **SipEp.InteropMaxForwardsValue** Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop. If the Max-Forwards value reaches 0 before the request reaches its destination, it is rejected with a “483 (Too Many Hops)” error response. The Max-Forwards SIP header is always present and the default value is 70.
- Resolving the route header: **SipEp.InteropResolveRouteHeaderEnable**
- Setting whether or not to ignore the Require header:
SipEp.InteropIgnoreRequireHeaderEnable
- Setting the SIP User-Agent header format: **SipEp.InteropUaHeaderFormat**

SIP INFO

- Set the call waiting Private Number Criteria for SIP INFO:
SipEp.InteropCallWaitingSipInfoPrivateNumberCriteria
- Defining the SIP INFO Without Content Answer behaviour:
SipEp.InteropSipInfoWithoutContentAnswer

Others

- Defining the local ring behaviour on provisional response:
SipEp.InteropSdpDirectionAttributeLevel
- Setting the maximum length of the session ID and the session version number:
SipEp.InteropSdpOriginLineSessionIdAndVersionMaxLength

- Overriding the register home domain value: **SipEp.InteropRegisterHomeDomainOverride**
- Enabling the DNS SRV record lock feature: **SipEp.InteropLockDnsSrvRecordPerCallEnable**
- Enabling the Early RTP feature: **SipEp.InteropListenForEarlyRtpEnable**

Note: Do not enable this feature unless the server supports early RTP (or early media). Failing so prevents any ringing to be heard for outgoing calls.

- Setting ACK branch matching: **SipEp.InteropAckBranchMatching**
- Setting the reject code: **SipEp.InteropRejectCodeForUnsupportedSdpOffer**
- Setting the keep alive option format: **SipEp.InteropKeepAliveOptionFormat**
- Defining the unsupported Content-Type behaviour: **SipEp.InteropUnsupportedContentType**
- If the configured DTMF transport is "Out-of-band using RTP", the unit rather uses the payload type found in the answer: **SipEp.InteropUseDtmfPayloadTypeFoundInAnswer**
- Determine the behaviour of the device when answering a request offering more than one active media: **SipEp.InteropAllowMultipleActiveMediaInAnswer**
- Enabling this parameter may improve interoperability with VoLTE endpoints:
SipEp.InteropSend183WithSdpBefore180WithoutSdp

10.7 Misc

10.7.1 Basic Concepts

10.7.1.1 SIP Penalty Box

The penalty box feature is useful when a given host FQDN resolves to a non-responding address. When the address times out, it is put into the penalty box for a given amount of time. During that time, this address is considered as “non-responding” for all requests

This feature is useful when DNS requests return multiple or varying addresses for a host FQDN. It makes sure that, when a host is down, no SIP request is sent to it for a minimal amount of time. When enabled, this feature takes effect immediately on the next call attempt.

The penalty box feature is applied only when using UDP or TCP connections established with a FQDN. A similar penalty box feature for the TLS persistent connections is available via the **TLS Persistent Retry Interval** parameter.

Note: The Penalty Box feature works only with Trunk Gateways, i.e. it is disabled when an Endpoint Gateway type is configured.

10.7.1.2 SIP Penalty Box vs Transport Types

Media5 recommends to use this feature with care when supporting multiple transports or you may experience unwanted behaviours. When the Mediatrix unit must send a packet, it retrieves the

destination from the packet. If the destination address does not specify a transport to use and does not have a DNS SRV entry that configures which transport to use, then the Mediatrix unit tries all transports it supports, starting with UDP. If this fails, it tries with TCP. The unit begins with UDP because all SIP implementations must support this transport, while the mandatory support of TCP was only introduced in RFC 3261.

Note: It is not the destination itself that is placed in the penalty box, but rather targets, which are a combination of address, port, and transport. Targets put in penalty box are not used unless all the targets are in the penalty box. In that case, the highest priority target is used.

Let's say for instance that the Mediatrix unit supports both the UDP and TCP transports. It tries to reach endpoint "B" for which the destination address does not specify a transport and there is no DNS SRV entry to specify which transports to use in which order. It turns out that this endpoint "B" is also down. In this case, the Mediatrix unit first tries to contact endpoint "B" via UDP. After a timeout period, the UDP target is placed in the penalty box and the unit then tries to contact endpoint "B" via TCP. This fails as well and the TCP target is also placed in the penalty box.

Now, let's assume endpoint "B" comes back to life and the Mediatrix unit tries again to contact it before UDP and TCP targets are released from the penalty box. First, the unit tries UDP, but it is currently in the penalty box and there is another transport left to try. The Mediatrix unit skips over UDP and tries the next target, which is TCP. Again, TCP is still in the penalty box, but this time, it is the last target the Mediatrix unit can try, so penalty box or not, TCP is used all the same to try to contact endpoint "B".

There is a problem if endpoint "B" only supports UDP (RFC 2543-based implementation). Endpoint "B" is up, but the Mediatrix unit still cannot contact it: with UDP and TCP in the penalty box, the unit only tries to contact endpoint "B" via its last choice, which is TCP.

The same scenario would not have any problem if the penalty box feature was disabled. Another option is to disable TCP in the Mediatrix unit, which makes UDP the only possible choice for the unit and forces to use UDP even if it is in the penalty box.

You must fully understand the above problem before configuring this feature. Mixing endpoints that do not support the same set of transports with this feature enabled can lead to the above problems, so it is suggested to either properly configure SRV records for the hosts that can be reached or be sure that all hosts on the network support the same transport set before enabling this feature.

10.7.1.3 Default Conversion of Standard SIP Error Codes To ISDN Q.850 Cause Codes

Mediatrix devices internally use Q.850 ISDN cause codes as the common representation for call errors and call terminations. Mediatrix devices are gateways used between SIP and conventional (i.e. non-SIP) telephony technologies; therefore converting SIP error codes to Q.850 ISDN cause codes is required in both directions i.e. from SIP to ISDN and ISDN to SIP.

The following table presents the conversion of SIP Error Codes to Q.850 ISDN Cause Codes. It is possible to override these default conversions and to configure the conversions of any other SIP error code between 400 and 699. (Refer to the Basic tasks)

SIP Error Codes	Q.850 ISDN Cause Codes
400: Bad Request	41 Temporary Failure
401: Unauthorized	21 Call rejected
402: Payment required	21 Call rejected
403: Forbidden	21 Call rejected
404: Not found	1 Unallocated number
405: Method not allowed	63 Service or option unavailable
406: Not acceptable	79 Service/option not implemented
407: Proxy authentication required	21 Call rejected
408: Request timeout	102 Recovery on timer expiry
410: Gone	22 Number changed (w/o diagnostic)
413: Request Entity too long	127 Interworking
414: Request-URI too long	127 Interworking
415: Unsupported media type	79 Service/option not implemented
416: Unsupported URI Scheme	127 Interworking
420: Bad extension	127 Interworking
421: Extension Required	127 Interworking
423: Interval Too Brief	127 Interworking
480: Temporarily unavailable	18 No user responding
481: Call/Transaction Does not Exist	41 Temporary Failure
482: Loop Detected	25 Exchange - routing error
483: Too many hops	25 Exchange - routing error
484: Address incomplete	28 Invalid Number Format
485: Ambiguous	1 Unallocated number
486: Busy here	17 User busy
500: Server internal error	41 Temporary failure
501: Not implemented	79 Not implemented, unspecified
502: Bad gateway	38 Network out of order
503: Service unavailable	41 Temporary failure
504:Server time-out	102 Recovery on timer expiry
504: Version Not Supported	127 Interworking
513: Message Too Large	127 Interworking

SIP Error Codes	Q.850 ISDN Cause Codes
600: Busy everywhere	17 User busy
603: Decline	21 Call rejected
604: Does not exist anywhere	1 Unallocated number

10.7.1.4 Default Conversion of Standard Q.850 ISDN Cause Codes to SIP Error Codes

Mediatrix devices internally use Q.850 ISDN cause codes as the common representation for call errors and call terminations. Mediatrix devices are gateways used between SIP and conventional (i.e. non-SIP) telephony technologies; therefore, converting SIP error codes to Q.850 ISDN cause codes is required in both directions i.e. from SIP to ISDN and ISDN to SIP.

The following table presents the conversion of Q.850 ISDN Cause Codes to SIP Error Codes. It is possible to override these default conversions and to configure the conversions of any other Q.850 ISDN Cause Codes between 1 and 127. (Refer to the Basic tasks.)

Normal Event

Q.850 ISDN Cause Codes	SIP Error Codes
1: Unassigned (unallocated) number.	404 Not Found
2: No route to specified transit network.	404 Not Found
3: No route to destination.	404 Not Found
6: Channel unacceptable.	500 Internal Server Error
7: Call awarded and being delivered in an established channel.	500 Internal Server Error
16 normal call clearing	--- BYE or CANCEL
17: User busy.	486 Busy Here
18: No user responding.	408 Request Timeout
19: User alerting, no answer.	480 Temporarily unavailable
20: Subscriber absent.	480 Temporarily unavailable
21: Call rejected.	403 Forbidden
22: Number changed (w/o diagnostic).	410 Gone
22: Number changed (w diagnostic).	301 Moved Permanently
23: Redirection to new destination.	410 Gone
26: Non-selected user clearing.	404 Not Found
27: Destination out of order.	502 Bad Gateway
28: Invalid number format (incomplete number)	484 Address incomplete
29: Facility rejected.	501 Not implemented
30: Response to STATUS ENQUIRY.	500 Internal Server Error
31 normal unspecified	480 Temporarily unavailable

Resource unavailable

ISUP Cause Value	SIP Response
34: No circuit/channel available.	503 Service unavailable
38: Network out of order.	503 Service unavailable
41: Temporary failure.	503 Service unavailable
42: Switching equipment congestion. .	503 Service unavailable
43: Access information discarded.	500 Internal Server Error
44: Requested circuit/channel not available.	500 Internal Server Error
47: Resource unavailable, unspecified	503 Service unavailable

Service or option not available

ISUP Cause Value	SIP Response
55: Incoming calls barred within CUG.	403 Forbidden
57: Bearer capability not authorized.	403 Forbidden
58: Bearer capability not presently available.	503 Service unavailable
63: Service or option not available, unspecified.	500 Internal Server Error

Service or option not implemented

ISUP Cause Value	SIP Response
65: Bearer capability not implemented.	488 Not Acceptable Here
66: Channel type not implemented.	500 Internal Server Error
69: Requested facility not implemented.	500 Internal Server Error
70: Only restricted digital information bearer. .	488 Not Acceptable Here
79: Service or option not implemented, unspecified	501 Not Implemented

Invalid Message

ISUP Cause Value	SIP Response
81: Invalid call reference value.	500: Internal Server Error
82: Identified channel does not exist.	500 Internal Server Error
83: A suspended call exists, but this call identity does not.	500 Internal Server Error
84: Call identity in use.	500 Internal Server Error
85: No call suspended.	500 Internal Server Error
86: Call having the requested call identity has been cleared.	500 Internal Server Error
87: user not member of CUG.	403 Forbidden
88: Incompatible destination..	503 Service unavailable
91: Invalid transit network selection.	500 Internal Server Error
95: Invalid message, unspecified	500 Internal Server Error

Protocol error

ISUP Cause Value	SIP Response
96: Mandatory information element is missing.	500: Internal Server Error
97: Message type non-existent or not implemented.	500: Internal Server Error
98: Message not compatible with call state or message type non-existent or not implemented.	500: Internal Server Error
99: Information element non-existent or not implemented.	500: Internal Server Error
100: Invalid information element contents.	500: Internal Server Error
101: Message not compatible with call state.	500: Internal Server Error
102: Recovery on time expiry.	504 Gateway timeout
111: Protocol error, unspecified.	500 Server internal error

Interworking

ISUP Cause Value	SIP Response
127: Interworking, unspecified	500 Server internal error

10.7.1.5 PRACK

Reliable provisional responses (PRACK) is supported as per RFC 3262.

It is possible to define the type of PRACK support when acting as a:

- user agent client
- user agent server

10.7.1.6 Session Timer Extension

The session timer extension allows detecting the premature end of a call caused by a network problem or a peer's failure by resending a refresh request periodically.

This refresh request sent by the Mediatrix unit is either a reINVITE or an UPDATE, according to the configuration of the **Session Refresh Request Method** parameter.

A successful response (200 OK) to this refresh request indicates that the peer is still alive and reachable. A timeout to this refresh request may mean that there are problems in the signalling path or that the peer is no longer available. In that case, the call is shut down by using normal SIP means.

10.7.1.7 SDP in Session Timer reINVITEs or UPDATEs

The reINVITE is sent with the last SDP that was negotiated. Receiving a session timer reINVITE should not modify the connection characteristics. If the reINVITE method is used, it is sent with the last SDP that was negotiated. Reception of a session timer reINVITE should not modify the connection characteristics. If the UPDATE method is used, it is sent without any SDP offer.

10.7.1.8 Relation Between Minimum and Maximum Values

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

It is up to the caller to decide what to do when it receives a 422 to its INVITE. The Mediatix unit will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the user agent server was ready to accept (located in the Min-SE header). This means that the maximum value as set in the Mediatix unit might not be followed. This has the advantage of establishing the call even if the two endpoints have conflicting values. The Mediatix unit will also keep retrying as long as it gets 422 answers with different Min-SE values.

10.7.1.9 Session Refresh

Sending a session timer reINVITE or UPDATE is referred to as refreshing the session.

Normally, the user agent server that receives the INVITE has the last word on who refreshes. The Mediatix unit always lets the user agent client (caller) perform the refreshes if the caller supports session timers. In the case where the caller does not support session timers, the Mediatix unit assumes the role of the refresher.

10.7.1.10 Event Handling

The Mediatix unit supports receiving event handling Notifications to start a remote reboot or a sync of configuration for specific endpoint(s).

The event handling Notifications "reboot" or "check-sync" is not specified in an Allow-Events header. The Mediatix unit supports the Notify without subscription.

Note: It is recommended to use these event handling notifications only when the SIP transport is secure (TLS) or when the firewall filters the requests sent to the unit.

10.7.2 Basic Tasks

10.7.2.1 Configuring the SIP Penalty Box

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **Penalty Box** table, from the **Penalty Box Activation** list, choose **Enable**.
- 3) In the **Penalty Box Times** field, enter the duration during which the SIP target will remain in the SIP penalty box.

Result

Penalty Box	
Penalty Box Activation:	Enable ▼
Penalty Box Time (s):	300

10.7.2.2 Overriding the Default Mapping for SIP Error Code to ISDN Cause

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **SIP to Cause Error Mapping** table, click **+**.
- 3) In the **Configure New SIP to Cause Error Mapping** table, from the **Suggestion** list, choose a SIP code and cause.
- 4) Click **Apply**.

Result

For example:

Configure New SIP to Cause Error Mapping	
Value	Suggestion
SIP Code: 400	--- Suggestion --- ▼
Cause: 1	--- Suggestion --- ▼

10.7.2.3 Overriding the Default Mapping for ISDN Cause to SIP Error Codes

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **Cause to SIP Error Mapping** table, click **+**.

- 3) In the **Configure New Cause to SIP Error Mapping** table, from the **Suggestion** list, choose a SIP code and cause.
- 4) Click **Apply**.

Result

Configure New Cause to SIP Error Mapping		
	Value	Suggestion
Cause	1	--- Suggestion ---
SIP Code	401	--- Suggestion ---

10.7.2.4 Choosing to Use Additional Headers

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **Additional Headers** table, set the **Reason Support**, the **Referred-By Support** and the **Privacy Headers In Response** fields as required.
- 3) Click **Apply**.

Result

The Reason and the Referred-By SIP Headers will be handled as chosen.

Additional Headers		
Reason Support:	Receive Q.850	
Referred-By Support:	Header Only	
Privacy Headers In Response:	Supported P-Asserted-Identity	

10.7.2.5 Defining the Type of PRACK Support

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **Prack** table, set the **UAC PRACK Support (RFC 3262)** and **UAS PRACK Support (RFC 3262)** fields as required.
- 3) Click **Apply**.

Result

When acting as a user agent server or client, the RFC 3262 (PRACK) will or not be supported.

PRACK		
UAS PRACK Support (RFC 3262):	Supported	
UAC PRACK Support (RFC 3262):	Unsupported	

10.7.2.6 Setting the Session Refresh Information

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **Session Refresh**, table, set the **Session Refresh Timer Enable** selection list to **Enable**.

Note: Disabling this parameter is not recommended since it will make 'dead' calls impossible to detect.

- 3) Set the **Minimum Expiration Delays** field.

Note: The value of the **Minimum Expiration Delays** must be equal or smaller than the **Maximum Expiration Delays** value.

- 4) Set the **Maximum Expiration Delays** field.

Note: The value of the **Maximum Expiration Delays** must be equal or higher than the **Minimum Expiration Delays** value.

Note: When the **Maximum Expiration Delays** value is lower than the **Minimum Expiration Delays** value, the minimum and maximum expiration delay values in INVITE packets are the same as the value set in the Minimum Expiration Delay field.

- 5) Set the **Session Refresh Request Method** field.

Note: Session Refresh Requests can be received via both methods, regardless of how this parameter is configured.

- 6) Click **Apply**.

Result

For example :

Session Refresh		
Session Refresh Timer Enable:	Enable	
Minimum Expiration Delay (s):	1800	
Maximum Expiration Delay (s):	3600	
Session Refresh Request Method:	ReInvite	

10.7.2.7 Overriding the SIP Domain Used

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **Gateway Configuration** table, in the **SIP Domain Override** field, enter the SIP domain name that should be used instead of the home domain proxy.
- 3) Click **Apply**.

Result

The specified SIP domain name will be used instead of the home domain proxy (**Proxy Host** field under **SIP/ Servers**) in the address of record and the request-URI. When it overrides the home domain proxy in the request-URI, the request-URI also contains a maddr parameter with the resolved home domain proxy to make sure the requests are routable.

Gateway Configuration		
Gateway Name	SIP Domain Override	
trunk_lines_gw		

10.7.2.8 Setting the Blind Transfer Method

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **SIP Transfer** table, from the **Blind Transfer Method** choose the required method.
- 3) Click **Apply**.

Result

The blind transfer will be achieved as set when participating in a transfer as the transferor. For example:

SIP Transfer	
Blind Transfer Method:	Semi Attended ▼

10.7.2.9 Configuring Call Diversion

Information

The Diversion feature is not available in the NI2 and QSIG signalling protocols. For more details on ISDN PRI interfaces, refer to the [DGW Configuration Guide - ISDN user guide](#) published on the [Media5 Documentation Portal](#).

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **Diversion** table, from the selection list, choose the required **Method**.
- 3) Click **Apply**.

Result

The Gateway will use the SIP method selected to receive/send call diversion information in an INVITE. For example:

Diversion	
Gateway Name	Method
phone_lines_gw	Diversion Header ▼
trunk_lines_gw	Diversion Header ▼

10.7.2.10 Configuring Supported DNS Queries

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **DNS** table, from the **Supported DNS Queries** selection , select the type of DNS queries that the SipEp service supports.
- 3) Click **Apply**.

Result

The SipEp service will support and use the selected DNS queries. For example:

DNS	
Supported DNS Queries:	NAPTR ▼

10.7.2.11 Configuring Event Handling

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **Event Handling** table, for each gateway, from the **Reboot** selection list, choose how the gateway handles the reboot SIP NOTIFY messages.
- 3) From the **Check Sync** selection list, choose how the gateway handles check-sync SIP NOTIFY messages.
- 4) Click **Apply**.

Result

The SIP Gateway will handle reboot SIP NOTIFY messages and the check-sync SIP NOTIFY messages as configured.

Event Handling		
Gateway Name	Reboot	CheckSync
phone_lines_gw	Rejected ▼	TransferScript ▼
trunk_lines_gw	Restart ▼	CWMP INFORM ▼

10.7.2.12 Enabling Messaging Subscription

Steps

- 1) Go to **SIP/Misc**.
- 2) In the **Messaging Subscription** table, from the selection list, choose **Enable**.
- 3) Click **Apply**.

Result

The unit will add the username in the request URI of MWI SUBSCRIBE requests.

Messaging Subscription	
Username in Request-URI:	Enable ▾

10.7.2.13 Configuring Advice of Charge (AOC)

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **AOC** table, for each gateway, choose from the **AOC-D Support** and **AOCE Support** fields how the AOC-D and AOC-E messages are sent.
- 3) Click **Apply**.

Result

The current charge will be sent either (D)uring the call in AOC-D messages or at the (E)nd of the call in AOC-E messages.

AOC			
Gateway Name	AOC-D Support	AOC-E Support	
phone_lines_gw	Transparent ▾	Transparent ▾	
trunk_lines_gw	Disabled ▾	Transparent ▾	

10.7.2.14 Enabling the Media Security Agreement Parameter

Steps

- 1) Go to **SIP/Misc.**
- 2) In the **Security Mechanism Agreement** table, from the **Media Security Agreement** selection list, choose **Enable**.
- 3) Click **Apply**.

Result

Once enabled, security headers are added to the SIP signalling to agree upon the security mechanism to be used for the media, i.e. SRTP with SDES.

Security Mechanism Agreement	
Media Security Agreement:	Enable v

10.7.3 Advanced Misc SIP Parameters

Although most of the DGW parameters can be configured in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- To set the forked provisional responses behaviour::
SipEp.interopForkedProvisionalResponsesBehavior
- To set the DNS failure concealment parameter: **Sip.DnsFailureConcealment**

Note: This parameter applies only to Endpoint Gateway types; it has no effect on Trunk Gateways. The behavior on Trunk Gateways always matches the "none" value.

11 MEDIA

11.1 Codec

11.1.1 Basic Codec Concepts

11.1.1.1 Codec Configuration

This document describes the steps required to enable or disable the codecs of the Mediatrix unit, as well as access the codec-specific parameters.

The Codec section allows setting two types of configurations:

- Default configurations that apply to all endpoints of the Mediatrix unit.
- Specific configurations that override the default configurations. Specific configurations can be set for each endpoint in the Mediatrix unit.

11.1.1.2 Codec Vs Bearer Capabilities

The Codec Vs. Bearer Capabilities Mapping section allows you to select the codec to prioritise or select in the outgoing INVITE when the incoming SETUP ITC (Information Transfer Capability) matches the configured one. It is also possible to select the ITC value to set in the outgoing SETUP bearer capabilities when the incoming INVITE codec matches the configured one.

Note: This section is only available for units with ISDN interfaces.

11.1.1.3 Generic Voice Activity Detection (VAD)

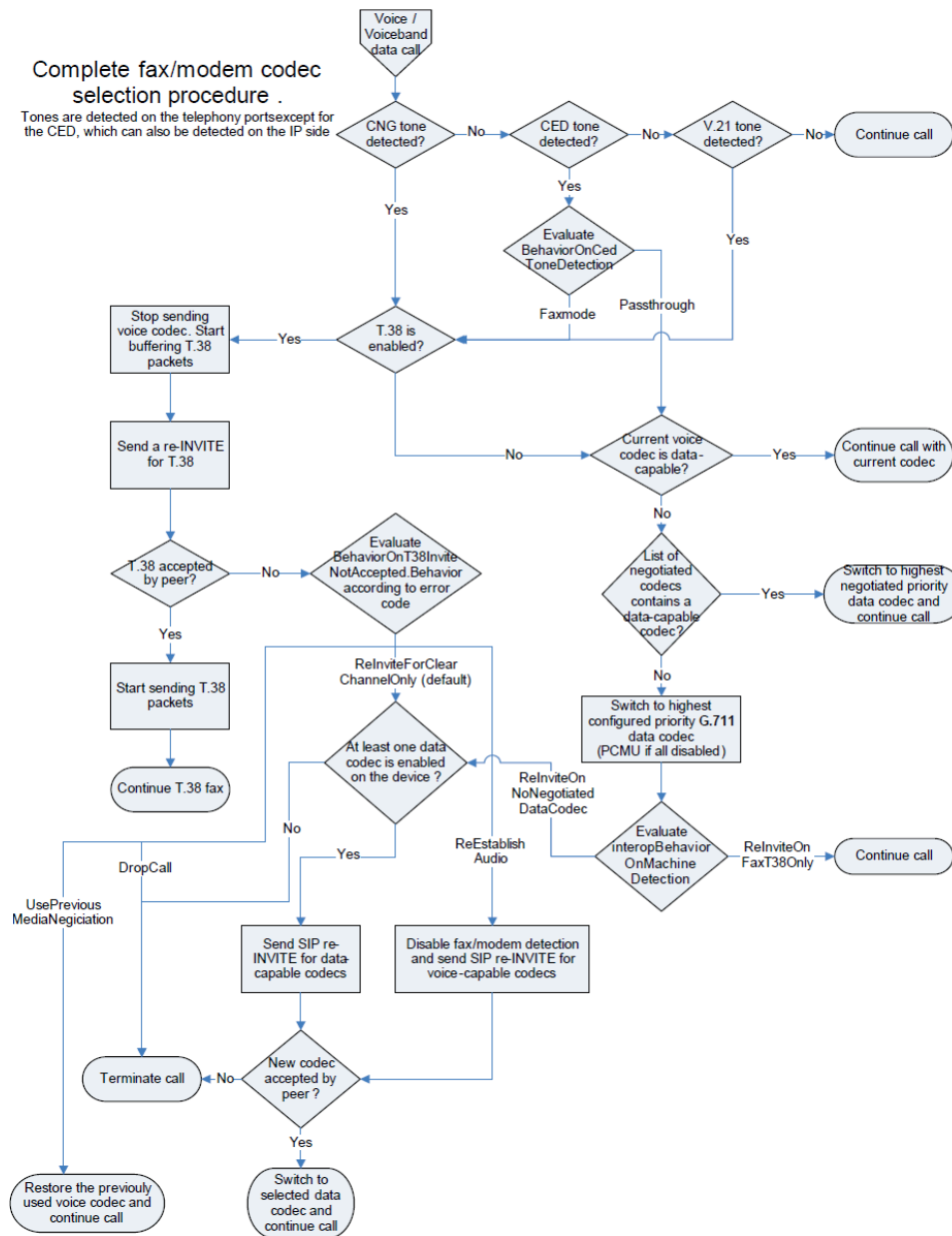
VAD defines how the Mediatrix sends information pertaining to silence. This allows the unit to detect when the user talks, thus avoiding to send silent RTP packets.

The Generic Voice Activity Detection (VAD) section allows selecting two types of configurations:

- Default configurations that apply to all endpoints of the Mediatrix unit.
- Specific configurations that override the default configurations. Specific configurations can be set for each endpoint in the Mediatrix unit.

11.1.1.4 Data Codec Selection Procedure Flow

The Mediatrix unit follows a procedure when selecting data codec. This procedure is the Mediatrix unit default behaviour. Some interop parameter may modify this procedure. Tones are detected on the analog ports only.



11.1.2 Basic Codec Tasks

11.1.2.1 Mipt Default vs Specific Endpoint Configuration Examples

Global>Mipt.EpSpecificCodec

EpId	EnableConfig	GenericVoiceActivityDetection
FX01	Disable	Conservative
FX02	Disable	Conservative
FX03	Disable	Conservative
FX04	Disable	Conservative
FXS1	Disable	Conservative
FXS2	Disable	Conservative
FXS3	Disable	Conservative
FXS4	Disable	Conservative

Global>Mipt.epSpecificCodecG711Mulaw

EpId	EnableConfig	VoiceEnable	VoicePriority	DataEnable
FX01	Disable	Enable	0	Enable
FX02	Disable	Enable	0	Enable
FX03	Disable	Enable	0	Enable
FX04	Disable	Enable	0	Enable
FXS1	Disable	Enable	0	Enable
FXS2	Disable	Enable	0	Enable
FXS3	Disable	Enable	0	Enable
FXS4	Disable	Enable	0	Enable

EpId	DataPriority	MinPtime	MaxPtime
FX01	0	30	30
FX02	0	30	30
FX03	0	30	30
FX04	0	30	30
FXS1	0	30	30
FXS2	0	30	30
FXS3	0	30	30
FXS4	0	30	30

```
Global>Mipt.epSpecificCodecG711Mulaw[EpId=FXS1].DataPriority=10
Global>mipt.Restart
Global>Mipt.epSpecificCodecG711Mulaw
```

EpId	EnableConfig	VoiceEnable	VoicePriority	DataEnable
FX01	Disable	Enable	0	Enable
FX02	Disable	Enable	0	Enable
FX03	Disable	Enable	0	Enable
FX04	Disable	Enable	0	Enable
FXS1	Disable	Enable	0	Enable
FXS2	Disable	Enable	0	Enable
FXS3	Disable	Enable	0	Enable
FXS4	Disable	Enable	0	Enable

EpId	DataPriority	MinPtime	MaxPtime
FX01	0	30	30
FX02	0	30	30
FX03	0	30	30
FX04	0	30	30
FXS1	10	30	30
FXS2	0	30	30
FXS3	0	30	30
FXS4	0	30	30

```
Global>Mipt.EpSpecificCodec[EpId=FXS1].EnableConfig=Enable
Global>Mipt.EpSpecificCodec[EpId=FXS1].GenericVoiceActivityDetection=Transparent
Global>Mipt.EpSpecificCodec
```

EpId	EnableConfig	GenericVoiceActivityDetection
FX01	Disable	Conservative
FX02	Disable	Conservative
FX03	Disable	Conservative
FX04	Disable	Conservative
FXS1	Enable	Transparent
FXS2	Disable	Conservative
FXS3	Disable	Conservative
FXS4	Disable	Conservative

11.1.2.2 Enabling Default Codecs

Steps

- 1) Go to **Media/Codecs**.

- 2) From the **Select Codec Bank**, choose if you want the G.722 , the G.723.1, G.726 or G.729 codec.

Note: All Codec Banks include the T.38, the Clear Mode, the Clear Channel, and the X-CCD codecs.

- 3) In the **Codec** table, select the desired codecs and **Enable** / **Disable** them.

Note: Codecs that appear in Red are not part of the selected codec Bank, thus they can be disabled without a problem.

- 4) Click  for Advanced codec settings.

Note: When enabling two codecs or more, the priority order can be modified by selecting the advanced options.

- 5) Click **Apply**.

Result

Select Codec Bank: G.723.1, G.726, and G.729 (always includes G.711, T.38, Clear Mode, Clear Channel, and X-CCD)
 Select Endpoint: Default

Codec	Voice	Data	Advanced	
G.711 a-Law	Enable	Enable		
G.711 u-Law	Enable	Enable		
G.722	Disable			
G.723.1	Disable			
G.726 16Kbps	Disable			
G.726 24Kbps	Disable			
G.726 32Kbps	Disable	Disable		
G.726 40Kbps	Disable	Disable		
G.729	Enable			
T.38		Enable		
Clear Mode	Disable	Disable		
Clear Channel	Disable	Enable		
X-CCD	Disable	Disable		

11.1.2.3 Enabling Codecs For Specific Endpoints

Steps

- 1) Go to **Media/Codecs**.
- 2) From the **Select Codec Bank**, choose if you want the G.722 , the G.723.1, G.726 or G.729 codec.

Note: All Codec Banks include the T.38, the Clear Mode, the Clear Channel, and the X-CCD codecs.

- 3) From the **Select Endpoint** drop-down list select the port you want to configure.

- 4) In the **Codec** table, from the **Endpoint Specific** drop-down list, select **Yes** for the desired codecs and **Enable/Disable** them.

Note: When enabling two codecs or more, the priority order can be modified by selecting the advanced options.

- 5) Click  for Advanced codec options.
- 6) Click **Apply**.

Result

Select Codec Bank: G.723.1, G.726, and G.729 (always includes G.711, T.38, Clear Mode, Clear Channel, and X-CCD)

Select Endpoint: Slot1/E1T1

Codec	Endpoint Specific	Voice	Data	Advanced	
G.711 a-Law	Yes	Enable	Disable		
G.711 u-Law	Yes	Enable	Disable		
G.722	No	Disable			
G.723.1	No	Enable			
G.726 16Kbps	No	Disable			
G.726 24Kbps	No	Disable			
G.726 32Kbps	No	Disable	Disable		
G.726 40Kbps	No	Disable	Disable		
G.729	No	Enable			
T.38	Yes		Enable		
Clear Mode	No	Disable	Disable		
Clear Channel	No	Disable	Disable		
X-CCD	No	Disable	Disable		

11.1.2.4 Configuring Codec Vs. Bearer Capabilities Mapping

Steps

- 1) Go to **Media/Codecs**.
- 2) In the **Codecs vs. Bearer Capabilities Mapping** table, select **Enable** from the **Enable** drop-down list.
- 3) For each enabled codec, complete the fields are required.
- 4) Click **Apply**.

Result

Codec vs. Bearer Capabilities Mapping					
Index	Enable	Codec	Mapping Type	ITC	
1	Enable	Clear Mode	Prioritize	unrestricted	
2	Disable	G.729	Prioritize	speech	
3	Disable	G.729	Prioritize	speech	

11.1.2.5 Configuring Generic Voice Activity Detection (VAD)

Steps

- 1) Go to **Media/Codecs**.
- 2) From the **Select Codec Bank**, choose if you want the G.722 , the G.723.1, G.726 or G.729 codec.

Note: All Codec Banks include the T.38, the Clear Mode, the Clear Channel, and the X-CCD codecs.

- 3) In the **Generic Voice Activity Detection (VAD)** table,
- 4) set **Enable (G.711, G.722 and G.726)** to the proper setting from the drop-down list.
- 5) Click **Apply**.

Result

Generic Voice Activity Detection (VAD)	
Enable (G.711, G.722, and G.726):	Disable

11.1.2.6 Configuring Generic Voice Activity Detection (VAD) For Specific Endpoint

Steps

- 1) Go to **Media/Codecs**.
- 2) From the **Select Endpoint** drop-down list select the port to configure.
- 3) In the **Generic Voice Activity Detection (VAD)** table, from the **Endpoint Specific** drop-down list, select **Yes**.
- 4) Enable the G.711 and G.726 Voice Activity Detection (VAD) by selecting the proper setting in the drop-down list.
- 5) Click **Apply**.

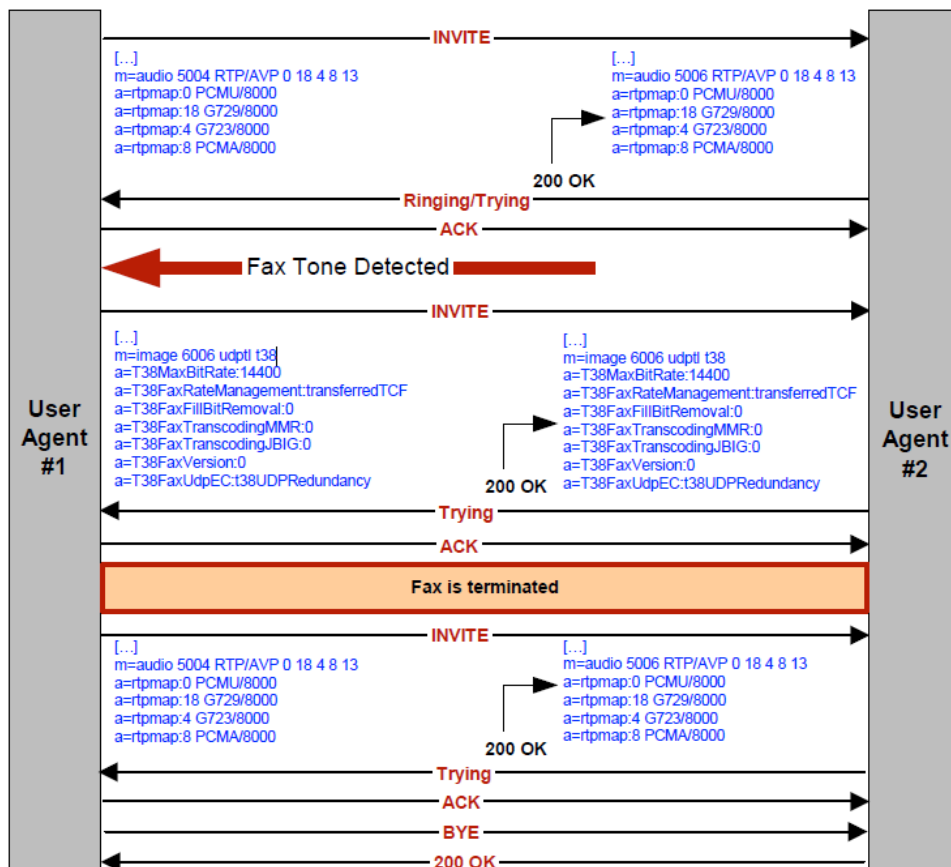
Result

Generic Voice Activity Detection (VAD)	
Endpoint Specific:	Yes
Enable (G.711, G.722, and G.726):	Disable

11.1.3 Basic Fax Concepts

11.1.3.1 T.38 Fax

The Mediatrix unit can send faxes in T.38 mode over UDP. T.38 is used for fax if both units are T.38 capable; otherwise, transmission in clear channel over G.711 as defined is used (if G.711 μ -law and/or G.711 A-law are enabled). If no clear channel codecs are enabled and the other endpoint is not T.38 capable, the fax transmission fails.



Note: The Mediatrix unit opens the T.38 channel only after receiving the "200 OK" message from the peer.

Note: Media5 recommends not to use a fax that does not send a CNG tone. If using such a fax to send a fax communication to the public network, this might result in a communication failure.

11.1.3.2 Fax Parameters

The Mediatrix unit handles G3 fax transmissions at speeds up to 14.4 kbps. Automatic fax mode detection is standard on all endpoints. Real-Time Fax Over UDP with the T.38 protocol stack is also available.

A fax call works much like a regular voice call, with the following differences:

- The fax codec may be re-negotiated by using a reINVITE.
- The goal of the reINVITE is to allow both user agents to agree on a fax codec, which is either:
 - Clear channel (G.711 or G.726) without Echo Cancellation nor Silence Suppression (automatically disabled).
 - T.38.
- Upon fax termination, if the call is not BYE, the previous voice codec is recovered with another reINVITE.
- For fax speeds higher than 14.4 kbps, the Clear channel codec is recommended.

11.1.3.3 Fax Information Required for Troubleshooting

Information	Type	
Fax Transmission Protocol	Clear Mode	T.38
Fax Transmission Speed	High speed	Low speed
Fax mode	Automatic	Manual
Receiving fax	Model	Make
Sending fax	Model	Make
Fax mode	ECM	non- ECM
Firewall	Yes	No

11.1.3.4 T.38 Fax Transmission

T.38 is an ITU recommendation for allowing transmission of fax over IP networks in real time.

PROs

- Allows for redundancy, therefore increases the reliability of the transmissions.
- Faxes in T.38 are not as sensitive to network imperfection like packet loss or jitter as faxes in Clear Channel.

CONs

- The number of redundancy packets will increase the bandwidth used
- The higher the speed, the more bandwidth is used.
- May take more bandwidth than a fax in Clear channel.

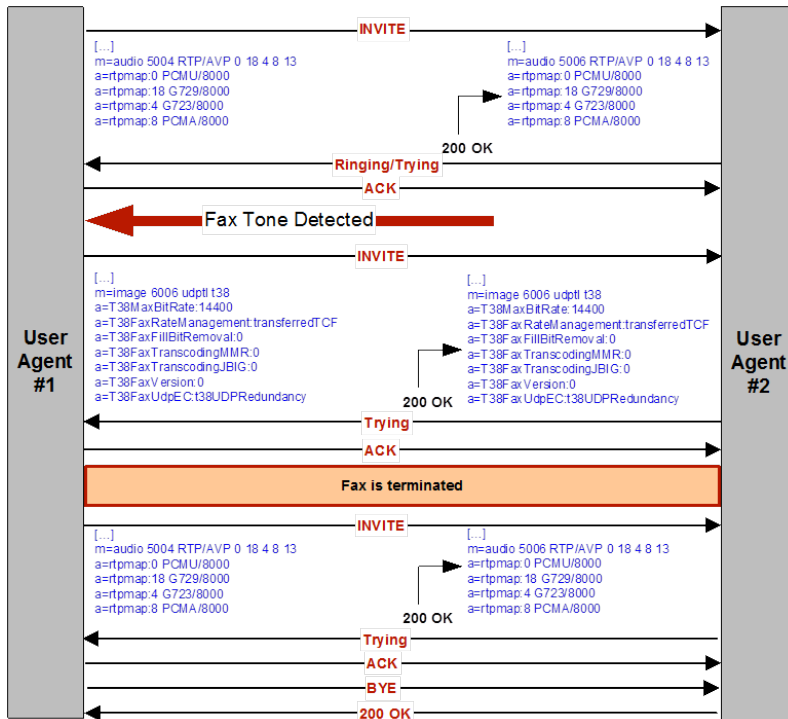
Requirements

- The Mediatrix must be able to detect a CNG , v21 preamble or T.38 packet to switch to T.38
- Reasonable delay, 1 second round trip is acceptable however 2 seconds could cause timeout or collision

Configuration

- [Enabling T.38 Fax Transmission](#) (p.335)
- [Setting the Redundancy Level](#) (p.335)
- [Allowing Unsecure T.38 with Secure RTP](#) (p.341)
- [Selecting the Base Port for T.38 Fax Calls](#) (p.358)
- [Configuring the Behavior of the T.38 INVITE Not Accepted](#) (p.302)

Call Flow



11.1.3.5 Fax Transmission through a Firewall

Using T.38 with a Firewall

Requirements

- The communication channel must remain open for a fax to go through a firewall i.e. the unit sends "no signal" packets to fill the dead air intervals that could occur during a fax transmission and cause the closure of the firewall.

Configuration

- [Configuring the T.38 No Signal](#) (p.336)

11.1.3.6 Clear Channel Fax Transmission

Modulated Fax information from the PSTN is passed in-band end-to-end over a voice speech path in a IP network.

There are 2 pass-through techniques.

- The configured voice codec is used for fax transmission. This technique works only when the configured codec is G711 with no VAD and no echo cancellation (EC) or when the configured codec is a clear channel codec or G.726/32. Low bit-rate codecs cannot be used for fax transmission.

- Gateway dynamically changes the codec from the codec configured for voice to G.711 with no VAD and no EC for the duration of the fax session. This method is referred to as "codec up speed" or "fax pass-through with up speed".

PROs

- Less intrusive, does not modify the packets
- Does not allow for redundancy
- Takes less bandwidth than a T.38 fax transmission
- The bandwidth usage is practically constant.
- Bandwidth only affected by the P-Time.

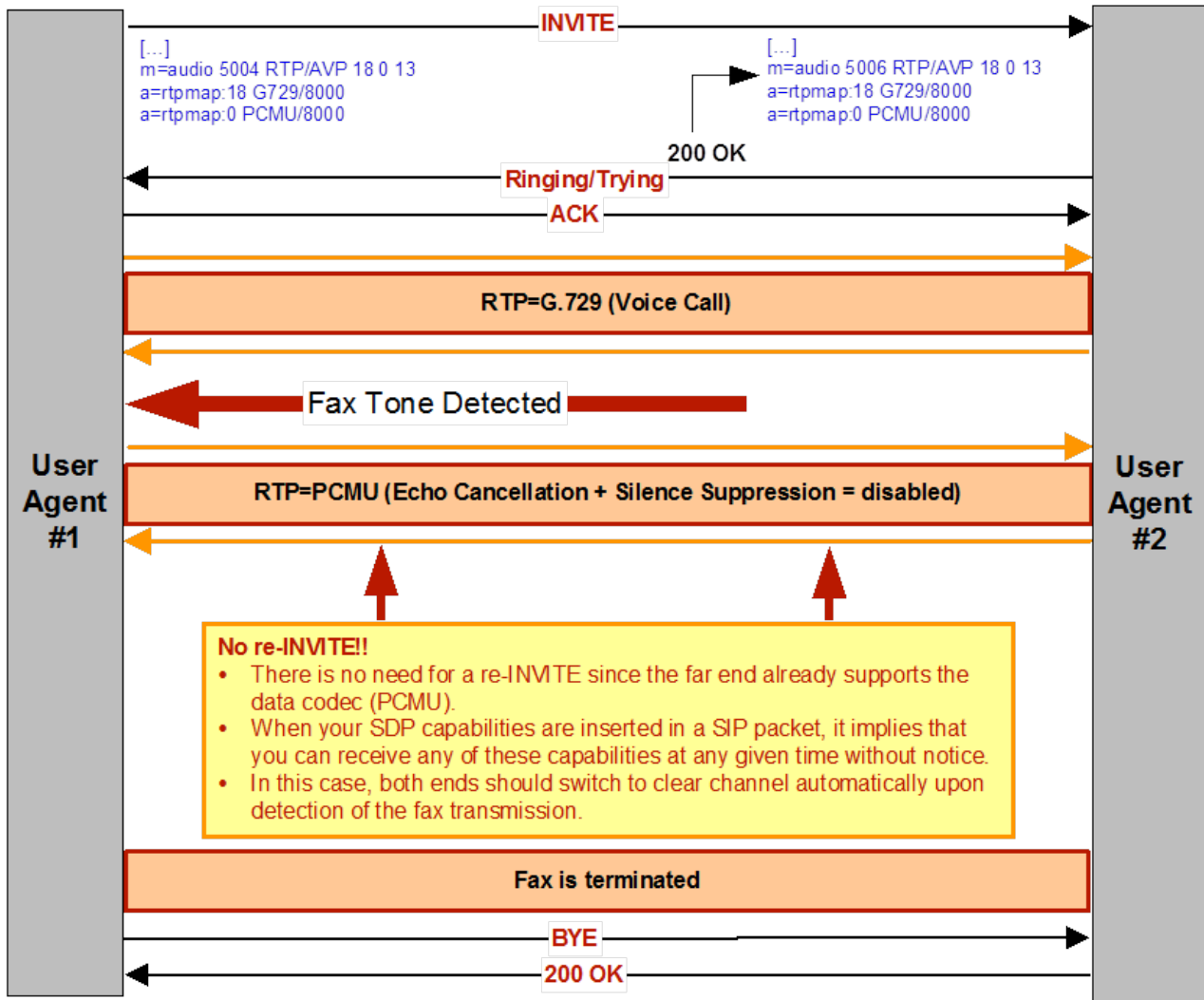
CONs

- Sensitive to network imperfection like packet loss or jitter

Configuration

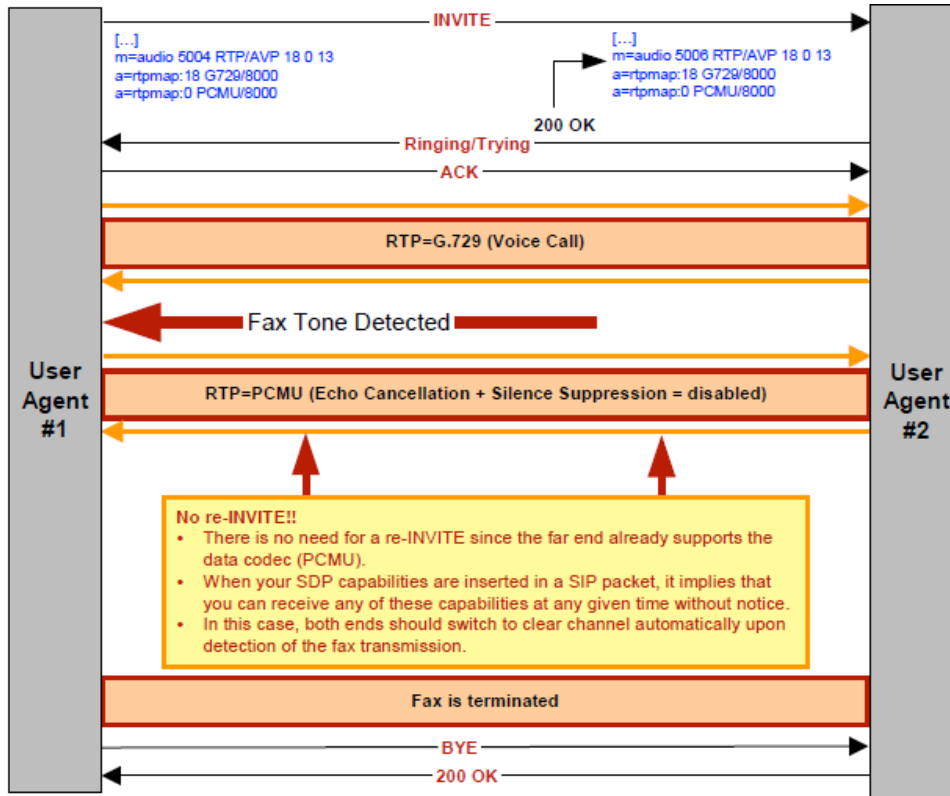
[Configuring the Clear Channel Fax Transmission](#) (p.337)

Call Flow



11.1.3.7 Clear Channel Fax Flow

For more details on Clear Channel Fax limitations, please refer to the [DGW Configuration Guide - Limitations of DGW Platforms](#) published on the [Media5 Documentation Portal](#).



11.1.3.8 FAX Detection Flow

IF	AND	THEN
If T.38 is enabled	- A CNG tone is detected, or - A V.21 preamble is detected, or - T.38 packets are received on the IP side	Then the Mediatix switches to T.38
- If a CED tone is detected (Answer Tone or ANS) and no other conditions indicates that a fax is present, or - If a fax is detected but T.38 is deactivated		Then the Mediatix unit switches to Clear mode.

IF	AND	THEN
If a CED Note: Note that the CED tone can be detected on both the IP side (egress side) or on the analog side (ingress side). is detected before a CNG		The Mediatrix unit will first switch to Clear Channel and if T.38 is enabled, it will then switch to T.38.

11.1.4 Basic Fax Tasks

11.1.4.1 Enabling T.38 Fax Transmission

Steps

- 1) Go to **Media/Codecs**.
- 2) In the **Codec** section, click  located on the same line as **T.38**.
- 3) Set the **Enable** filed to **Enable**.
- 4) Click **Apply**.

Result

T.38	
Enable:	Enable ▼
Priority:	10
Redundancy Level:	3
Detection Threshold:	Default ▼
Frame Redundancy Level:	0
No Signal:	Disable ▼
No Signal Timeout:	1

11.1.4.2 Setting the Redundancy Level

Steps

- 1) Go to **Media/Codecs**.
- 2) In the **Codec** section, click  located on the same line as **T.38**.

- 3) In the **T.38** table, set the **Redundancy Level** .

Note: Using redundancy increases transmission reliability, however the number of redundancy packets will also increase the bandwidth being used.

- 4) Set the **Frame Redundancy Level**.

Note: The repetition of the final frame will help prevent losing the end of a message, v.21 or end of page message. Losing the end of packet message can create a major problem in the transmission since the Redundancy is not use in this situation.

- 5) Click **Apply**.

Result

T.38	
Enable:	Enable ▼
Priority:	10
Redundancy Level:	3
Detection Threshold:	Default ▼
Frame Redundancy Level:	0
No Signal:	Disable ▼
No Signal Timeout:	1

11.1.4.3 Configuring the T.38 No Signal

Steps

- 1) Go to **Media/Codecs**.
- 2) Click  located on the same row as **T.38**.
- 3) Set the **No Signal** selection list to **Enable**.
- 4) Set the **No Signal Timeout** selection list to **Enable**.

Note: In order to keep RTP ports opened for T.38 packets, the unit will send 'no signal' packets to fill the dead air intervals that could occur during a fax transmission and cause the closure of the firewall.

- 5) Click **Apply**.

Result

T.38	
Enable:	Enable ▼
Priority:	10
Redundancy Level:	3
Detection Threshold:	Default ▼
Frame Redundancy Level:	0
No Signal:	Disable ▼
No Signal Timeout:	1

11.1.4.4 Configuring the T.38 No Signal Timeout

Steps

- 1) Go to **Media/Codecs**.
- 2) Click  located on the same row as **T.38**.
- 3) Set the **No Signal Timeout** selection list to **Enable**.

Note: In order to keep RTP ports opened for T.38 packets, the unit will send 'no signal' packets to fill the dead air intervals that could occur during a fax transmission and cause the closure of the firewall.

- 4) Click **Apply**.

Result

T.38	
Enable:	Enable ▼
Priority:	10
Redundancy Level:	3
Detection Threshold:	Default ▼
Frame Redundancy Level:	0
No Signal:	Disable ▼
No Signal Timeout:	1

11.1.4.5 Configuring the Clear Channel Fax Transmission

Steps

- 1) Go to **Media/Codecs**.

- 2) In the **Codec** section, click  located on the same line as the Codec you wish to use for Fax Transmission.
- 3) In the selected Codec table, set the fields as required.
- 4) Make sure to enable the **Data Transmission**.
- 5) Click **Apply**.

Result

For example:

Clear Mode	
Voice Transmission:	Disable ▾
Voice Priority:	0
Data Transmission:	Enable ▾
Data Priority:	10
Payload Type:	124
Minimum Packetization Time:	10 ms ▾
Maximum Packetization Time:	30 ms ▾

11.2 Security

11.2.1 Basic Security Concepts

11.2.1.1 Secure Real-Time Transport Protocol

Secure Real-time Transport Protocol (SRTP) is a profile of Real-time Transport Protocol (RTP) that provides encryption, message authentication, and replay attack protection.

SRTP can be enabled on all Mediatrix unit endpoints, or on one or more specific endpoints. However, SRTP encryption and authentication requires more processing therefore, if SRTP is enabled, the number of calls that the Mediatrix unit can handle simultaneously may be reduced, depending of the enabled codecs . (For more details on resources limitations with SRTP and conferences, refer to the [DGW Configuration Guide - Limitations of DGW Platforms](#) document published on the [Media5 Documentation Portal](#)).

To reduce the impact on the number of simultaneous calls a Mediatrix unit can handle, is it possible to disable all voice or data codec, including the T.38 protocol, and keep only the G.711 voice codec enabled.

IMPORTANT: If Secure RTP (SRTP) is enabled on at least one line, it is acceptable to have the secure SIP transport (TLS) disabled for testing purposes. However, this configuration must never be used in a production environment, since an attacker could easily break it. Enabling TLS for SIP Transport

is strongly recommended and is usually mandatory for security interoperability with third-party equipments.

The Mediatrix unit supports the MIKEY protocol using pre-shared keys (MIKEY-PS as per RFC 3830) or the SDES protocol for negotiating SRTP keys

11.2.2 Basic Tasks

11.2.2.1 Enabling Secure Media (SRTP) on All Endpoints

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose **Default**.
- 3) In the **Security** table,
 - a) From the **Mode** drop box, select **Secure** or **Secure with fallback**.
 - b) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the **a=crypto** line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the **a=key-mgmt :mikey** line within the SDP Session Attributes.

- c) From the drop box, select the **AES_CM_128** encryption algorithm.
- d) From the **Allow Unsecure T.38 with Secure RTP** selection, choose if unsecure **T.38** is allowed with RTP.

Note: **T.38** packets will never be encrypted. The setting **Allow Unsecure T.38 with Secure RTP** will make possible to use **T.38**, otherwise it will be rejected. If not using **T.38** for faxing, to avoid an impact on the number of simultaneous calls a Mediatrix unit can handle in SRTP, set the **Allow Unsecure T.38 with Secure RTP** parameter to **No** and refer to the [Standard Fax Configuration](#) document to disable **T.38** Fax Transmission.

- 4) In the **SRTP Preferences** table,
 - a) From the **Crypto Mode When Sending Offer** drop box, select the preferred mode.
 - b) From the **Crypto Mode When Sending Answer** drop box, select the preferred mode.
 - c) From the **Crypto Context Behavior** drop box, select the preferred behavior.

Note: For more information about the recommended **SRTP Preferences**, please refer to [Recommended SRTP Preferences for a Typical VoIP Network](#) section of the [Setting the Security Parameters of the RTP Stream](#) document.

Note: For troubleshooting the SRTP interoperability, please refer to the [SRTP Troubleshooting](#) document.

- 5) Click **Apply**.

Result

All new SIP exchanges will contain RTP/SAVP negotiation elements.

Select Endpoint: Default ▾

Security	
RTP	
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾
T.38	
Allow unsecure T.38 with secure RTP:	No ▾

SRTP Preferences	
Crypto Mode When Sending Offer:	Mode when sending SDP offer with SRTP ▾
Crypto Mode When Sending Answer:	Mode when sending SDP answer with SRT ▾
Crypto Context Behavior:	Behavior of the SRTP Context ▾

11.2.2.2 Enabling Secure Media (SRTP) on a Specific Endpoint

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose an endpoint.

Note: The list of available endpoints will vary depending on the type of unit being used.

- 3) In the **Security** table, from the **Mode** drop box, select **Secure** or **Secure with fallback**.
- 4) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the a=crypto line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the a=key-mgmt:mikey line within the SDP Session Attributes.

- 5) From the drop box, select the **AES_CM_128** encryption algorithm.
- 6) Click **Apply**.

Result

All new SIP exchanges going through the specified endpoint will contain RTP/SAVP negotiation elements.

Select Endpoint: Chosen Endpoint ▾

Security	
RTP	
Endpoint Specific:	Yes ▾
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾

11.2.2.3 Allowing Unsecure T.38 with Secure RTP

Information

The T.38 protocol must be enabled under **Media/Codec**.

This procedure is required only if SRTP is used and is available provided the **Select Endpoint** selection list is set to **Default**.

Steps

- 1) Go to **Media/Security**.
- 2) In the **Security** table, under the **RTP** section, set the **Mode** selection list to **Secure with fallback**.
- 3) Under the **T.38** section, set the **Allow Unsecure T.38 with Secure RTP** selection list to **Yes**.
- 4) Click **Apply**.

Result

Select Endpoint: Default 

Security	
RTP	
Mode:	Secure with fallback 
Key Management Protocol:	Key Management Protocol for SRTP 
Encryption:	AES_CM_128 
T.38	
Allow unsecure T.38 with secure RTP:	Yes 

11.2.2.4 Modifying the SRTP Basic Port

Steps

- 1) Go to **Media/Misc.**
- 2) In the **Base Ports** table, in the field next to **SRTP**, indicate in the field to first port to use in SRTP.

Result

The first port to be used in SRTP will be the one specified.

Base Ports	
RTP:	5004
SRTP:	First port to use
T.38:	6004

11.2.3 Advanced RTP Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- **Mipt.EnforceSymmetricRtpEnable:** to enforce that incoming RTP packets are from the same source as the destination of outgoing RTP packets.

- **Mipt.InteropDtmfRtpInitialPacketQty:** to specify the quantity of packets sent at the beginning and at the ending of an Out-of-Band DTMF using RTP.
- **Mipt.InteropPacketReceptionMode:** to select the mode that control the range of packetisation times (ptime) applied at the reception of RTP packets.

11.3 RTP Statistics Configuration

11.3.1 Basic RTP Statistics Concepts

11.3.1.1 RTP Packet Statistics

The Mediatrix unit collects valuable RTP statistics that can be read via the DGW Web interface, SNMP, and the CLI.

The statistics are sent as Mipt notification messages, therefore the syslog information must be configured properly before setting the statistics (under **System/ Event Log/Notification Events**). (For more details, refer to the [DGW Configuration Guide - Generating Logs](#) published on the [Media5 Documentation Portal](#)).

There are two types of statistics:

- statistics for the last 10 connections (under **Media/RTP Statistics/Connection Statistics**)
- statistics for the last 10 collection periods (under **Media/RTP Statistics/Collection Period Statistics**)

Statistic	Connection Statistics	Collection Period Statistics
Octets Tx	Number of octets transmitted during the connection.	Number of octets transmitted during the collection period. This value is obtained by cumulating the octets transmitted in all connections that were active during the collection period.
Octets Rx	Number of octets received during the connection.	Number of octets received during the collection period. This value is obtained by cumulating the octets received in all connections that were active during the collection period.
Packets Tx	Number of packets transmitted during the connection.	Number of packets transmitted during the collection period. This value is obtained by cumulating the packets transmitted in all connections that were active during the collection period.
Packets Rx	Number of packets received during the connection.	Number of packets received during the collection period. This value is obtained by cumulating the packets received in all connections that were active during the collection period.
Packets Lost	Number of packets lost during the connection. This value is obtained by subtracting the expected number of packets based on the sequence number from the number of packets received.	Number of packets lost during the collection period. This value is obtained by cumulating the packets lost in all connections that were active during the collection period.
Min. Jitter	Minimum interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Minimum interarrival time, in ms, during the collection period. This value is the lowest interarrival jitter for all connections that were active during the collection period.

Statistic	Connection Statistics	Collection Period Statistics
Max. Jitter	Maximum interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Maximum interarrival time, in ms, during the collection period. This value is the highest interarrival jitter for all connections that were active during the collection period.
Avg. Jitter	Average interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Average interarrival time, in ms, during the collection period. This value is the weighted average of the interarrival jitter for all connections that were active during the collection period. For each connection, the total jitter of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.
Min. Latency	Minimum latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Minimum latency, in ms, during the collection period. This value is the lowest latency for all connections that were active during the collection period.
Max. Latency	Maximum latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Maximum latency, in ms, during the collection period. This value is the highest latency for all connections that were active during the collection period.

Statistic	Connection Statistics	Collection Period Statistics
Avg. Latency	Average latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Average latency, in ms, during the collection period. This value is the weighted average of the latency for all connections that were active during the collection period. For each connection, the total latency of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.

11.3.1.2 Channel Statistics

The Mediatrix unit collects valuable RTP statistics that can be read via SNMP and the CLI. Channel statistics are cumulated RTP statistics for all calls using a specific channel of a telephony interface. Channel statistics are updated at the end of each call.

The statistics are associated with the channel in use at the end of the call. In some cases, such as in hold/resume scenarios, the channel assignment may change during a call. This can result in discrepancies between the RTP statistics and the actual usage of the telephony interface.

Parameter	Description
PacketsSent	Number of packets transmitted on the channel since service start. This value is obtained by cumulating the packets transmitted in all the connections that ended during the collection period.
PacketsReceived	Number of packets received on the channel since service start. This value is obtained by cumulating the packets received in all the connections that ended during the collection period.
BytesSent	Number of bytes transmitted on the channel since service start. This value is obtained by cumulating the bytes transmitted in all the connections that ended during the collection period.
BytesReceived	Number of bytes received on the channel since service start. This value is obtained by cumulating the bytes received in all the connections that ended during the collection period.
AverageReceiveInterarrivalJitter	Average interarrival time, in microseconds, for the channel since service start. This value is based on the average interarrival jitter of each call ended during the collection period. The value is weighted by the duration of the calls.

11.3.2 Basic Tasks

11.3.2.1 Configuring RTP Statistic Collection

Before you start

You must set the Media IP Transport (Mipt) service to the Info or Debug level (under **System/Event Log**).

Steps

- 1) Go to **Media/RTP Statistics**.
- 2) In the **Statistics Configuration** table, set the **Collection Period (minutes)** parameter.

Note: The value 0 disables the collection period statistics feature.

- 3) From the **End-of-Connection Notification** selection list, choose whether or not to enable end-of-connection notifications.
- 4) From the **End-of-Period Notification** selection list, choose whether or not to enable end-of-period notifications.

- 5) Click **Apply** or **Apply & Reset Current Collection Period Statistics**

11.3.3 Advanced RTP Statistic Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI

For more details, refer to the [DGW Configuration Guides - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- **Mipt.ChannelStatistics**: Table with Statistics per endpoint/channel since last reboot or statistics reset.
- **Mipt.ChannelStatistics.Reset**: To reset channel statistics values of a specific endpoint to zero: **Mipt.ChannelStatistics[EpChannelId=<endpoint>].Reset=Reset** For example: **Mipt.ChannelStatistics[EpChannelId=FXS1].Reset=Reset**
- **Mipt.StatsCollectionPeriodDuration**: Specifies the collection period duration (in minutes).
- **Mipt.StatsPerConnectionNotificationEnable**: Enables the generation of connection end statistics notification.
- **Mipt.StatsPerPeriodNotificationEnable**: Enables the generation of period statistics notification.
- **Mipt.LastConnectionsStats**: Table with Last 10 connections statistics.
- **Mipt.LastPeriodsStats**: Table with Last 10 periods statistics.
- **Mipt.MinSeverity**: To set the minimal severity to issue a notification message incoming from this service.

11.4 Misc

11.4.1 Basic Media Misc Concepts

11.4.1.1 Jitter Buffer

Because of network congestion, timing drift, or route changes, data packets can arrive at different intervals and pace. These variations in packet arrival time are called jitter which can be the cause of sound distortion. To insure a clear connection, incoming voice data packets are intentionally delayed by a jitter buffer and then sent in evenly spaced intervals to the voice processor.

Media5 recommends to avoid changing the target and maximum jitter buffer values unless experiencing or strongly expecting one of the following symptoms:

- If the voice is scattered, try to increase the maximum jitter buffer value.
- If the delay in the voice path (end to end) is too long, you can lower the target jitter value, ONLY if the end-to-end delay measured matches the target jitter value

For instance, if the target jitter value is 50 ms, the maximum jitter is 300 ms and the delay measured is 260 ms, it would serve nothing to reduce the target jitter.

However, if the target jitter value is 100 ms and the measured delay is between 100 ms and 110 ms, then you can lower the target jitter from 100 ms to 30 ms.

11.4.1.2 Dual Tone Multi Frequency (DTMF)

DTMF (dual tone multi frequency) is the signal that is generated from a touch key of a phone and that is sent to the phone company.

DTMF, also commonly called Touchtone, has replaced loop disconnect dialing, also called pulse dialing. With DTMF, each key of the phone combines one tone from a high-frequency group of tones and a tone from low frequency group.

Key digit	Low frequency (Hz)	High Frequency (Hz)
1	697	1209
2	697	1336
3	697	1477
4	770	1209
5	770	1336
6	770	1477
7	852	1209
8	852	1336
9	852	1477
0	941	1209
*	941	1336
#	941	1477

11.4.1.3 DTMF Out-of-Band Transport Method

When using the Out-of-Band transport method, the DTMFs and the voice are transmitted in two different streams where the voice is sent over RTP, but DTMF is sent either in RTP or SIP depending on the chosen transport method (**Out-of-Band using RTP** or **Out-of-Band using SIP**). However, the Out-of-Band transport method can only be used if the SIP peer supports the method, otherwise the DTMF transport method falls back to In-band.

Because some 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 regenerating the true tones. Such a mechanism is known as Out-of-Band DTMF. The Mediatrix unit receives and sends Out-of-Band DTMFs as per ITU Q.24. DTMFs supported are 0-9, A-D, *, #.

The DTMF Out-of-Band (using either SIP or RTP) transport method is configurable by endpoint, or can be selected for all the endpoints of the unit. ISDN endpoints are normally configured to use an Out-of-Band transport method for DTMF transmission.

11.4.1.4 DTMF In-band Transport Method

This is the most used transport method for DTMFs transmission. In this case, the DTMFs and the voice are transmitted together in the RTP stream.

This transport method is only reliable with G.711 or G.729 codecs. The DTMF In-band transport method is configurable by endpoint, or the same method can be selected for all the endpoints of the unit. In general, FXS, FXO, R2, and E&M endpoints are configured to use the In-band transport method for DTMF transmission.

11.4.2 Basic Media Misc Tasks

11.4.2.1 Configuring the Jitter Buffer of all Endpoints

Steps

- 1) Go to **Media/Misc**.
- 2) From the **Select Endpoint** drop down list, choose **Default**.
- 3) In the **Jitter Buffer** table, from the **Level** selection list choose one of the following
 - **Normal**
 - **Optimize Quality**
 - **Optimize Latency**
- 4) Click **Apply**.

Result

All endpoints of the unit will be configured with the same jitter buffer.

Jitter Buffer	
Level:	Normal
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed
Minimum:	0
Nominal:	67
Maximum:	135

11.4.2.2 Configuring the Jitter Buffer of a Specific Endpoint

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose the endpoint for which the jitter buffer need to be configured.
- 3) In the **Jitter Buffer** table, from the **Endpoint Specific** selection list, choose **Enable**.
- 4) From the **Level** selection list choose one of the following:
 - **Normal**
 - **Optimize Quality**
 - **Optimize Latency**
- 5) Click **Apply**.

Result

The selected endpoint of the unit will have the customised jitter buffer.

Jitter Buffer	
Endpoint Specific:	Enable ▾
Level:	Optimize Quality ▾
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed ▾
Minimum:	0
Nominal:	67
Maximum:	125

11.4.2.3 Configuring the Jitter Buffer of all Endpoints for Fax/Modem

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose **Default**.
- 3) In the **Jitter Buffer** table, from the **Level** selection list, choose **Fax/Modem**.
- 4) Click **Apply**.

Result

All endpoints of the unit will be configured with a jitter buffer for Fax/Modem.

Jitter Buffer	
Level:	Fax / Modem
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed
Minimum:	0
Nominal:	67
Maximum:	135

11.4.2.4 Configuring the Jitter Buffer of a Specific Endpoint for Fax/Modem

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose the endpoint you wish to configure for fax or modem.
- 3) In the **Jitter Buffer** table, from the **Endpoint Specific** selection list, choose **Enable**.
- 4) From the **Level** selection list, choose **Fax/Modem**.
- 5) Click **Apply**.

Result

The selected endpoint will be configured with a jitter buffer for Fax/Modem.

Jitter Buffer	
Endpoint Specific:	Enable v
Level:	Fax / Modem v
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed v
Minimum:	0
Nominal:	67
Maximum:	125

11.4.2.5 Customising the Jitter Buffer of all Endpoints

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose **Default**.
- 3) In the **Jitter Buffer** table, from the **Level** selection list, choose **Custom**.
- 4) Complete the fields of the **Voice Call** and **Data Call** sections.
- 5) Click **Apply**.

Result

All endpoints of the unit will have the configured jitter buffer.

Jitter Buffer	
Level:	Custom v
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed v
Minimum:	0
Nominal:	67
Maximum:	135

11.4.2.6 Customising the Jitter Buffer of a Specific Endpoint

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose an endpoint.
- 3) In the **Jitter Buffer** table, from the **Endpoint Specific** selection list, choose **Enable**.
- 4) From the **Level** selection list, choose **Custom**.
- 5) Complete the fields of the **Voice Call** and **Data Call** sections.
- 6) Click **Apply**.

Result

The selected endpoint of the unit will have the selected jitter buffer.

Jitter Buffer	
Endpoint Specific:	Enable ▾
Level:	Custom ▾
Voice Call	
Minimum:	30
Nominal:	0
Maximum:	125
Data Call	
Playout Type:	Fixed ▾
Minimum:	0
Nominal:	67
Maximum:	125

11.4.2.7 Configuring Machine Detection

Information

Note: This procedure is only required if your fax machine is directly connected to a specific FXS port and if this port is not used for modem transmission.

Steps

- 1) Go to **Media/Misc.**
- 2) Set the **CNG Tone Detection** selection list to **Enable**.
- 3) Set the **CED Tone Detection** selection list to **Enable**.
- 4) Set the **V.21 Modulation Detection** selection list to **Enable**.
- 5) Set the **Behavior On CED Tone Detection** selection list to **Fax Mode**.
- 6) Click **Apply**.

Result

Machine Detection	
CNG Tone Detection:	Enable ▾
CED Tone Detection:	Enable ▾
V.21 Modulation Detection:	Enable ▾
Behavior On CED Tone Detection:	Fax Mode ▾

11.4.2.8 Configuring DTMF Transport for all Endpoints

Steps

- 1) Go to **Media/Misc.**
- 2) From the **Select Endpoint** drop down list, choose **Default**.

- 3) From the **Transport Method** drop down list, choose the transport method set in the VoIP server.
 - a) **In-band**
 - b) **Out-of-Band using RTP**, (RFC2833). This is usually the preferred method. Remember to set the payload type if different (e.g.: 96, 101 or 110 in some cases)
 - c) **Out-of-Band using SIP**. For Cisco or Avaya systems, from the **SIP Transport Method** field use **Info DTMF Relay**. For legacy Nortel and others, leave **Draft Choudhuri SIP Info Digit 00**.
 - d) **Signaling Protocol Dependent** choose this method if unsure. It will try to use the method negotiated by the VoIP server.
- 4) Click **Apply**.

Result

The selected DTMF transport will be applied to all endpoints unless an endpoint was specifically configured using [Configuring DTMF Transport for a Specific Endpoint](#) (p.357) .

DTMF Transport		
Transport Method:	Out-of-Band using RTP	
SIP Transport Method:	Draft Choudhuri SIP Info Digit 00	
Payload Type:	101	

11.4.2.9 Configuring DTMF Transport for a Specific Endpoint

Steps

- 1) Go to **Media/Misc**.
- 2) From the **Select Endpoint** drop down list, choose the endpoint for which you wish to configure DTMF transport.
- 3) In the **DTMF Transport** table, from the **Endpoint Specific** drop down list, choose **Enable**.
- 4) From the **Transport Method** drop down list, choose the transport method set in the VoIP server.
 - a) **In-band**
 - b) **Out-of-Band using RTP**, (RFC2833). This is usually the preferred method. Remember to set the payload type if different (e.g.: 96, 101 or 110 in some cases)
 - c) **Out-of-Band using SIP**. For Cisco or Avaya systems, from the **SIP Transport Method** field use **Info DTMF Relay**. For legacy Nortel and others, leave **Draft Choudhuri SIP Info Digit 00**.
 - d) **Signaling Protocol Dependent** choose this method if unsure. It will try to use the method negotiated by the VoIP server.
- 5) Click **Apply**.

Result

The selected DTMF transport method will be applied to the selected endpoint. All other endpoints, unless they are specifically configured, will use the transport method selected in the [Configuring DTMF Transport for all Endpoints](#) (p.356)..

DTMF Transport	
Endpoint Specific:	Enable v
Transport Method:	Out-of-Band using RTP v
Payload Type:	101

11.4.2.10 Selecting the Base Port for T.38 Fax Calls

Steps

- 1) Go to **Media/Misc.**
- 2) In the **Base Port** table, enter the first port to be used for T.38 Fax calls in the **T.38** field.

Note: If you do not know which port to use, refer to the [Technical Bulletin - Ports and Protocol Settings](#) published on the [Media5 Documentation Portal](#).

- 3) Click **Apply**.

Result

Base Ports	
RTP:	5004
SRTP:	5004
T.38:	First port number to use

11.4.3 Advanced Jitter Buffer Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

To start a call in voiceband data mode: **Telif.InteropDtmfDetectionRiseTimeCriteria**

11.4.4 Advanced DTMF Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configurationn Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

DTMF Detection

- To set the Rise Time criteria: **Telif.InteropDtmfDetectionRiseTimeCriteria**
- To set the Detection Positive Twist: **Telif.InteropDtmfDetectio.PositiveTwist**
- To set the Detection Negative Twist: **Telif.InteropDtmfDetection.NegativeTwist**
- To set the Max Power Threshold: **Telif.InteropDtmfDetection.MaxPowerThreshold**
- To set the Min Power Threshold: **Telif.InteropDtmfDetection.MinPowerThreshold**
- To set the Detection Break Power Threshold:
Telif.InteropDtmfDetection.BreakPowerThreshold

Using the Payload Type Found in the Answer

- To use the payload type found in the answer:**SipEp.InteropUseDtmfPayloadTypeFoundInAnswer**

Initial quantity of RTP packets, only available when using the Out-of-Band using RTP transport method.

- To set the initial quantity of RTP packets: **Mipt.InteropDtmfRtpInitialPacketQty**

12 Telephony

12.1 DTMF Maps

12.1.1 Basic DTMF Maps Concepts

12.1.1.1 DTMF Maps

A DTMF map (also called digit map or dial map) allows you to compare the number users just dialed to a pattern string. Depending on the DTMF maps, the call can be accepted or rejected.

When a number is dialed, it is compared to the numbers of the DTMF maps:

- If the dialed number matches an entry of the **Allowed DTMF Map**, the call is accepted.
- If the dialed number matches an entry of the **Refused DTMF Map** table, then the call is refused and an error tone i.e. reorder tone, network congestion, or fast busy tone is played.
- If the dialed number matches no entry of either the **Allowed DTMF Map** or the **Refused DTMF Map**, the call is refused and an error tone i.e. reorder tone, network congestion, or fast busy tone is played.
- If the dialed number matches an entry of both the **Allowed DTMF Map** and the **Refused DTMF Map**, the call is refused and an error tone i.e. reorder tone, network congestion, or fast busy tone is played.

Note: The **Refused DTMF Map** table has precedence over the **Allowed DTMF Map** table.

12.1.1.2 DTMF Maps Order

The order in which the DTMF maps are used is very important. You must use specific DTMF maps first and then more generic ones. Otherwise you may end up with all calls being directed the same way. This is true when creating the DTMF maps in the **Allowed DTMF Map** table and in the **DTMF Map** field of this table.

For example, lets say

- all employees have a 3-digit extension all starting with 1, 2 or 3.
- All managers have an extension finishing with 9

When a 3-digit extension is dialed, the call should be directed to the colleague's extension. But, you also wish that all calls made to managers be redirected the management's assistant extension.

If you put the DTMF map for management calls first,

```
[1-3]x9
```



```
[1-3]xx
```

calls made to a managers, will always be redirected to the Manager's assistant extension.

On the other hand, if you put the DTMF for extension redirections before the DTMF for management redirection,

```
[1-3]xx  
[1-3]x9
```

managers will always directly receive their calls without going through the Manager's assistant extension.

12.1.1.3 DTMF Map vs DTMF Map Transformation

When creating DTMF maps to allow or refuse calls, the DTMF maps must be written and a transformation to be applied to the dialed number may be required.

The DTMF map is used to recognise the dialed numbers and the transformation modifies the dialed numbers before sending the call. A transformation is not mandatory, it depends if the dialed number must be changed or not before the call is made.

For example, when the dialed number is the extension of a colleague, no transformation is required. The DTMF map will recognise that the dialed numbers are the allowed extension of a colleague, and the call will be made with the dialed number.

However, in the example where calls made to management extensions are redirected to the management's assistant, a transformation is required. For example, if the DTMF is xx9 and the transformation 123, this means that whenever an extension finishing by 9 is dialed, the call is sent to extension 123.

12.1.1.4 DTMF Maps Syntax

The permitted DTMF map syntax is taken from the core MGCP specification, RFC 2705, section 3.4:

```
DigitMap = DigitString / '(' DigitStringList ')'
DigitStringList = DigitString 0* ( '|' DigitString )
DigitString = 1*(DigitStringElement)
DigitStringElement = DigitPosition ['.']
DigitPosition = DigitMapLetter / DigitMapRange
DigitMapLetter = DIGIT / '#' / '*' / 'A' / 'B' / 'C' / 'D' / 'T'
DigitMapRange = 'x' / '[' 1*DigitLetter ']'
DigitLetter ::= ((DIGIT '-' DIGIT) / DigitMapLetter)
```

12.1.1.5 DTMF Maps Special Characters

DTMF maps use specific characters and digits in a particular syntax

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). Note: Enclose the DTMF map in parenthesis when using the “ ” option.
.	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.

12.1.2 Basic DTMF Maps Tasks

12.1.2.1 Configuring Endpoint-Specific DTMF Timers

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) In the **General Configuration** table, click **Edit Endpoints**.
- 3) In the **Endpoint Specific** table, for each Endpoint to configure, from the **Override** selection list, choose **Enable**.
- 4) For each enabled endpoint, complete the timeout fields as required.
- 5) Click **Apply**

Result

Each enabled endpoint will use the endpoint-specific timeout.

12.1.2.2 Creating a DTMF Map that Applies to all Endpoints

Steps

- 1) Go to **Telephony/DTMF Maps**.

- 2) From the **DTMF Map** selection list, choose:
 - a) if you wish to create DTMF maps that accept calls
 - b) **Refused** if you wish to create DTMF maps that refuse calls
- 3) In the **Allowed DTMF Map** or **Refused DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Unit**.

Note: the **Transformation** field is not required if you are not changing the dialed number before making the call. For example, when the dialed number is the extension of a colleague. However, if the dialed number must be transformed, for example to add a 0 at the beginning of the dialed number, then a transformation is required. Refer to [Basic DTMF Transformations](#) (p.367)

- 5) Complete all the other fields, as required.
- 6) Click **Apply**

12.1.2.3 Creating a DTMF Map that Applies to Specific Endpoints

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) From the **DTMF Map** selection list, choose:
 - a) **Allowed** if you wish to create DTMF maps that accept calls
 - b) **Refused** if you wish to create DTMF maps that refuse calls
- 3) In the **Allowed DTMF Map** or **Refused DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoints for which you wish to associate a DTMF map.
- 6) Complete all the other fields, as required.

Note: the **Transformation** field is not required if you are not changing the dialed number before making the call. For example, when the dialed number is the extension of a colleague. However, if the dialed number must be transformed, for example to add a 0 at the beginning of the dialed number, then a transformation is required. Refer to [Basic DTMF Transformations](#) (p.367)

- 7) Click **Apply**

12.1.3 DTMF Maps Examples

12.1.3.1 Default DTMF Maps

Two default DTMF maps are configured in a unit that is set up with the factory settings.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Unit		--- Suggestion ---	x.#	x{#}		Disable
2	Enable	Unit		--- Suggestion ---	x.T	x		Disable
3	Enable	Unit		--- Suggestion ---	x.T	x		Disable
4	Enable	Unit		--- Suggestion ---	x.T	x		Disable
5	Enable	Unit		--- Suggestion ---	x.T	x		Disable
6	Enable	Unit		--- Suggestion ---	x.T	x		Disable
7	Enable	Unit		--- Suggestion ---	x.T	x		Disable
8	Enable	Unit		--- Suggestion ---	x.T	x		Disable
9	Enable	Unit		--- Suggestion ---	x.T	x		Disable
10	Enable	Unit		--- Suggestion ---	x.T	x		Disable

- x.# indicates to dial, right away, a number that finishes by a #. The transformation indicates to not dial the #.
- x.T indicates to dial the number if not digit is dialed after 3 seconds.

12.1.3.2 Configuring a DTMF Map to Use a Timer to Make a Call

Before you start

This should always be the last DTMF map of the **Allowed DTMF Map** table.

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) Make sure the **DTMF Map** selection list, is set to **Allowed**.
- 3) In the **Allowed DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoint for which you wish to associate a DTMF.
- 6) in the **DTMF Map** field enter [2-9]xxxxxxT.

Note: xT indicates that the number will be dialed after the delay set for the timer, (T)

Note: When making the actual call and dialing the number, the Mediatrix unit automatically removes the "T" found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only; no transformation is required to remove it.

7) Click **Apply**

Result

The call will be made if the first number is either 2 to 9 and that it has 7 digits, and no digits have been dialed for the time set in the timer.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Endpoint	Slot1/E1T1	--- Suggestion ---	[2-9]xxxxxxT			Disable

12.1.3.3 Configuring a DTMF Map to make a Call with an Extension

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) Make sure the **DTMF Map** selection list, is set to **Allowed**.
- 3) In the **Allowed DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoints for which you wish to associate a DTMF map.
- 6) in the **DTMF Map** field enter **[2-4]xx**
- 7) Click **Apply**

Result

When a 3-digit extension starting by either 2, 3, or 4 is made from the specified endpoint, the call is made. However, if the dialed number begins with anything else than 2, 3, or 4, the call is not made and you get a busy signal.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Endpoint	Slot1/E1T1	--- Suggestion ---	[2-4]xx			Disable

12.1.3.4 Configuring a DTMF Map to make an Internal (extension) or External Call

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) Make sure the **DTMF Map** selection list, is set to **Allowed**.
- 3) In the **Allowed DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoint for which you wish to associate a DTMF.

- 6) in the **DTMF Map** field enter `(([2-4]xx|9[2-9]xxxxxx))`.

Note: The DTMF map is enclosed in parentheses when using the “|” option.

- 7) Click **Apply**

Result

The call is made if the number begins with 2, 3, or 4 and the number has 3 digits, or if the number begins with 9, the number has 7 digits and the second digit is any digit between 2 and 9.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Endpoint	Slot1/E1T1	--- Suggestion ---	<code>(([2-4]xx 9[2-9]xxxxxx))</code>			Disable

12.1.3.5 Configuring a DTMF Map to Force the Use of the # OR * to Dial a Number

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) Make sure the **DTMF Map** selection list, is set to **Allowed**.
- 3) In the **Allowed DTMF Map** table, from the **Enable** selection list, choose, **Enable**.
- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoint for which you wish to associate a DTMF.
- 6) in the **DTMF Map** field enter `(xxxxxxx#|xxxxxxx*)`.

Note: The DTMF map is enclosed in parentheses when using the “|” option.

- 7) In the **Transformation** field, enter `(x{#}|x{*})`
- 8) Click **Apply**

Result

The “#” or “*” character in the **DTMF Map** field indicates that users must dial the “#” or “*” character at the end of their number to indicate it is completed. The **Transformation** field indicates that the # or * must be removed to send the call.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Endpoint	Slot1/E1T1	--- Suggestion ---	<code>(xxxxxxx# xxxxxxx*)</code>	<code>(x{#} x{*})</code>		Disable

12.1.3.6 Configuring a DTMF Map to Make a Call Outside the Country

Steps

- 1) Go to **Telephony/DTMF Maps**.
- 2) Make sure the **DTMF Map** selection list, is set to **Allowed**.
- 3) In the **Allowed DTMF Map** table, from the **Enable** selection list, choose, **Enable**.

- 4) From the **Apply to** selection list, choose **Endpoint**.
- 5) From the **Suggestion** selection list, choose the endpoint for which you wish to associate a DTMF map.
- 6) in the **DTMF Map** field enter **(0T|00T)**.

Note: The DTMF map is enclosed in parentheses when using the “|” option.

Note: When making the actual call and dialing the number, the Mediatrix unit automatically removes the “T” found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only; no transformation is required to remove it.

- 7) Click **Apply**

Result

The call will be made if the dialed number starts with 0, or 00.

Allowed DTMF Map								
Index	Enable	Apply To	Endpoints	Suggestions	DTMF Map	Transformation	Target	Emergency
1	Enable	Endpoint	Slot1/E1T1	--- Suggestion ---	(0T 00T)			Disable

12.1.3.7 Basic DTMF Transformations

DTMF Transformations will modify the dialed number. For example, let's say that the dialed number is 18195551111#.

Action	Transformation	Result
Add the prefix “0” to the dialed number	0x	018195551111#
Remove the suffix “#” from the dialed number	x{#}	018195551111
Remove the first four DTMFs from the dialed number	(4)x	5551111#
Remove the international code and termination and replace the area code by another one	(1){819}514x{#}	5145551111
Replace the signalled DTMFs by a extension "123"	123	123

12.2 Call Forward

12.2.1 Basic Call Forward Tasks

12.2.1.1 Configuring Call Forward on Busy

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Call Forward**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration, select **Enable**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Forward On Busy** section, complete the fields as required.
- 5) Click **Apply**.

12.2.1.2 Configuring Call Forward on No Answer

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Call Forward**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration, select **Enable**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Forward on No Answer** section, complete the fields as required.
- 5) Click **Apply**.

12.2.1.3 Configuring Call Forward Unconditional

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Call Forward**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration, select **Enable**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Forward Unconditional** section, complete the fields as required.
- 5) Click **Apply**.

12.3 Telephony Services

12.3.1 Basic Telephony Services Concepts

12.3.1.1 Default vs Specific Endpoint Configuration

It is possible to configure all endpoints to the default value, or an endpoint to a specific value, or a mix of both.

When you do not change your configuration, the values keep the default configuration. In order to modify the codec settings for a specific endpoint, the endpoint must first be selected from the drop-down list. It is also possible to have a default configuration followed by one or more specific endpoint configurations.

- Default configuration
- Mix of default and specific endpoint configurations
- All endpoints enabled with specific configurations

12.3.1.2 Automatic Call

The automatic call feature allows you to define a telephone number that is automatically dialed when taking the handset off hook. When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

12.3.1.3 Call Completion

The call completion service allows you to configure the Completion of Calls on No Reply (CCNR) and Completion of Calls to Busy Subscriber (CCBS) features. CCBS allows a caller to establish a call with a “busy” callee as soon as this callee is available to take the call. It is implemented by monitoring the activity of a UA and look for the busy-to-idle state transition pattern. CCNR allows a caller to establish a call with an “idle” callee right after this callee uses his phone. It is implemented by monitoring the activity of a UA and look for the idle-busy-idle state transition pattern. The information about the call completion is not kept after a restart of the EpServ service. This includes the call completion activation in the Pots service and the call completion monitoring in the SipEp service.

12.3.1.4 Call Waiting

The call waiting tone indicates to an active call that a new call is waiting on the second line. 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.

12.3.2 Basic Telephony Services Tasks

12.3.2.1 TelIf Default vs Specific Endpoint Configuration Examples

Here are some examples from the command line interface CLI for default parameters, followed by specific endpoint configuration.

```
Global>TelIf.DefaultCountryCustomizationUserGainInputOffset
0
```

```
Global>TelIf.DefaultCountryCustomizationUserGainOutputOffset
0
```

```
Global>TelIf.SpecificCountryCustomizationUserGain
```

InterfaceId	EnableConfig	InputOffset	OutputOffset
Slot1/E1T1	Disable	0	0
Slot2/E1T1	Disable	0	0
Slot3/E1T1	Disable	0	0
Slot4/E1T1	Disable	0	0

Slot5/FXS1	Disable	0	0
Slot5/FXS2	Disable	0	0
Slot5/FXS3	Disable	0	0
Slot5/FXS4	Disable	0	0
Slot6/FX01	Disable	0	0
Slot6/FX02	Disable	0	0
Slot6/FX03	Disable	0	0
Slot6/FX04	Disable	0	0
Slot7/FXS1	Disable	0	0
Slot7/FXS2	Disable	0	0
Slot7/FXS3	Disable	0	0
Slot7/FXS4	Disable	0	0
Slot8/FX01	Disable	0	0
Slot8/FX02	Disable	0	0
Slot8/FX03	Disable	0	0
Slot8/FX04	Disable	0	0

Command examples with their results.

```
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot1/
E1T1].EnableConfig = Enable
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot1/
E1T1].InputOffset = -6
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot1/
E1T1].OutputOffset = -8

TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot5/
FXS3].EnableConfig = Enable
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot5/
FXS3].InputOffset = -3
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot5/
FXS3].OutputOffset = -3
```

Global>TelIf.SpecificCountryCustomizationUserGain

InterfaceId	EnableConfig	InputOffset	OutputOffset
Slot1/E1T1	Enable	-6	-8
Slot2/E1T1	Disable	0	0
Slot3/E1T1	Disable	0	0
Slot4/E1T1	Disable	0	0
Slot5/FXS1	Disable	0	0
Slot5/FXS2	Disable	0	0
Slot5/FXS3	Enable	-3	-3
Slot5/FXS4	Disable	0	0
Slot6/FX01	Disable	0	0
Slot6/FX02	Disable	0	0
Slot6/FX03	Disable	0	0
Slot6/FX04	Disable	0	0
Slot7/FXS1	Disable	0	0
Slot7/FXS2	Disable	0	0
Slot7/FXS3	Disable	0	0

Slot7/FXS4	Disable	0	0
Slot8/FX01	Disable	0	0
Slot8/FX02	Disable	0	0
Slot8/FX03	Disable	0	0
Slot8/FX04	Disable	0	0

```
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot3/
E1T1].InputOffset = -1
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot3/
E1T1].OutputOffset = +1
```

```
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot7/
FXS3].InputOffset = +2
TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot7/
FXS3].OutputOffset = -4
```

Global>TelIf.SpecificCountryCustomizationUserGain

InterfaceId	EnableConfig	InputOffset	OutputOffset
Slot1/E1T1	Enable	-6	-8
Slot2/E1T1	Disable	0	0
Slot3/E1T1	Disable	-1	1
Slot4/E1T1	Disable	0	0
Slot5/FXS1	Disable	0	0
Slot5/FXS2	Disable	0	0
Slot5/FXS3	Enable	-3	-3
Slot5/FXS4	Disable	0	0
Slot6/FX01	Disable	0	0
Slot6/FX02	Disable	0	0
Slot6/FX03	Disable	0	0
Slot6/FX04	Disable	0	0
Slot7/FXS1	Disable	0	0
Slot7/FXS2	Disable	0	0
Slot7/FXS3	Disable	2	-4
Slot7/FXS4	Disable	0	0
Slot8/FX01	Disable	0	0
Slot8/FX02	Disable	0	0
Slot8/FX03	Disable	0	0
Slot8/FX04	Disable	0	0

```
Global>TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot3/
E1T1].EnableConfig
Disable
```

```
Global>TelIf.SpecificCountryCustomizationUserGain[InterfaceId=Slot7/
FXS3].EnableConfig
Disable
```

12.3.2.2 Configuring Telephony Services for all Endpoints

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default**.
- 3) Complete the fields as required.
- 4) Click **Apply**.

12.3.2.3 Configuring Telephony Services for a Specific Endpoint

Information

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select the endpoint to configure.
- 3) From the **Endpoint Specific** drop-down menu, select **Yes**.
- 4) Complete the remaining fields as required.
- 5) Click **Apply**.

12.3.2.4 Configuring Hook Flash Processing

Before you start

Note: Depending on your unit model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **General Configuration** section, complete the field as required.

- 5) Click **Apply**.

12.3.2.5 Configuring Automatic Calls

Before you start

Note: Depending on your unit model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Automatic Call** section, complete the fields as required.
- 5) Click **Apply**.

12.3.2.6 Configuring Call Completion

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Completion** section, complete the fields as required.

- 5) Click **Apply**.

12.3.2.7 Configuring Call Transfer

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: The blind transfer allows a user to transfer a call on hold to a call that is still ringing (unanswered) without speaking to the person, whereas the attended transfer allows the user to speak to the person before transferring the call.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Transfer** section, complete the fields as required.
- 5) Click **Apply**.

12.3.2.8 Configuring Call Waiting

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Call Waiting** section, complete the fields as required.

- 5) Click **Apply**.

12.3.2.9 Configuring Conference

Before you start

Only 3-way conference calls are supported on DGW, when hosted locally. If a conference server is used, the limit depends on the server capacity.

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Conference** section, complete the field as required.
- 5) Click **Apply**.

12.3.2.10 Configuring Delayed Hotline

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Delayed Hotline** section, complete the fields as required.

- 5) Click **Apply**.

12.3.2.11 Configuring Direct IP Address Call

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Direct IP Address Call** section, complete the field as required.
- 5) Click **Apply**.

12.3.2.12 Configuring Hold

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Hold** section, complete the field as required.

- 5) Click **Apply**.

12.3.2.13 Configuring Second Call

Before you start

Note: Depending on your model, whether it has E1/T1, FXS, or FXO ports, when you select a specific endpoint, the configuration parameters will vary and may not be available.

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select **Default** or a specific endpoint.

Note: For more information, refer to the [Default vs Specific Endpoint Configuration](#) section.

- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Second Call** section, complete the field as required.
- 5) Click **Apply**.

12.4 Tone Customisation

12.4.1 Basic Tone Customisation Tasks

12.4.1.1 Identifying the Tone Pattern

Steps

- 1) Go to **Telephony/Tone Customisation**.

- 2) From the **Select Tone** drop-down, select the tone to identify.

Note: For more information on tones, refer to [DGW Configuration Guides - Country Specification](#) published on the [Media5 Documentation Portal](#).

12.4.1.2 Overriding the Pattern of a Tone

Before you start

Before you continue, make sure you have done the following [Identifying the Tone Pattern](#) (p.378).

Steps

- 1) Go to **Telephony/Tone Customisation**.
- 2) From the **Override Current Tone Values** field, select **Enable**.
- 3) Click **Copy Current Tone Definition To Overriden**.

Note: You cannot edit the tones in the **Current Tone Definition** and **Current Tone States** tables.

Note: For more information on tones, refer to [DGW Configuration Guides - Country Specification](#) published on the [Media5 Documentation Portal](#).

- 4) Modify the **Overriden Tone Definition** table as required.
- 5) Modify the fields in the **Overriden Tone States** table as needed.
- 6) Click **Apply**.
- 7) Click **restart required services**, located at the top of the page.

Result

Next time the tone is used, your new settings will be applied.

12.5 Music on Hold

12.5.1 Basic Music on Hold Concepts

12.5.1.1 MP3 File Upload

You can only upload MP3 music files. Before you start, you must choose to upload the MP3 file either from the Server (this file will be loaded every time the unit restarts) or from the Web Browser (loaded once).

To load the music file from a server, refer to [Importing an MP3 File from a Server](#) (p.380). To load the music on your unit, refer to [Importing an MP3 File from a Web Browser](#) (p.555).

12.5.1.2 MP3 File Requirements

The MP3 file must be encoded following the MPEG 2.5 Audio Layer III specifications:

- Sample Rate: 8kHz
- Mono

Note: The file must be smaller than 1024 Kilobytes unless specified otherwise in a customer profile.

Note: The file name must not contain spaces.

12.5.2 Basic Music on Hold Tasks

12.5.2.1 Enabling Music on Hold

Before you start

Before you start, make sure you have configured the appropriate server in order to transfer the MP3 file. The [Importing an MP3 File from a Server](#) (p.380) or [Importing an MP3 File from a Web Browser](#) (p.555) task must first be completed.

Steps

- 1) Go to **Telephony/Music on Hold**.
- 2) From the **Music on Hold Configuration** table, from the **Streaming** drop-down menu, select **Enable**.
- 3) Click **Apply**.

Result

From the **Status** table, make sure the **File Status** field displays **File Ready**.

12.5.2.2 Importing an MP3 File from a Server

Before you start

Before you start, make sure you have configured the appropriate server in order to transfer the MP3 file. Refer to: [Configuring the TFTP Server](#) (p.28), [Configuring the FTP Server](#) (p.27), [Configuring the HTTP Server](#) (p.27).

Steps

- 1) Go to **Telephony/Music on Hold**.

- 2) From the **Transfer Configuration** table, in the **URL** field, enter the URL of the MP3 file to use.

Note: When the port is not included in the URL, the default port for the chosen protocol is used.

- 3) If your server requires authentication when downloading the MP3 file, set the **User Name** and **Password**.
- 4) In the **Reload Interval** field, set the time in hours.
- 5) Click **Apply & Transfer Now**.

Result

In the **Status** table, the **Last Transfer Result** displays **Success**.

12.6 Misc

12.6.1 Basic Misc Telephony Concepts

12.6.1.1 Call Detail Record (CDR)

Call detail record (CDR) in VoIP contains information about recent system usage such as:

- the identities of sources (points of origin)
- the identities of destinations (endpoints)
- the duration of each call
- the total usage time in the billing period
- etc.

12.6.1.2 Call Detail Record Example

Call Detail Record	
Syslog Remote Host	192.168.0.50
Syslog Format	%id;%ocgnum;%ocdnum;%cd;%dr;%sipdr;%ccy;%ccmm;%cch;%ccm;%ccs
Syslog Facility	Local0 ▼

Syslog message: LOCAL0.INFO: 1;1141399338;1140175242;37;16;200;2017;07;07;15;00;20

- 1:CDR ID (internal)
- 1141399338: calling number (before being transformed by the Call Router)
- 1140175242: called number (before being transformed by the Call Router)

- 37: call duration (seconds)
- 16: reason for ISDN disconnection
- 200: reason for SIP disconnection
- 2017: year
- 07: month
- 07: day
- 15: hour
- 00: minute
- 20: second

12.6.1.3 Formal Protocol Syntax Description

Syntax elements:

- Macro=%[Width][.[Precision]]Macroid
- Width=DIGIT
- Precision=DIGIT

Examples for: sipid=SipUser001

- CDR Log : %sipid --> CDR Log : SipUser001
- CDR Log : %15sipid --> CDR Log : SipUser001
- CDR Log : %15.5sipid --> CDR Log : SipUs
- CDR Log : %.5sipid --> CDR Log : SipUs

12.6.1.4 Call Detail Record Macros and Control Characters

Control characters

- %% : %
- \n : Split message

Call detail record macros :

- %id : CDR ID. The CDR ID is unique. The ID is incremented by one each time it is represented in a CDR record.
- %sipid : SIP call ID. Blank if no SIP interface was used during the call.
- %ocgnum : Original calling number. Calling number as received by the unit.
- %cgmnum : Calling number. Calling number after manipulation by the call router.
- %ocdnum : Original called number. Called number as received by the unit.
- %cdnum : Called number. Called number after manipulation by the call router.

- %oiname : Origin interface name. Interface on which the call was received. Ex. isdn-Slot2/Pri1.
- %diname : Destination interface name. Interface on which the call was relayed. Ex. SIP-Default.
- %chan : Channel number. Blank if no PRI/BRI interface was used during the call. If 2 PRI/BRI interfaces were involved, display the originating interface.
- %sipa : SIP local IP address.
- %sipra : SIP remote IP address or FQDN (next hop).
- %siprp : SIP remote port (next hop).
- %mra : Media remote IP address. Source IP address of the incoming media stream. If the stream was modified during the call, display the last stream.
- %mrsp : Media remote source port. Source port of the incoming media stream. If the stream was modified during the call, display the last stream.
- %mrp : Media remote port. Destination port of the outgoing media stream. If the stream was modified during the call, display the last stream.
- %tz : Local time zone
- %cd : Call duration (in seconds) (connect/disconnect).
- %sd : Call duration (in seconds) (setup/connect).
- %pdd : Post dial delay (in seconds) (setup/progress).
- %css : Call setup second (local time)
- %csm : Call setup minute (local time)
- %csh : Call setup hour (local time)
- %csd : Call setup day (local time)
- %csmm : Call setup month (local time)
- %csy : Call setup year (local time)
- %ccs : Call connect second (local time)
- %ccm : Call connect minute (local time)
- %cch : Call connect hour (local time)
- %ccd : Call connect day (local time)
- %ccmm : Call connect month (local time)
- %ccy : Call connect year (local time)
- %cds : Call disconnect second (local time)
- %cdm : Call disconnect minute (local time)
- %cdh : Call disconnect hour (local time)
- %cdd : Call disconnect day (local time)
- %cdmm : Call disconnect month (local time)
- %cdy : Call disconnect year (local time)
- %miptxc : IP Media last transmitted codec
- %miptxp : IP Media last transmitted p-time

- %dr : Call disconnect reason, expressed as a Q.850 cause. The Q.850 codes are used to represent the disconnect cause no matter what type of interface initiated the disconnect (SIP, FXS, ISDN, ...). A value of 0 means that no cause code is available.
- %rxp : Received media packets. Excluding T.38.
- %txp : Transmitted media packets. Excluding T.38.
- %rxpl : Received media packets lost. Excluding T.38.
- %rxmd : Received packets mean playout delay (ms, 2 decimals). Excluding T.38.
- %rxaj : Received packets average jitter (ms, 2 decimals). Excluding T.38.
- %sipdr : SIP status code of the received SIP response that caused the disconnect or rejection. A value of 0 means that no status code is available.

12.6.2 Basic Misc Telephony Setting Tasks

12.6.2.1 Configuring the Country for a Specific Endpoint

Information

You cannot configure specific endpoints with different countries. Once you select the country, it will be valid for all endpoints.

12.6.2.2 Configuring the Country for all Endpoints

Steps

- 1) Go to **Telephony/Misc**.
- 2) Make sure the **Select Endpoint** drop-down list is set to **Default**.
- 3) In the **Country** table, select your country from the drop-down list.
- 4) Click **Apply**.

Result

Country	
Country Selection:	NorthAmerica1 ▼

12.6.2.3 Configuring the User Gain for all Endpoints

Steps

- 1) Go to **Telephony/Misc**.
- 2) From the **Select Endpoint** drop-down menu, leave the selection to **Default**.
- 3) From the **User Gain** table, fill out the fields as required.

- 4) Click **Apply**.

Note: In case you had selected a specific endpoint, and if your **Endpoint Specific** is set to **Yes**, then this endpoint will not use the default values.

12.6.2.4 Configuring the User Gain for Specific Endpoints

Steps

- 1) Go to **Telephony/Misc**.
- 2) From the **Select Endpoint** drop-down menu, select an endpoint.
- 3) From the **User Gain** table, in the **Endpoint Specific** drop-down menu, select **Yes**.

Note: Use these settings with great care. Media5 recommends not to modify the user gain parameters unless absolutely necessary because default calibrations may no longer be valid. Modifying user gains may cause problems with DTMF detection and voice quality – using a high user gain may cause sound saturation (the sound is distorted). Furthermore, some fax or modem tones may no longer be recognised. The user gains directly affect the fax communication quality and may even prevent a fax to be sent.

- 4) From the **User Gain** table, fill out the **Input Offset** and **Output Offset** fields as required.
- 5) Click **Apply**.

12.6.2.5 Starting the CDR Service

Before you start

By default, this service is not activated.

Steps

- 1) Go to **System/Services**.
- 2) From the **User Service** table, on the **Call Detail Record (CDR)** line, click .
- 3) Click **Apply**.

Result

In the **User Service** table, the **Status** of the CDR service is **Started**.

12.6.2.6 Configuring the CDR

Before you start

The CDR service must be started. Refer to [Starting the CDR Service](#) (p.385).

Steps

- 1) Go to **Telephony/Misc**.

- 2) In the **Syslog Remote Host** field, enter the host name and optional port number of the server that archives the CDR log entries, using the following format: hostname[:port].

Note: For an example of format, refer to the [Formal Protocol Syntax Description](#) (p.382).

Note: Specifying no port (or port 0) sends notifications to port 514.

- 3) In the **Syslog Format** enter your format. You must use one of the supported macros displayed in the **Show Help**. You cannot create new macros because they will not be supported.

Note: Field separators can be done with a coma (,), a semicolon (;), a colon (:), or/and space. The maximum number of characters allowed in the **Format** field is 1024.

Note: For an example of record, refer to [Call Detail Record Example](#) (p.381).

- 4) In the **Syslog Facility** field, select the one used to route the Call Detail Record messages.
- 5) Click **Apply**.

12.7 Advanced Telephony Parameters

12.7.1 User Gain Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by:

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

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) and for more information on scripting language, refer to [DGW Configuration Guide Configuration Scripting Language Syntax](#) available on the [Media5 Documentation Portal](#).

Parameters
Tellf.DefaultCountryCustomizationUserGainInputOffset
Tellf.DefaultCountryCustomizationUserGainOutputOffset
Tellf.SpecificCountryCustomizationUserGain[].EnableConfig
Tellf.SpecificCountryCustomizationUserGain[].InputOffset
Tellf.SpecificCountryCustomizationUserGain[].InterfaceId
Tellf.SpecificCountryCustomizationUserGain[].OutputOffset

12.7.2 Advanced Dialing Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by:

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

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) and for more information on scripting language, refer to [DGW Configuration Guide Configuration Scripting Language Syntax](#) published on the [Media5 Documentation Portal](#).

Parameters
Tellf.DefaultCountryCustomizationDialingDtmfDuration
Tellf.DefaultCountryCustomizationDialingInterDtmfDialDelay
Tellf.DefaultCountryCustomizationDialingInterMfR1DialDelay
Tellf.DefaultCountryCustomizationDialingMfR1Duration
Tellf.DefaultCountryCustomizationDialingOverride
Tellf.SpecificCountryCustomizationDialing[].DtmfDuration
Tellf.SpecificCountryCustomizationDialing[].EnableConfig
Tellf.SpecificCountryCustomizationDialing[].InterDtmfDialDelay
Tellf.SpecificCountryCustomizationDialing[].InterMfR1DialDelay
Tellf.SpecificCountryCustomizationDialing[].MfR1Duration
Tellf.SpecificCountryCustomizationDialing[].Override

12.7.3 Fax Calling Tone Detection Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by:

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

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) and for more information on scripting language, refer to [DGW Configuration Guide Configuration Scripting Language Syntax](#) both available on the [Media5 Documentation Portal](#).

Parameters
Tellf.DefaultMachineDetectionBehaviorOnCedToneDetection
Tellf.DefaultMachineDetectionCedToneDetection
Tellf.DefaultMachineDetectionCngToneDetection
Tellf.DefaultMachineDetectionV21ModulationDetection
Tellf.SpecificMachineDetection[].BehaviorOnCedToneDetection
Tellf.SpecificMachineDetection[].CedToneDetection
Tellf.SpecificMachineDetection[].CngToneDetection
Tellf.SpecificMachineDetection[].EnableConfig
Tellf.SpecificMachineDetection[].InterfaceId
Tellf.SpecificMachineDetection[].V21ModulationDetection

12.8 Testing Telephony Services

12.8.1 Testing the Hold Service

Before you start

The **Hold Activation** field under the **Telephony > Services > Hold** section must be set to **Enable**.

Information

Endpoints are set as follows:

- Endpoint A: 123

- Endpoint B: 456
- Endpoint C: 789

Steps

- 1) A calls B.
- 2) Hook flash from A.
- 3) Verify that B is on hold.
- 4) Hook flash again from A.
- 5) Verify that voice path is back.
- 6) Release the call.

12.8.2 Testing the Call Waiting Service

Before you start

The **Call Waiting Activation** field under **Telephony** > **Services** > **Call Waiting** section must be set to **Enable**.

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456
- Endpoint C: 789

Steps

- 1) A calls B.
- 2) Verify the voice path.
- 3) C calls A.
- 4) Verify that A hears the stutter dial tone.
- 5) Hang up all endpoints.

12.8.3 Testing the Second Call Service

Before you start

The **Second Call Activation** field under **Services** > **Telephony** > **Second Call** section must be set to **Enable**.

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456

- Endpoint C: 789

Steps

- 1) Place a call between A and B.
- 2) Hook flash on A.
- 3) A initiates a « Second Call » to C.
- 4) Verify that the second voice path (between A and C) is established.

12.8.4 Testing the Blind Transfer Service

Before you start

The **Blind Transfer Activation** field under **Telephony > Services > Call Transfer** section must be set to **Enable**.

Steps

- 1) A calls B.
- 2) When the call is established, hook flash on B.
- 3) Wait for the second dial tone on B.
- 4) B calls C.
- 5) Wait for the ring back in B and then hang up B.
- 6) C should ring in the mean time.
- 7) You should now hear a ring back in A.
- 8) C answers the call.

Result

Call is established between A and C.

12.8.5 Testing the Attended Transfer

Before you start

The **Attended Transfer Activation** field under **Telephony > Services > Call Transfer** section must be set to **Enable**.

Steps

- 1) A calls B.
- 2) When the call is established, hook flash on B.
- 3) Wait for the second dial tone on B.
- 4) B calls C.
- 5) Answer C when it is ringing.
- 6) Verify voice path between B and C.
- 7) Hang up B.

- 8) The call should be transferred.
- 9) Call is established between A and C.

12.8.6 Testing the Conference Call Service

Before you start

The **Conference Activation** field under **Telephony > Services > Conference** section must be set to **Enable**.

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456
- Endpoint C: 789

Steps

- 1) Place a call between A and B.
- 2) Hook flash on A.
- 3) A initiates a « Second Call » to C .
- 4) Once the voice path between A and C is established, hook flash again on A to start the conference between A, B and C.
- 5) Verify that a 3 way voice path is established.

12.8.7 Testing the Automatic Call Service

Steps

- 1) Go to **Telephony/Services**.
- 2) In the **Services Configuration** table, enable the **Automatic Call Activation** on endpoint A.
- 3) Set the **Automatic Call Target** to 456 (endpoint B).
- 4) Click **Apply**.
- 5) Pick up telephone A.
- 6) A call between A and B should be automatically established.

Result

Services Configuration		Unit Defaults	
General Configuration			
Hook Flash Processing:		Process Locally	
Automatic Call			
Automatic Call Activation:		Enable	
Automatic Call Target:		456	

12.8.8 Testing the Delayed Hotline Call Service

Steps

- 1) Go to **Telephony/Services**.
- 2) In the **Services Configuration** table, under the **Delayed Hotline** section, enable the **Delayed Hotline Activation** on endpoint A.
- 3) Set the **Delayed Hotline Condition** to **FirstDTMFTimeout**.
- 4) Set the **Delayed Hotline Target** to 456 (endpoint B).
- 5) Click **Apply**.
- 6) Pick up phone A and wait for the First DTMF timer expiration.

Result

A call between A and B should automatically be established. First DTMF timer is the First DTMF Timeout defined under **Telephony/ DTMF Maps**. The respective parameter has the name "DtmfMapTimeoutFirstDtmf" and can also be modified via CLI or SNMP. Its default value is 20.000 ms , i.e. 20 seconds.

General Configuration			
First DTMF Timeout	Inter DTMF Timeout	Completion Timeout	Digit Detection (FXS/FXO)
20000	3000	60000	When Pressed v Edit Endpoints

12.8.9 Configuring the Call Forward Service for Testing

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456
- Endpoint C: 789

Steps

- 1) Go to **Telephony/Services**
- 2) In the **Call Forward Unconditional** section, set the **Allow Activation via Handset** to **Enable** on endpoint A.

- 3) Set the **DTMF Map Activation** field to *54.
- 4) Set the **DTMF Map Deactivation** field to *55.
- 5) Set the **Activation** field to **Active**.
- 6) Set the **Forwarding Address** to 456 (endpoint B).
- 7) Click **Apply**.

12.8.9.1 Testing the Call Forward Service

Before you start

The [Configuring the Call Forward Service for Testing](#) (p.392) task must be completed.

Steps

- 1) From C, dial A.

Note: You should hear a short ring from A and then B should ring.

- 2) Answer the call and verify the voice path between B and C.
- 3) Hang up all telephones.
- 4) From A, dial *55 to deactivate the service and hang up.
- 5) C calls A again.
- 6) Verify that the Call Forward is not active anymore.
- 7) From A, dial *54 to re-activate the service and hang up.
- 8) C calls A again.
- 9) Verify the forwarding to B.
- 10) Hang up all telephones.
- 11) From A, dial *54 789 and hang up. 789 is the C endpoint.
- 12) Refresh the Web page and verify that the **Forwarding Address** has changed to 789 (C).
- 13) B calls A and verify that the call is forwarded to C (789).

12.8.10 Configuring the CCBS Call Completion Service for Testing

Before you start

The configured SIP server must support the reception of SIP SUBSCRIPTION messages. Mediatrix Gateways do not support them

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456

- Endpoint C: 789

Steps

- 1) Go to **Telephony/Services**.
- 2) In the **Services Configuration** table, under the **Call Completion** section, set the **Allow CCBS Activation via Handset** to **Enable** on endpoint A.
- 3) Set the **CCBS DTMF Map Activation** field to *98.
- 4) Set the **CCBS DTMF Map Deactivation** field to *99.
- 5) Click **Apply**.

12.8.10.1 Testing the CCBS Call Completion Service

Information

Endpoints are set as follows:

- Endpoint A: 123
- Endpoint B: 456
- Endpoint C: 789

Steps

- 1) Make a call from B to C.
- 2) Once the call is established between B and C, call B from A.
- 3) A should hear the busy tone.
- 4) Dial *98 to activate the CCBS service.
- 5) Hang up A.
- 6) Hang up B and C.
- 7) Wait a few seconds.
- 8) A will hear a special ring.
- 9) Pick up A and the call will be completed with B.

12.8.11 Testing the Direct IP Call Service

Before you start

The **Direct IP Address Call Activation** field under **Telephony > Services > Direct IP Address Call** section, must be set to **Enable**.

Steps

- 1) Dial '**' .
- 2) Dial the numerical DTMFs of the IP address.

Note: For the dot '.', use the star '*' sign.

- 3) Terminate the IP call without specifying a phone number by using the star '*' or continue with a phone number by using the pound '#' sign.

- 4) Optionally, dial the phone number.

Note: Example: IP calls to a unit at IP address '1.2.3.4': – If the phone number is not required, the user must dial the following DTMFs sequence: **1*2*3*4*. – To reach the phone number '3330001', the user must dial the following DTMFs sequence: **1*2*3*4#3330001.

12.9 Default Ports Used by DGW

Connection Type	Default Port Number	Transport Protocol
Debug Signaling Log Host	6000	UDP
DHCP	68	UDP
FTP	21	TCP
HTTP	80	TCP
HTTPS	443	TCP
Persistent TLS Base Port	16000	TCP
Radius default port for accounting	1813	TCP
Radius default port for authentication	1812	TCP
RTP (including RTCP)	Range starting from 5004 ¹	UDP
Secure SIP	5061	TCP
SIP	5060	UDP
SNMP Listening	161	UDP
SNMP Trap	162	UDP
SNTP	123	UDP
SRTP (including SRTCP)	Range starting from 5004 ¹	UDP
SSH	22	TCP
Syslog	514	UDP
T.38	6004	UDP
Telnet	23	TCP
TFTP	69	UDP
1: For more details, refer to Calculating the RTP Port Range of a Mediatrix Unit (p.397)		

12.9.1 Calculating the RTP Port Range of a Mediatrix Unit

To calculate the port range of a Mediatrix unit, use the [Amount of Ports to Reserve](#) (p.398) and the [Default Ports Used by DGW](#) (p.396) tables.

When opening a port range for RTP/SRTP, the first port of the range is for RTP/SRTP (usually 5004) and the second port (usually 5005) is for RTCP/SRTCP. Therefore subsequent even ports of the range will be for RTP/SRTP and uneven ports will be for RTCP/SRTCP.

Note: It is a common practice to start the port range of the RTP/SRTP on an even number.

RTP (including RTCP)	(Base RTP port) to (Base RTP port + amount of ports to reserve for all the telephony ports of the unit)
SRTP (including SRTCP)	(Base SRTP port) to (Base SRTP port + amount of ports to reserve for all the telephony ports of the unit)
T.38	(Base T.38 port) to (Base T.38 port + amount of ports to reserve for all the telephony ports of the unit)

12.9.1.1 Amount of Ports to Reserve

Telephony ports	Amount of Ports to Reserve for	
	RTP/SRTP	T.38
2 FXS	16	2
4 FXS	24	4
8 FXS	40	8
16 FXS	80	16
24 FXS	112	24
28 FXS	128	28
2 FXO	16	2
4 FXO	24	4
8 FXO	40	8
16 FXO	80	16
24 FXO	112	24
28 FXO	128	28
1 E1	136	30
2 E1	272	60
3 E1	408	90
4 E1	544	120
5 E1	680	150
6 E1	816	180
7 E1	952	210
8 E1	1088	240
1 T1	108	23
2 T1	216	46
3 T1	324	69
4 T1	432	92
5 T1	540	115
6 T1	648	138
7 T1	756	161

Telephony ports	Amount of Ports to Reserve for	
	RTP/SRTP	T.38
8 T1	864	184
1 BRI	16	2
2 BRI	24	4
4 BRI	40	8
8 BRI	80	16
16 BRI	144	32

12.9.1.2 Examples of Port Range Calculations

For Voice: 5004 to (5004 + number of reserved ports for all the telephony ports of the unit).

For T.38: 6004 to (6004 + number of reserved ports for all the telephony ports of the unit).

Mediatix G7 with 2 E1 and 4 FXS ports

Use the [Amount of Ports to reserve](#) table to locate how many ports must be reserved for all the telephony ports of the unit.

Note: RTP Port 5004 and T.38 port 6004 are the base ports used by DGW. To verify the values used on your unit, open the DGW Web page of your unit, under **Media/Misc** in the **Base Ports** table. For more details, refer to the **Mipt.IpTransportRtpBasePort** and **Mipt.IpTransportT38BasePort** parameters in the [DGW Configuration Guide - Reference Guide](#) published on the Media5 documentation portal at <https://documentation.media5corp.com>

	Voice in RTP/SRTP	T.38
Ports reserved for 2 E1	272	60
Ports reserved for 4 FXS	24	4
Base port	5004	6004
Upper port	$5004 + 272 + 24 = 5300$	$6004 + 60 + 4 = 6068$
Port Range	5004 to 5300	6004 to 6068

Sentinel 400 with 2 T1, 4 FXS , and 4 FXO ports

	Voice in RTP/SRTP	T.38
Ports reserved for 2 T1	216	46
Ports reserved for 4 FXS	24	4
Ports reserved for 4 FXO	24	4
Base port	5004	6004
Upper port	$5004 + 216 + 24 + 24 = 5268$	$6004 + 46 + 4 + 4 = 6058$
Port Range	5004 to 5268	6004 to 6058

13 Call Router

13.1 Call Router Basic Concepts

13.1.1 Call Router Configuration Limitations

Configuration Parameter	Maximum Number
Route	40
Signaling Property	40
Transformations	40
Transformation Rules	100
SIP Header Translations	100
Call Property Translation Override	100

13.1.2 Call Router

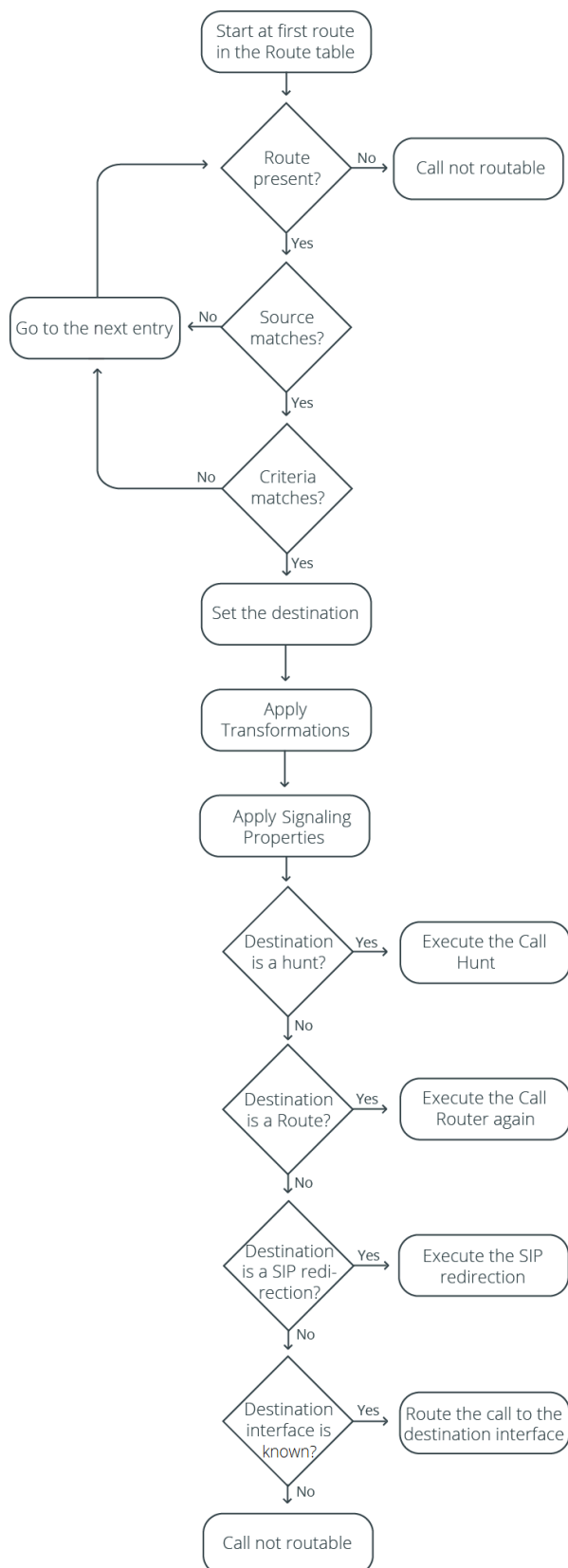
The DGW Call Router uses the Call Routing service (CRout) to route calls between a SIP gateway and an endpoint (FXS, FXO, PRI, or BRI).

In some specific cases, the Call Router can also route a call from an endpoint to another endpoint. Calls between the following telephony interfaces are allowed:

- ISDN to ISDN (TDM hairpinning)
- ISDN to SIP
- E&M to E&M (TDM hairpinning)
- E&M to SIP
- R2 to R2 (TDM hairpinning)
- R2 to SIP
- FXS to SIP
- FXO to SIP

The Call Router can not route a call from one SIP gateway to another SIP gateway. This is however possible on the Sentinel 100 and 400 using the Sbc service.

13.1.2.1 General Call Router Workflow



13.1.3 Call Router Specific Naming Rules

When working with call router parameters, you must prefix the name of:

- a route with "route-", for instance: route-isdn_sip.
- a SIP interface with "sip-", for instance: sip-default.
- an ISDN interface with "isdn-", for instance: isdn-default.
- a hunt with "hunt-", for instance: hunt-trunkLines.

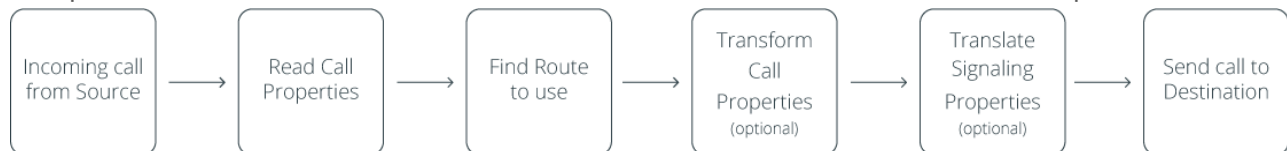
13.1.4 Routing

Routing is the operation that consists in finding which route to use for a call, and applying the various transformations and translations defined within the route.

Simply said, routing consists in sending a call from a source to a destination by using a user-defined route. For more details on sources and destinations, refer to the [Source and Destination](#) (p.405) section. When a call is established, two call legs exist:

- The inbound call leg, for the incoming call that entered the Call Router.
- The outbound call leg, for the outgoing call made to the callee after the processing made by the Call Router.

The following diagram is a simplified overview of the steps occurring during call routing. For a complete workflow of the Call Router, refer to the [General Call Router Workflow](#) (p.402) section.



Step	Description
Incoming Call	A call coming from a telephony interface (FXO, FXS, BRI, or PRI) or from SIP.
Read Call Properties	The Call Router reads the call properties of the call's signaling data. Call properties are common to all telephony technologies and contain information that the Call Router will use to route the call. For more details on call properties, refer to the DGW Configuration Guides -Call Properties document published on the Media5 Documentation Portal.
Find Route	The Call Router sequentially selects, from several routes defined in the Routes table, the proper route to use for the call. The route is chosen if the destination is valid and provided the value of the following criteria are matched with the call properties of the call: • Call source • Criteria rule matching the criteria property
Transform Call Properties (optional)	Transformations applied to call properties are defined in the Transformations and Transformation Rules tables. Specific, user-defined transformations are applied to a call property criteria. Transformations can include, for example, to: • add or remove prefixes to the called number • modify or block the caller ID For more details on call properties, refer to the DGW Configuration Guides - Call Properties document published on the Media5 Documentation Portal.

Step	Description
Translate Signalling Properties (optional)	Translations applied to the signaling properties are defined in the Signaling Properties table. Translations can include, for example, to: • control SIP features such as the destination host, privacy level of the call, or ringing feedback (180 vs 183). • override the default mapping between SIP headers and call properties (Call properties translations and SIP header translations). For more details, refer to SIP Signaling Properties (p.406).
Send Call to Destination	When the Call Router has completed its processing, the call is sent to its destination which is the exit point (SIP gateway, PRI interface, FXS interface, etc.) on which the outgoing call leg is created to forward the call to the callee.

13.1.4.1 Source and Destination

A call always has a source and a destination.

A call can go through several destinations before reaching its final destination.

A source and a destination can be:

- an endpoint (FXS, FXO, PRI, or BRI)
- a SIP gateway
- a route
- a hunt

However, an initial source and a final destination can only be either:

- an endpoint (FXS, FXO, PRI, or BRI)
- a SIP gateway

13.1.5 Signaling Properties

Signaling properties specify how to set up a call to the destination i.e. either a Mediatrix unit or a third-party equipment.

Signaling properties are assigned to a route and used to modify the behaviour of the call at the SIP protocol level. Signaling properties are applied after the call has been validated against the transformations, if there is a transformation specified in the route. As for the routes, the call is

validated against the call signaling properties one after the other until the call matches one signaling property. At this point, the transformation is executed by modifying the behaviour of the call. Up to 40 signalling properties can be added.

13.1.6 SIP Signaling Properties

SIP signaling properties are signaling properties used on the SIP leg of routing to control several SIP features.

SIP signaling properties are used by the mechanism through which the Call Router controls several SIP features of the calls during the SIP leg of the call. As for call properties, SIP signaling properties are used by the Call Router to apply routing decisions, but on the SIP leg.

SIP signalling properties are assigned to a route and used to modify the behaviour of the call at the SIP protocol level. Once a Route has been chosen, transformations are applied and then SIP signaling properties are applied.

A SIP signaling property transformation overrides the default value of the SIP signaling properties of an incoming SIP message. It modifies the properties before the call is sent to its destination. When a Route is chosen, SIP signaling properties are applied if possible. At this point, the transformation of the SIP signaling properties is performed.

13.1.7 Routes

Routes are used by the Call Router to send calls from one endpoint to another.

Routes are defined in the **Routes** table of the DGW Web interface. A call will be routed through a specific route only if the source criteria, the criteria property, and the criteria rule match. If there is a match, the call will be routed and transformations will be applied. The route includes information such as:

- the source the call must come from for the route to be applied
- the call properties the call must match for the route to be applied i.e. the property criteria
- the criteria rule, i.e. the regular expression applied to call property
- the transformations that will be applied to the call properties i.e. which transformation are used
- the call signaling properties
- the destination of the call

13.1.7.1 Route Ordering - Very Important

The order of the routes in the **Routes** table is important.

The most exclusive routes should be first and the most inclusive routes last, otherwise all calls will be routed by the same route, hence routed to the same destination.

For example, one of the first routes could be for a specific username for which the call would systematically be sent to a specific destination. The last route could route the unmatched calls to the receptionist's extension. If a call cannot be matched to any route, then the call is cancelled and an error message is issued.

13.1.8 Call Property Transformations

A Call Property Transformation is a mechanism through which the Call Router transforms call properties on the basis of specific criteria. Because this mechanism is applied when routing is processed by the Call Router, it provides a fine level of granularity to act on the signaling data of the call, allowing the user to route calls just about anywhere or to choose what signaling data will be displayed in the Caller Id.

A Call Property Transformation consists in:

- Defining on which criteria the transformation is based on and which criteria the transformation is applied to, both criteria being a call property, either identical or not. If the value of the **Criteria Based On** and **Criteria Rule** fields matches, then the transformation rule is applied to the le call property defined in the **Transformation Applies To** field.
- Transforming the call property specified in the transformation criteria.

Call property transformations can be used, for example, to:

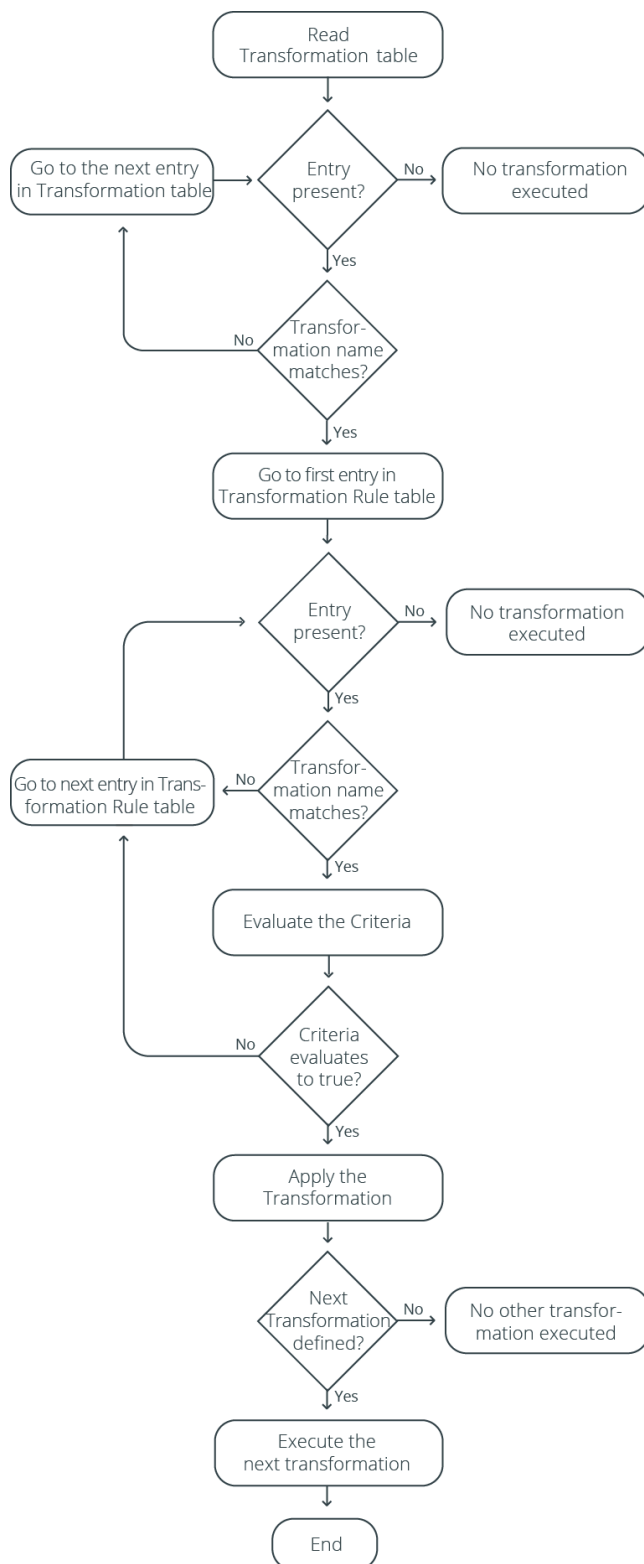
- Modify or block caller IDs
- Add or remove prefixes to the called number
- Block outgoing international calls
- Send all calls to a specific extension

Call property transformations thus influence routing and/or the setup message leaving the call router. They are specifically called within a route. As for the **Routes** table, the **Transformations** table finds the first matching entry. It then executes it by transforming a call property. A transformation always examines one call property and changes another property. The call router executes all transformations that match by following the **Transformation Rules** table rows as they are entered. If you want the Call Router to try to match one row before another one, you must put that row first.

Transformations can be applied to:

- calling party call properties
- called party call properties
- generic properties used for call properties that apply to both calling and called parties

13.1.8.1 Call Property Transformation Workflow



13.1.8.2 Route/Transformation/Next Transformation Recursiveness Example

```

|-Route 1
|  |-Transformation 1
|  |  |-Next Transformation 1
|  |  |  |-Next Transformation 2
|  |  |  |  |-Next Transformation 3
|  |  |  |  |  |-Next Transformation 4
|  |  |  |  |  |  |-Next Transformation 5
|  |  |-Transformation 2
|  |  |  |-Next Transformation 1
|  |  |  |  |-Next Transformation 2
|  |  |  |  |  |-Next Transformation 3
|  |  |-Transformation x
|  |  |-Transformation 40
|-Route 2
|  |-Transformation 1
|  |-Transformation 2
|  |-Transformation 3
|  |  |-Next Transformation 1
|  |  |  |-Next Transformation 2
|  |  |  |  |-Next Transformation 3
|-Route 3
|-Route x
|-Route 40

```

13.1.9 Call Properties

Although telephony technologies (SIP, FXS, ISDN, R2, CAS, etc.) all have the same purpose, i.e. make calls, they all have their own signaling, their own set of conventions, and their own vocabulary. Call properties are the common representation of the basic information pieces (signaling data) that all telephony technologies carry to route calls. The Call Router uses the call properties to apply routing decisions.

Using this single common representation simplifies the way we create routes in the Call Router because we can make abstraction, to a certain point, of the individual telephony technologies.

There is a large number of call properties, some of which are very generic and others more specific to certain types of telephony interfaces. During a call, only the call properties that make sense for the telephony interface being used are set with the relevant information. Therefore, a call property can be:

- Undefined: No value is assigned to the call property
- Defined: A value is assigned to the call property
- Empty: The call property is defined, but its value is empty (e.g. an empty string)

For example, when a call comes from ISDN, a number of call properties are set with the information extracted from the ISDN signaling: Calling Name, Called E164, ... The other Call Properties that are not relevant to ISDN are left undefined: for instance Calling Host and Calling URI, which makes sense only for calls coming from SIP.

For more details on call properties, refer to [Call Properties - Incoming Calls](#) and [Call Properties - Outgoing Calls](#) sections .

The transformation applied to the call properties can be configured in the **Transformations** and **Transformation Rules** tables of the DGW 2.0 Web interface.

13.1.9.1 Calling vs Called Call Properties

Many Call Properties exist in a Calling and Called version, with names such as CallingXxx or CalledXxx. This indicates if the Call Property is related to the Calling (incoming) or the Called (outgoing) side of the call.

For example, in a SIP to ISDN call from 987654321@voipprovider.com to 8191234567, the CallingE164 and CalledE164 Call Properties are assigned the 987654321 and 8191234567 values, respectively.

Note: within one single call, depending on the context, many call properties may only have a value set for the Called or the Calling version, and in some cases, no value can be set for either the Called or Calling version of the call properties.

Note: in a call, depending on the context, the Calling and/or Called versions of the call properties, may, or may not, be set to a value.

Note: Depending on the context, a call property with a calling and called version

13.1.9.2 SIP Call Properties - Source

Call Property	SIP Information
Called URI	Use the URL of the 'To' field as the 'Called URI' Call Property.
Calling URI	Use the URL of the 'From' field as the 'Calling URI' Call Property.
Called Name	Use the 'friendly name' Call Property of the 'To' field as the 'Called Name' Call Property. If there is no 'friendly name', the 'Called Name' Call Property is undefined.
Calling Name	Use the 'friendly name' Call Property of the 'From' field as the 'Calling Name' Call Property If there is no 'friendly name' Call Property , the 'Calling Name' Call Property is undefined.
Called E164	If the 'username' Call Property of the 'Request-Uri' field is E164 compatible, then the 'username' Call Property of the 'Request-Uri' field is used as the 'Called E164' Call Property. The "+" prefix and "-" separator are removed. If there is no 'username' Call Property or if the 'username' Call property is not E164 compatible, then the 'Called E164' Call Property remains empty.
Calling E164	If the 'username' Call Property of the 'From' field is E.164 compatible, then the 'username' Call Property of the 'From' field is used as the 'Calling E164' Call Property. The "+" prefix and the "-" separator are removed. If there is no 'username' Call Property or if the 'username' Call Property is not E.164 compatible, then the 'Calling E164' Call Property is undefined.
Called Host	Use the 'Host' Call Property of the 'To' field as the 'Called Host' Call property.
Calling Host	Use the 'Host' Call Property of the 'Contact' field as the 'Calling Host' Call Property.
Called TON	If the 'username' Call Property of the 'To' field is E.164 compatible and has the + sign in front, the 'Called TON' Call Property is 'international'. Otherwise the 'Called TON' Call Property is undefined.
Calling TON	If the 'user name' Call Property of the 'From' field is E.164 compatible and has a + sign in front, the 'Calling TON' Call Property is 'international'. Otherwise the 'Calling TON' Call Property is undefined.
Called Phone Context	If the 'username' Call Property of the 'phone-context' Call Property of the 'To' field is E.164 compatible, then the 'Called Phone Context' Call Property is the 'phone-context' Call Property of the 'username' Call property of the 'To' field. Otherwise the 'Called Phone Context' Call Property is undefined.

Call Property	SIP Information
Calling Phone Context	If the 'username' Call Property of the 'phone-context' Call Property of the 'From' field is E.164 compatible, then the 'Calling Phone Context' Call Property is the 'phone-context' of the 'username' of the 'To' field. Otherwise the 'Calling Phone Context' Call Property is undefined.
Called SIP Username	Use the 'username' Call Property of the 'Request-Uri' field as the 'Called SIP Username' Call Property. Note that this does not include the 'username' Call Properties such as the 'phone-context'.
Calling SIP Username	Use the 'username' Call Property of the 'From' field as the 'Calling SIP Username' Call Property. Note that this does not include the 'username' Call Property such as the 'phone-context' Call Property.
Last Diverting Reason	If the INVITE field contains at least one 'Diversion' header, then the value of the 'Last Diverting Reason' is the 'reason' field of the first 'Diversion' header: • "user-busy": cfb • "unconditional":cfu • "no-answer": cfna • All other values: unknown Otherwise, the value of the 'Last Diverting Reason' is undefined. The 'Reason' field is not case sensitive.

Call Property	SIP Information
Original Diverting Reason	If the INVITE field contains more than one 'Diversion' header, the 'Original Diverting Reason' Call Property is the 'Reason' field of the last 'Diversion' header: • user-busy": cfb • "unconditional":cfu • "no-answer": cfna • All other values: unknown Otherwise, the 'Original Diverting Reason' Call Property is undefined. The 'reason' field is not case sensitive.
Last Diverting E.164	If the INVITE field contains at least one 'Diversion' header, the value of the 'Last Diverting E.164' Call Property is the 'username' Call Property of the URI (can be a SIP URI, SIPS URI, or TEL URI) of the first 'Diversion' header converted into an E.164. If the 'username' Call Property of the URI has no value, or if it is not E.164 compatible, then the 'Last Diverting E.164' Call Property is undefined.
Original Diverting E.164	If the INVITE field contains more than one 'Diversion' header, the 'Original Diverting E.164' is the 'username' Call Property of the URI (can be a SIP URI, SIPS URI, or TEL URI) of the last 'Diversion' header converted into an E.164. If the 'username' Call Property has no value or is not E.164 compatible, the 'Original Diverting E.164' Call Property is undefined.
Diverting Counter	If the INVITE field contains at least one 'Diversion' header, the 'Diverting Counter' is the sum of the value of the 'counter' field of all 'Diversion' headers. If a 'Diversion' header does not contain the 'counter' field, the value is assumed to be one for the header.
All others	The property is undefined.

13.1.9.3 SIP Call Properties - Destination

Note: This table explains how the SIP fields are populated from the Call properties of the incoming call. In all cases, the value of the Call properties are used provided they are available.

SIP Field	Description
To	Use the value of the 'Calling URI' Call Property as the value of the 'To' field. If the 'Calling URI' Call Property has no value, the 'To' field is built with the following elements: • The 'username' Call Property is set to the first value available within the following Call Properties, in the specified order: • called 'SipUsername' Call Property • E164 Call Property • SipEp.InteropDefaultUsername parameter • Use the value of the 'Called Phone Context' Call Property as the value of the user's 'Phone Context' Call Property.@@@si 'Called Phone Context' n'a pas de valeur???? otherwise?????. If the 'user' part of the URI has a value, the value of the 'user' part is also added. The value of the 'user' Call Property of the URI can be found in the SipEp.InteropSipUriUserParameterValue parameter. • If the SipEp.InteropSipUriUserParameterValue parameter has no value, the value of the 'Phone' field is added to the 'Called Phone Context' Call Property . • If the 'Called Host' Call Property has a value, it is used as the 'Host' Call Property, otherwise the home domain proxy host is used. • If the 'Call TON' is 'international', add the + sign and the 'user' Call Property of the URI to the 'Phone' Call Property. • If the 'user' part of the URI has no value and the SipEp.InteropSipUriParameterValue parameter has a value then the value of the SipEp.InteropSipUriParameterValue is used as the value of the URI.

SIP Field	Description
From	If the 'Called URI' Call Property has a value, it is used as the value of the 'From' field. Otherwise, the 'From' field is built with the following elements: • If the 'Calling Name' Call Property has a value it is used as the value of the 'Friendly Name' Call Property. • The 'Username' Call Property is set to the first value available within the following Call Properties, in the specified order: • calling 'SipUsername' Call Property • E164 Call Property • SipEp.InteropDefaultUsername parameter • If the 'Calling Phone Context' Call Property has a value, it is used as the value of the user's 'Phone Context' Call Property. If the 'user' username part of the URI has a value, it also added. The value of the 'user' Call Property of the URI can be found in the SipEp.InteropSipUriUserParameterValue parameter. • If the SipEp.InteropSipUriUserParameterValue parameter has no value, the value of the 'Phone' field is added to the 'Called Phone Context' Call Property. • If the 'Calling Host' Call Property has a value, it is used as the value of the 'Host' Call Property, otherwise the value of the 'home domain proxy host' is used. • If the call 'TON' is 'international', add the + sign and the 'user' property of the URI parameter to the 'Phone' property. • If there is no 'user' part defined in the URI parameter and the SipEp.InteropSipUriUserParameterValue parameter has a value, then the value is added.

SIP Field	Description
Request URI	Use the value of the 'Calling URI' Call Property as the value of the 'Request URI' field. If the 'Calling URI' Call Property has no value, the 'Request URI' field is built with the following elements: • The 'username' Call Property is set to the first value available within the following Call Properties, in the specified order: • called 'SipUsername' Call Property • E164 Call Property • SipEp.InteropDefaultUsername parameter • Use the value of the 'Called Phone Context' Call Property as the value of the user's 'Phone Context' Call Property.@@@si 'Called Phone Context' n'a pas de valeur???? otherwise?????. If the 'user' part of the URI has a value, the value of the 'user' part is also added. The value of the 'user' Call Property of the URI can be found in the SipEp.InteropSipUriUserParameterValue parameter. • If the SipEp.InteropSipUriUserParameterValue parameter has no value, the value of the 'Phone' field is added to the 'Called Phone Context' Call Property . • If the 'Called Host' Call Property has a value, it is used as the 'Host' Call Property, otherwise the home domain proxy host is used. • If the 'Call TON' is 'international', add the + sign and the 'user' Call Property of the URI to the 'Phone' Call Property. • If the 'user' part of the URI has no value and the SipEp.InteropSipUriParameterValue parameter has a value then the value of the SipEp.InteropSipUriParameterValue is used as the value of the URI.

SIP Field	Description
Contact	If the 'Called URI' Call Property has a value, it is used as the value of the 'Contact' field. Otherwise, the 'Contact' field is built with the following elements: • If the 'Calling Name' Call Property has a value it is used as the value of the 'Friendly Name' Call Property. • The 'Username' Call Property is set to the first value available within the following Call Properties, in the specified order: • calling 'SipUsername' Call Property • E164 Call Property • SipEp.InteropDefaultUsername parameter • If the 'Calling Phone Context' Call Property has a value, it is used as the value of the user's 'Phone Context' Call Property. If the 'user' username part of the URI has a value, it also added. The value of the 'user' Call Property of the URI can be found in the SipEp.InteropSipUriUserParameterValue parameter. • If the SipEp.InteropSipUriUserParameterValue parameter has no value, the value of the 'Phone' field is added to the 'Called Phone Context' Call Property. • If the 'Calling Host' Call Property has a value, it is used as the value of the 'Host' Call Property, otherwise the value of the 'current IP address/port' is used. • If the call 'TON' is 'international', add the + sign and the 'user' property of the URI parameter to the 'Phone' property. • If there is no 'user' part defined in the URI parameter and the SipEp.InteropSipUriUserParameterValue parameter has a value, then the value is added.

SIP Field	Description
Diversion	If the 'Last Diverting E.164' Call property has a value, the value of the 'Diversion' header is added. The 'Diversion' header is built with the following elements: • Use the value of the 'Last Diverting E.164' Call Property as the value of the 'username' part of the URI . • The value of the 'home domain proxy host' is used as the 'host' part of the URI. • The value of the 'Last Diverting Reason' Call Property is used as the value of the 'reason' field: • cfu: "unconditional" • cfb: "user-busy" • cfmr: "no-answer" • All other values or when undefined: 'unknown'. • If the 'OriginalDivertingE164' Call Property has no value, then value of the 'Counter' field is set to the value of the 'DivertingCounter' Call Property, otherwise the 'Counter' field is set to the value of the 'DivertingCounter' Call Property -1. If the 'Last Diverting E.164' and 'Original Diverting E.164' Call Properties have a value, then a second 'Diversion' header is added. This Diversion header is built with the following elements: • The value of the 'Original Diverting E.164' Call Property is used as the 'username' Call Property of the URI. • The configured 'home domain proxy host' is used as the 'host' Call Property of the URI. • The value of the 'Original Diverting Reason' Call Property is used as the value of the 'Reason' field: • cfu: "unconditional" • cfb: "user-busy" • cfmr: "no-answer" • All other values or when undefined: "unknown" The field counter is set to 1.

13.1.10 SIP Header Translations Override

A SIP Header Translation overrides the default value of SIP headers in an outgoing SIP message.

It modifies the SIP headers before the call is sent to its destination. As for the **Routes** table, the **SIP Header Translation Overrides** table finds the first matching entry. It then executes it by modifying the behaviour of the call.

13.1.11 Hunt

A hunt consists in a group of destinations that can be associated with a route.

A hunt is used to make sure that if a destination is not available, that other destinations will be tried to route the call. For example, if the hunt specifies 4 different port destinations, then each destination will be checked for availability to route the call. If the first port is not available, the second port will be checked, and so on.

To use a hunt, the destination of a route must designate the hunt (i.e. the name of an entry in the **Hunt** table). The hunt name must be unique in the **Hunt** table.

The behavior of a hunt is defined by:

- A list of destinations to try
- An algorithm defining the sequence in which the hunt is performed. The Hunt configuration must specify which algorithm to use
- A timeout value
- A list of rejection causes that causes the hunt to continue

A maximum of 40 hunts can be created and used.

The execution order of the hunt destinations is defined by the sequential order of the **Hunt** table, separated by commas. The first destination defined is the first one used.

13.1.12 Auto-Routing

When the auto-routing feature is enabled, the Call Router can automatically create routes from a source to a destination.

If the `auto-routable` parameter is enabled for an endpoint (FXS, FXO, PRI, or BRI), two routes are generated and added to the Call Router:

- one directing incoming calls from the associated auto-routing SIP gateway to the endpoint
- one sending outgoing calls from the endpoint to the associated auto-routing SIP gateway

The auto-routing routes are not displayed in the **Route Config** page because you cannot edit them. They are however listed in the **Status** page and are attributed a type:

- User: the route has been manually entered

- Auto: this is an auto-routing route.

Note: By default, auto-routing can only be used if the username of the endpoint is an E.164 string and the username part of the request-URI of the received INVITE can be converted into an E.164. This can be changed in the **Auto-Routing** menu by setting the criteria to SIP Username.

13.1.13 TDM Hairpinning and SIP Loopback

TDM Hairpinning is defined as a standard inbound telephony call that is simply routed back out using the same Information Layer 1 Protocol. TDM Hairpinning is only supported between ISDN to ISDN, E&M to E&M or R2 to R2 endpoints and needs both calls to use the same codec.

However, a different approach, SIP loopback, is possible between two telephony interfaces for cases where TDM hairpinning is not supported.

SIP loopback can be achieved by:

- creating a route from the source telephony interface to a different SIP gateway which points to the unit itself
- overriding the SIP destination by using a call property, for example Called E164
- creating a route from the SIP interface to the destination telephony interface

For example:

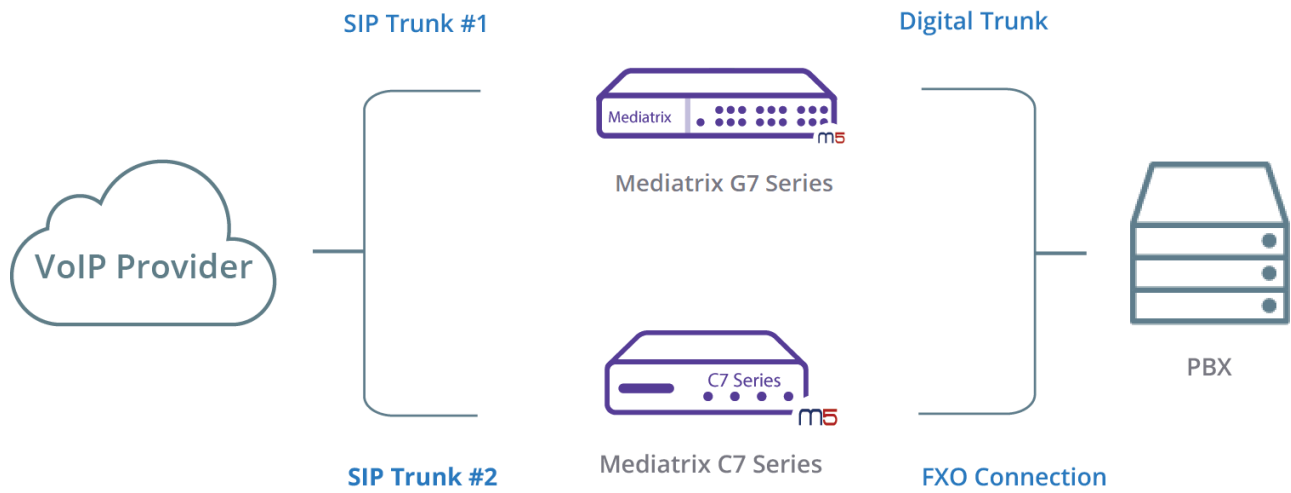
Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	fxs-Slot5/FXS1, fxs-Slot5/FXS2	Called E164	555....\$			sip-loopback	    
2	sip-loopback	Called E164	5551111			fxs-Slot5/FXS1	    
3	sip-loopback	Called E164	5552222			fxs-Slot5/FXS2	    
							

13.1.14 SIP Redirects

The SIP redirect feature allows a user to redirect a SIP call.

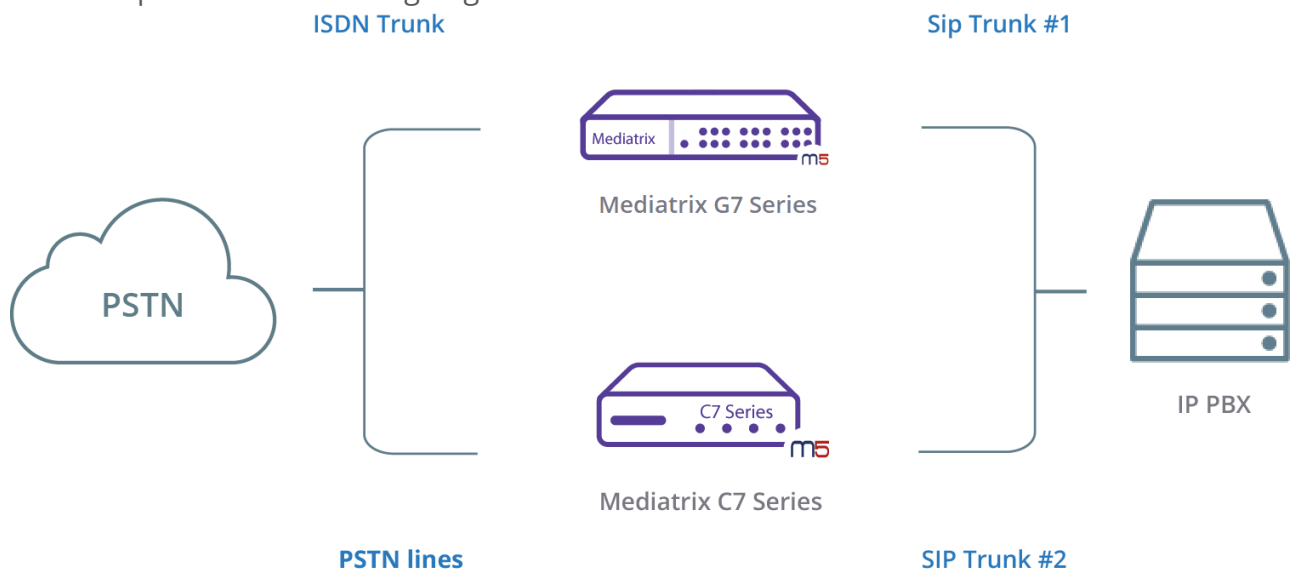
The SIP redirection can be used as a Route destination. When the route source is a SIP interface, incoming SIP INVITES are replied with a 302 "Moved Temporarily" SIP response. This type of destination is only valid when the source of the route is a SIP interface. When a route is configured with a SIP redirect destination, incoming SIP INVITES are replied with a 302 "Moved Temporarily" SIP response.

For example: cascade for incoming calls



m5 Media5 Portfolio

For example: cascade for outgoing calls
ISDN Trunk



m5 Media5 Portfolio

13.2 Basic Call Router Tasks

13.2.1 Creating a Basic Route

Several configuration steps are required to be able to route a call from one endpoint to another.

Steps

- 1) Create a route to determine the destinations the calls should be sent to.
 - a) [Creating a Route from a SIP Gateway to a Destination](#) (p.435)
 - b) [Creating a Route from a Physical Interface to a SIP Destination](#) (p.435)
- 2) Create the transformation rules to be applied to selected call properties by creating a transformation.
 - a) [Creating a Call Property Transformation](#) (p.437)
- 3) Associate the call property transformations to a specific route.
 - a) [Associating a Call Property Transformation to a Route](#) (p.440)
- 4) Apply changes.

13.2.2 Examples of Call Property Transformations

13.2.2.1 Replace 1xxx by 102

Any destination with prefix 1 will be replaced by destination 102 and send the call through the ISDN-BRI1 interface

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-sip_default	None		ModCalled		ISDN-BRI1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	ModCalled	Called E164	Called E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	ModCalled	1(.+)	102	    
				

13.2.2.2 Replace the Prefix 9 by 1 800 in an Outgoing Phone Number

For every called number coming from the SIP interface and beginning with 9, replace the 9 by 1 800, then send the call through the ISDN-BRI1 interface.

Routes						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination
1	sip-sip_default	None		ModCalled		ISDN-BRI1
						    
						

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	ModCalled	Called E164	Called E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	ModCalled	9(.+)	1800\1	    
				

13.2.2.3 Add the 1 450 Prefix to an Outgoing Phone Number

For every called number coming from the SIP interface add 1 450 in front of the number and then send the call through the ISDN-BRI1 interface

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-sip_default	None		ModCalled		ISDN-BRI1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	ModCalled	Called E164	Called E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	ModCalled	.+	1450\0	    
				

13.2.2.4 Send last 3 Digits

For every called number coming from a SIP interface, only keep the 3 last digits of the called number and send the call through the ISDN-BRI1 interface.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	None		stripforDDI		ISDN-BRI1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	stripforDDI	Called E164	Called E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	stripforDDI	.*{...}	\1	    
				

13.2.2.5 Replacing the Entire Source Phone Number by 1800 123 4567

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-sip_default	None		ModCalling		ISDN-BRI1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	ModCalling	Calling E164	Calling E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	ModCalling	.+	18001234567	    
				

13.2.2.6 Multiple Called URI Transformations

For all outgoing calls, send the 3 last digits of the called URI in the INVITE, display the U037098000 number in the **From** field, and forward to the SIP server all the 2-digit numbers beginning with 2.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	isdn-Bri1	Calling E164	2.\$	internal		sip-default	 
2	isdn-Bri1	None			fix_from_number	sip-default	 
3	sip-default	None		to_PBX	fix_from_number	hunt-hunt_PBX	 

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	to_PBX	Called URI	Called E164	 
2	internal	None	Called E164	 

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	to_PBX	sip:u.+(..)@	\1	 
2	internal		u037098001	 

Signaling Properties

Signaling Properties									
Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Header Translation Overrides	Call Property Translation Overrides
1	fix_from_number	Disable	Disable		Enable	Enable	Disable	fix_from_number	

SIP Header Translation Overrides				
Index	Name	SIP Header	Based On	Fixed Value
1	fix_from_number	From Header (User Part)	Fixed Value	u037098001  

13.2.2.7 Setting called numbers NPI and TON ISDN properties

Setting called numbers NPI and TON ISDN properties on SIP to ISDN calls.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	None		TON,NPI		fxs-Port1	   
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	TON	None	Calling TON	   
2	NPI	None	NPI	   
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	TON		national	   
2	NPI		isdn	   
				

13.2.2.8 SIP to Two Destinations

For every called number coming from the SIP interface, two destinations are possible.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Called E164	5(.+)	pri1		fxs-Port1	   
2	sip-default	Called E164	7(.+)	pri2		fxs-Port2	   
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	pri1	Called E164	Called E164	   
2	pri2	Called E164	Called E164	   
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	pri1	5(.+)	\1	   
2	pri2	7(.+)	\1	   
				

13.2.2.9 Send Specific Host to FXS phone1

On a Mediatrix 4102S, send all calls coming from the **somewhere.com** host to FXS phone 1.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Calling Host	somewhere\com			fxs-phone-Fax1	  
							

13.2.2.10 Allow Specific Number Range

Allow outgoing Sip calls only for users with an extension number ranging from 76610 to 76619, 76650 to 76659, and 76660 to 76669.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default		766([156])[0-9])			ISDN	   
2	ISDN		766([156])[0-9])			sip-default	   
							

13.2.2.11 Remove the Prefix 9

For every called number coming from the SIP interface and beginning with 9, remove the 9 from the number and send the call through the ISDN-BRI1 interface.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	None		ModCalled		ISDN-BRI1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	ModCalled	Called E164	Called E164	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	ModCalled	9(.+)	\1	    
				

13.2.2.12 Add CLIR Feature

Add the CLIR feature to every outgoing call coming from a SIP interface going through an FXS interface.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Called E164		Restric_num		fxs-Phone-Fax1	    
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	Restric_num	Called E164	Calling PI	    
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	Restric_num		restricted	    
				

13.2.2.13 Block Incoming International Call

Block all incoming international calls (i.e. numbers starting with 00) by sending the calls to a dead-end destination.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Called E164	00(.+)			Block_Call	    
							

13.2.2.14 Block Outgoing International Call

Block all outgoing international calls (i.e. numbers starting with 00) by sending the call to a dead-end destination.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Calling E164	00(.+)			Block_Call	   
							

13.2.2.15 Anonymous Call Rejection

Reject any anonymous calls from a Sip interface to a Sip interface.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	Calling SIP Username	[Aa][Nn][Oo][Nn][Yy][Mm] [Oo][Uu][Ss][Rr][Ee][Ss][Tt] [Rr][Ii][Cc][Tt][Ee][Dd]			sip-default	   
							

13.2.2.16 Calling E164 Transformations

Modify the calling E164 number with the user ID and for incoming calls send to the PBX the user ID present in the "To" string of the INVITE.

Routes							
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	sip-default	None			changed called E164	hunt-hunt_PBX	   
2	isdn-Bri1	None		username from		sip-default	   
							

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	username from	None	Calling E164	  
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	username from		100-000199-01-011	  
				

Signaling Properties

Signaling Properties									
Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Header Translation Overrides	Call Property Translation Overrides
1	change called E164	Disable	Disable		Enable	Enable	Disable		change called E164
									  

SIP Header Translation Overrides				
Index	Name	SIP Header	Based On	Fixed Value
				

Call Property Translation Overrides				
Index	Name	Call Property	Based On	Fixed Value
1	change called E164	Called E164	To Header (User Part)	  
				

13.2.3 Routes

13.2.3.1 Creating a Route from a SIP Gateway to a Destination

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Routes** table, click **+**.
 - click **+** located on the same row as an existing route to add a new route above or,
 - click **+** located at the bottom of the table to add a route at the end of the table.

Note: A maximum of 40 routes can be created.

- 3) In the **Configure Route** table, from the selection list of the **Sources** field, select a SIP gateway.
- 4) If necessary, from the selection list of the **Destination** field, select an Interface or a hunt group.

Note: Leave the **Signaling Properties**, the **Transformations** and **Criteria Property** fields empty.

- 5) Click **Save**.

Result

A new route is created and will appear in the **Routes** table.

Configure New Route		
	Value	Suggestion
Sources	Sip Gateway	--- Suggestion ---
Criteria Property	None	
Criteria Rule		--- Suggestion ---
Transformations		--- Suggestion ---
Signaling Properties		--- Suggestion ---
Destination	Destination	--- Suggestion ---
Config Status		

13.2.3.2 Creating a Route from a Physical Interface to a SIP Destination

Steps

- 1) Go to **Call Router/Route Config**.

- 2) In the **Routes** table, click .
- 3) In the **Configure Route** table, from the selection list of the **Sources** field, select an interface.
- 4) From the selection list of the **Destination** field, select a SIP Gateway or a SIP hunt group.

Note: Leave the **Signaling Properties**, the **Transformations** and **Criteria Property** fields empty.

Note: A maximum of 40 routes can be created.

- 5) Click **Save**.

Result

Configure New Route		
	Value	Suggestion
Sources	Interface	--- Suggestion ---
Criteria Property	None	
Criteria Rule		--- Suggestion ---
Transformations		--- Suggestion ---
Signaling Properties		--- Suggestion ---
Destination	Sip-Gateway	--- Suggestion ---
Config Status		

13.2.3.3 Modifying a Route

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Routes** table, click  located on the same row as the route you wish to modify.
- 3) In the **Configure Route** table, modify the fields as required.

Note: If you selected **Date/Time** as a criteria property, remember to click **Date/Time Criteria Editor** to edit the date and the time.

- 4) Click **Save**.

Result

When the route is used, the modifications will be applied.

Configure Route 1		
	Value	Suggestion
Sources	Source	--- Suggestion ---
Criteria Property	Criteria property	
Criteria Rule	sip:.*@somewhere.com	--- Suggestion ---
Transformations		--- Suggestion ---
Signaling Properties		--- Suggestion ---
Destination	Destination	--- Suggestion ---
Config Status		

13.2.3.4 Deleting a Route

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Routes** table, click  located on the same row as the route you wish to delete.
- 3) Click **Save**.

Result

The route is permanently deleted and will no longer be displayed in the **Routes** table.

13.2.3.5 Modifying the Execution Priority Level of a Route

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Routes** table, click  or  located on the same row as the route you wish to prioritise.
- 3) Click **Save**.

Result

Calls will be evaluated against the Routes in the new order.

13.2.4 Call Property Transformations

13.2.4.1 Creating a Call Property Transformation

Steps

- 1) Go to **Call Router/Route Config**.

2) In the **Transformations** table, click **+**.

- click **+** located on the same row as an existing call property transformation to add a new call property transformation above or,
- click **+** located at the bottom of the table to add a call property transformation at the end of the table.

Note: A maximum of 40 call property transformations can be created.

- 3) In the **Configure Transformation** table, in the **Name** field, enter a name for the call property transformation.
- 4) From the selection list of the **Criteria Based On** field, select the call property that must be matched to apply the Transformation.
- 5) From the selection list of the **Transformation Applies To** field, select the call property to transform.
- 6) Click **Save and Insert Rule**.
- 7) In the **Configure Transformation Rule** table, from the **Name** selection list, select the name entered at step 3.
- 8) In the **Criteria** field, indicate the call property criteria to match to apply the transformation.
- 9) In the **Transformation** field, select the transformation to apply to the call property.
- 10) Click **Save** or **Save and Insert Rule** to add another Transformation.

Result

The new Call Property Transformation is available to be used in a route.

Call Property Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	Name	Call Property to match	Call property to Transform	   
2				   
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	Name	Call Property criteria to match	Transformation to apply	   
2	Name	Call Property criteria to match	Transformation to apply	   
				

13.2.4.2 Modifying a Call Property Transformation

Steps

- 1) Go to **Call Router /Route Config**.

- 2) In the **Transformations** table, click  located on the same row as the call property transformation you wish to modify.
- 3) In the **Configure Transformation** table, modify the fields as required.

Note: If you selected **Date/Time** as a criteria property, remember to click **Date/Time Criteria Editor** to edit the date and the time.

- 4) Click **Save**.

Result

When the call property transformation is used by a route, the modifications will be applied.

13.2.4.3 Modifying a Call Property Transformation Rule

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Transformation Rules** table, click  located on the same row as the transformation you wish to modify.
- 3) In the **Configure Transformation Rule** table, modify the fields as required.
- 4) Click **Save**.

Result

When the Call Property Transformation Rule is used by a Call Property Transformation, the modifications will be applied.

13.2.4.4 Deleting a Call Property Transformation

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Transformations** table, click  located on the same row as the transformation you wish to delete.
- 3) Click **Save**.

Result

The call property transformation is permanently deleted and will no longer be displayed in the **Transformations** table hence will no longer be available to be associated with a route.

13.2.4.5 Deleting a Call Property Transformation Rule

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Transformation Rules** table, click  located on the same row as the call property transformation rule you wish to delete.

- 3) Click **Save**.

Result

The call property transformation rule will be permanently deleted and will no longer be displayed in the **Transformation Rules** table to be associated with a call property transformation.

13.2.4.6 Modifying the Execution Priority Level of a Call Property Transformation Rule

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Transformation Rules** table, click  or  located on the same row as the call property transformation rule you wish to move.
- 3) Click **Save**.

Result

Call property transformations will be validated against the call property transformation rules in the new order. The order is important, because rules are executed in the listed order.

13.2.4.7 Associating a Call Property Transformation to a Route

Before you start

The [Creating a Call Property Transformation](#) (p.437) step must be completed.

Steps

- 1) In the **Routes** table, click  located on the same line as the route you wish to associate a call property transformation to.
- 2) From the selection list of the **Transformations** field, select the transformation you wish to associate to the route.
- 3) Click **Save**.

Result

For each incoming call from SIP or an interface, the associated call property transformation defined in the transformation will be applied. Transformations are executed in sequence, separated by commas.

Routes						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination
1	Sip or Interface			Transformation name		Sip or Interface     
						

13.2.5 Signaling Properties

13.2.5.1 Creating a Signaling Property

Steps

- 1) Go to **Call Router /Route Config**.
- 2) In the **Signaling Properties** table, click .
 - click  located on the same row as an existing signaling property to add a new signaling property above or,
 - click  located at the bottom of the table to add a signaling property at the end of the table.

Note: A maximum of 40 signaling properties can be created.

- 3) In the **Configure Signaling Property** table, modify the fields as required.
- 4) Click **Save**.

Result

The signaling property will be available to be used in a route.

13.2.5.2 Modifying a Signaling Property

Steps

- 1) Go to **Call Router /Route Config**.
- 2) In the **Signaling Properties** table, click  located on the same row as the signaling property you wish to modify.
- 3) In the **Configure Signaling Property** table, modify the fields as required.
- 4) Click **Save**.

Result

When the signaling property is used in a route, the modifications will be applied.

13.2.5.3 Deleting a Signaling Property

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Signaling Properties** table, click  located on the same row as the signaling property you wish to delete.
- 3) Click **Save**.

Result

The signaling property is permanently deleted and will no longer be displayed in the **Signaling Properties** table to be associated with a Route.

13.2.5.4 Modifying the Execution Priority Level of a Signaling Property

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Signaling Properties** table, click  or  located on the same row as the signaling property you wish to move.
- 3) Click **Save**.

Result

The Routes will be evaluated against the signaling properties in the new order.

13.2.6 SIP Header Translations

13.2.6.1 Creating a SIP Header Translation Override

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **SIP Header Translation Overrides** table,
 - click  located on the same row as an existing SIP header translations to add a new SIP header translation above or,
 - click  located at the bottom of the table to add a SIP header translations at the end of the table.

- 3) In the **Configure SIP Header Translation Override** table, complete the fields as required.

Note: You can add up to 100 SIP header translations.

- 4) Repeat steps [Step 2](#) to [Step 3](#) to add another SIP header translation.
- 5) Click **Save**.

Result

The SIP header translation override will be available in the **Configure Signaling Property** table, in the **SIP Header Translation Overrides** drop-down list.

Configure New SIP Header Translation Override	
Name	Header
SIP Header	From Header (Host Part) ▼
Based On	Fixed Value ▼
Fixed Value	
Config Status	

13.2.6.2 Modifying a SIP Header Translation Override

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **SIP Header Translation Overrides** table, click  located on the same row as the route you wish to modify.
- 3) In the **Configure SIP Header Translation Override** table, modify the fields as required.
- 4) Click **Save**.

Result

When the SIP header translation override is used by a signaling property the modifications will be applied.

13.2.6.3 Deleting a SIP Header Translation Override

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **SIP Header Translation Overrides** table, click  located on the same row as the signaling property you wish to delete.
- 3) Click **Save**.

Result

The SIP header translation will no longer be displayed in the **SIP Header Translation Overrides** table and will no longer be available to be associated with a signaling property.

13.2.7 Call Property Translations Override

13.2.7.1 Creating a Call Property Translation Override

Steps

- 1) Go to **Call Router /Route Config**.
- 2) In the **Call Property Translation Override** table, click  located on the same row as the route you wish to modify.
- 3) In the **Configure Call Property Translation Override** table,
 - click  located on the same row as an existing call property translation override to add a new call property translation override above or,
 - click  located at the bottom of the table to add a call property translation override at the end of the table.

Note: You can create up to 100 call property translation overrides.

- 4) Click **Save**.

Result

When the call property translation override is used by a signaling property, the modifications will be applied.

13.2.7.2 Modifying a Call Property Translation Override

Steps

- 1) Go to **Call Router /Route Config**.
- 2) In the **Call Property Translation Override** table, click  located on the same row as the route you wish to modify.
- 3) In the **Configure Call Property Translation Override** table, modify the fields as required.

Note: If you selected **Date/Time** as a criteria property, remember to click **Date/Time Criteria Editor** to edit the date and the time.

- 4) Click **Save**.

Result

When the call property translation override is used by a signaling property, the modifications will be applied.

13.2.7.3 Deleting a Call Property Translation Override

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Call Property Translation Override** table, click  located on the same row as the call property translation override you wish to delete.
- 3) Click **Save**.

Result

The call property translation override will no longer be displayed in the **Call Property Translation Override** table and will no longer be available to be associated with a signaling property.

13.2.8 SIP Redirects

13.2.8.1 Creating SIP Redirection

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **SIP Redirects** table, click .
 - click  located on the same row as an existing SIP redirection to add a new SIP redirection above or,
 - click  located at the bottom of the table to add a SIP redirection at the end of the table.
- 3) Set the **Name** field.
- 4) Set the **Destination Host** field.
- 5) Click **Save**.

Result

The SIP redirection will be available to be used in routes.

Configure New SIP Redirect	
Name	Name
Destination Host	FQDN/IP address
Config Status	

13.2.8.2 Modifying a SIP Redirect

Steps

- 1) Go to **Call Router /Route Config**.
- 2) In the **SIP Redirects** table, click  located on the same row as the SIP redirect you wish to modify.
- 3) In the **Configure SIP Redirects** table, modify the fields as required.
- 4) Click **Save**.

Result

When the SIP redirect is used, the modifications will be applied.

13.2.8.3 Deleting a SIP Redirect

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **SIP Redirects** table, click  located on the same row as the SIP redirect you wish to delete.
- 3) Click **Save**.

Result

The SIP redirect will no longer be displayed in the **SIP Redirects** table and will no longer be available.

13.2.9 Hunt

13.2.9.1 Creating a Hunt

Steps

- 1) Go to **Call Router/Route Config**.

2) In the **Hunt** table,

- click **+** located on the same row as an existing hunt to add a new hunt above or,
- click **+** located at the bottom of the table to add a hunt at the end of the table.

Note: You can create up to 40 hunts.

3) In the **Configure Hunt** table, enter a name in the **Name** field.

4) From the **Suggestion** selection list next to the **Destinations** field, select 1 or several destinations.

5) From the **Suggestion** selection list next to the **Causes** field, select the causes pertinent to your situation.

6) To create another hunt group, repeat steps 2 to 5.

Note: Up to 40 hunt groups can be created.

7) Click **Save**.

Result

The hunt is available to be used in a route.

Configure New Hunt	
	Suggestion
Name	Name
Destinations	Select Destination --- Suggestion ---
Selection Algorithm	Sequential
Timeout (seconds)	0
Causes	Select Causes --- Suggestion ---
Config Status	

13.2.9.2 Modifying a Hunt

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Hunt** table, click **✎** located on the same row as the hunt group you wish to modify.
- 3) In the **Configure Hunt** table, modify the fields as required.
- 4) Click **Save**.

Result

The modifications will take effect immediately in all the instances where the hunt is used.

13.2.9.3 Deleting a Hunt

Steps

- 1) Go to **Call Router/Route Config**.
- 2) In the **Hunt** table, click  located on the same row as the Hunt group you wish to delete.
- 3) Click **Save**.

Result

The Hunt group is permanently deleted and is no longer displayed in the **Hunt** table to be associated to a route.

13.2.10 Auto-Routing

13.2.10.1 Enabling Auto-Routing

Steps

- 1) Go to **Call Router/Auto-Routing**.
- 2) From the **Auto-Routing** drop-down list, select **Enable**.
- 3) Complete the fields as required.

Note: **E164** is the default value of the **Criteria Type** field.

- 4) Click **Apply**.

13.2.10.2 Linking an Endpoint to Several SIP Gateways

Before you start

The [Enabling Auto-Routing](#) (p.448) procedure must be completed.

Information

This procedure is for outgoing calls only. For incoming calls, only one destination is used, however, it is possible to set a hunt to multiple SIP gateways.

Steps

- 1) Go to **Call Router/Auto-Routing**.
- 2) From the **Endpoints auto-routing** table, click  located on the row of the endpoint you wish to link to several SIP gateways.
- 3) From the **Configure Auto-Routing** section, complete the fields as required.

- 4) From the **Apply To The Following Endpoints** table, select the endpoints you wish to link to the gateways selected at previous step.
- 5) Click **Apply**.
- 6) Click **Apply**, again.

13.3 Routing Examples

This is an example on how a call is routed to it's final destination.

In this scenario, the user makes a call to 5145552222 using the fxs-Slot3/FXS1 port and src-E164=5551111 call property.

Routes	Source	Criteria Property	Criteria Rule	Transformation	Signaling properties	Destination
1	sip-default					fxs-Slot3/FXS1
2	fxs-Slot3/FXS1	Called E164	911	map911		sip-default
3	fxs-Slot3/FXS1			normalize	privacyId	sip-default

Find the Route

- Route 1 does not match because "fxs-Slot3/FXS1 does not match the "sip-default"
- Route 2 does not match because although "fxs-Slot3/FXS1" matches the fxs-Slot3/FXS1" source, the "911" criteria rule does not match 4505552222.
- Route 3 is chosen because "fxs-Slot3/FXS1" matches the source "fxs-Slot3/FXS1" source and the criteria rule included all criteria rules

The SIP-default destination is associated with the call. Therefore the call will be routed to the network using the SIP default gateway.

Transformation	Name	Criteria	Transformation
1	map911		Called E164
2	normalize	Called E164	Called E164

Apply transformations

- Transformation 1 is not used, because "map911" name does not match.
- Transformation 2 is applied because both name and criteria match.

Name	Criteria Rule
map911	
normalize	819.....\$
normalize	514.....\$
normalize	450.....\$

Apply criteria rule

- Criteria rule 1 is not applied because the name does not match.
- Criteria rule 1 does not apply because the criteria does not match (called number does not start by 819) even if the name matches.
- Criteria rule 3 does not apply because the criteria does not match (called number does not start by 514) even if the name matches.
- Criteria rule 4 is applied because the name and the criteria match.

Signaling properties	Name	...	Privacy	...
1	privacyId		Id	

Apply signaling properties "privacyId"

- Signaling property 1 is chosen because the name matches (no criteria to validate) therefore the "privacy=ID" property is added to the call.

For more Route examples, refer to [DGW Configuration Guide - Call Router Basic Routes](#) document published on the [Media5 Documentation Portal](#).

13.4 Regular Expressions

A regular expression is a string used to find and replace strings in other large strings.

Regular expressions can be used in the DGW software to enter a value in several routing types, often by using wildcard characters. These characters provide additional flexibility in designing call routing and decrease the need for multiple entries in configuring number ranges.

- The expression cannot begin by "^", it is implicit in the expression.
- The matching criterion implicitly matches from the beginning of the string, but not necessarily up to the end. For instance, 123 will match the criterion 1, but it will not match the criterion 2.
- To match the whole string, you must end the criterion with "\$". For instance, 123 will not match the criterion 1\$ and will match the criterion 123\$.
- Use the "local_ip_port" macro to replace the properties by the local IP address and port of the listening network of the SIP gateway used to send the INVITE.

13.4.1 Regular Expression Wildcards

Character	Description
.	Single-digit place holder. For instance, 555 matches any dialed number beginning with 555, plus at least four additional digits. Note that the number may be longer and still match.
*	Repeats the previous digit 0, 1, or more times. For instance, in the pattern: 1888*1 the pattern matches: 1881, 18881, 188881, 1888881 Note: If you are trying to handle the asterisk (*) as part of a dialed number, you must use *.
[]	Range of digits. • A consecutive range is indicated with a hyphen (-), for instance, [5-7]. • A nonconsecutive range is indicated without a delimiter, for instance, [58]. • Both can be used in combination, for instance [5-79], which is the same as [5679]. You may place a (^) symbol right after the opening bracket to indicate that the specified range is an exclude list. For instance, [^01] specifies the same range as [2-9]. Note: The call router only supports single-digit ranges. You cannot specify the range of numbers between 99 and 102 by using [99-102].
()	Indicates a group (also called pattern), for instance, 555(2525). It is used when replacing a number in a mapping. For more details, refer to Regular Expression Groups (p.452).
?	Matches 0 or 1 occurrence of the previous item. For instance, 123?4 matches both 124 and 1234..
+	Repeats the previous digit one or more time. For instance 12+345 matches 12345, 122345, etc. (but not 1345). If you use the + at the end of a number, it repeats the last number one or more times. For instance: 12345+ matches, 12345, 123455, 1234555, etc.
	Indicates a choice of matching expressions (OR).

13.4.2 Regular Expression Groups

Groups can be used in Transformation Rules to reuse parts of the Call Property that was used in the Criteria.

A group is placed within parenthesis. You can use up to nine groups defined by “\1” to “\9” and matching is not case sensitive. “\0” represents the whole string. Lets say for instance you have the following string: 9(123(45)6)

The following describes how groups are replaced in a property transformation:

Replacement	Result
\0	9123456
\1	123456
\2	45
\3	

Groups can only be used with the following routing types:

- Calling/Called E.164
- Calling/Called Name
- Calling/Called Host
- Calling/Called URI

13.4.3 Information on Regular Expressions

For more information on Regular Expressions (RegEx) refer to:

- <https://regex101.com/>
- <http://www.regular-expressions.info/>
- http://www.w3schools.com/jsref/jsref_obj_regexp.asp

14 Management

14.1 Configuration Scripts

14.1.1 Basic Configuration Scripts Concepts

14.1.1.1 Configuration Scripts Import and Export

Importing and exporting configuration scripts allows you to modify in whole or in part the configuration script used on your unit.

Configuration scripts are files containing textual commands that are sent over the network to a Mediatrix unit. Upon receiving the file, the unit executes each command line in sequence. Script commands can assign values to configuration variables, or execute configuration commands.

A configuration script can be used on any firmware version, regardless of the firmware version it was exported from. It is possible to import a complete configuration script, a subset of the configuration script or even a few lines of a configuration script.

Importing a configuration script can be useful to:

- Change one or several script commands
- Add new commands
- Change parameter values
- Add parameters
- Replace the complete configuration script

Scripts are written by the system administrator and can be used to accomplish various tasks, such as automating recurrent configuration tasks or batch-applying configuration settings to multiple devices. Scripts can be executed once or periodically at a specified interval. They can also be scheduled to be executed when the Mediatrix unit starts.

14.1.1.2 Configuration Scripts vs. Backup and Restore

- Configuration scripts are files containing textual commands that are sent over the network to a Mediatrix unit. Upon receiving the file, the Mediatrix unit executes each command line in sequence. Script commands can assign values to configuration variables, or execute configuration commands.
Scripts are written by the system administrator and can be used to execute several operations, such as automating recurrent configuration tasks or batch-applying configuration settings to

multiple devices. Scripts can be executed once or periodically at a specified interval. They can also be scheduled to execute when the Mediatrix unit restarts.

- The backup/restore feature is used to backup a specific Mediatrix unit's configuration for safety purposes. When needed, the configuration image file that is generated by a backup operation can be restored to put the unit back into the exact configuration it was when the backup was taken.

Configuration image files contain a Mediatrix unit's configuration information. They are not intended to be edited and must not be confused with configuration scripts. When restoring a configuration image, the whole Mediatrix unit's current configuration is replaced with the configuration found in the configuration image file. Restoring a configuration image is therefore an operation that is completely different from executing a configuration script.

14.1.1.3 How to Write a Configuration Script

Configuration scripts are text files containing command lines that are interpreted by the Mediatrix unit. Most commands contained in a script assign values to configuration variables. Script commands can also execute configuration commands.

Writing configuration scripts requires a bit of knowledge about the Mediatrix unit's configuration variables tree structure. Each parameter that is accessed via the Mediatrix unit's web interface maps to a variable in the configuration tree.

The following sub-sections give sample commands performing common tasks.

Assigning Scalar Values

The following is a sample script command assigning a value to a scalar configuration variable:

Assigning Table Cell Values

The following is a sample script command assigning a value to a configuration table cell:

Executing Commands

Configuration commands are used to make the Mediatrix unit perform actions such as restarting the unit, restarting a service, refreshing its SIP registration, etc.

The following is a sample script command executing a configuration command:

14.1.1.4 DHCPv4 Auto-Provisioning

The Mediatrix unit can be configured to automatically download new configuration scripts upon receiving options 66 (tftp-server) or 67 (bootfile), or vendor-specific option 43 using sub-options 66 and 67 in a DHCPv4 answer

A DHCP server answer includes both Bound and Renew. The contents of option 66, 67 or 43 defines which script to download. The unit's configuration is not used to download the script. This allows the unit, for instance, to download a script from a server after a factory reset and to reconfigure itself without a specific profile. If the imported configuration script is identical to the last executed script, it will not be run again. The script retry mechanism is not enabled for the DHCPv4 triggered scripts. If options 66, 67 and 43 are received, all scripts are executed independently. The script defined by

the tftp-server (option 66) option is executed first. If you are using HTTPS to transfer scripts, you must have a time server SNTP that is accessible and properly configured.

14.1.2 Basic Configuring Scripts Tasks

14.1.2.1 Configuring a Privacy Key

Steps

- 1) Go to **Management > Configuration Scripts**.
- 2) In the **Execute Scripts** table, set a privacy key of your choosing in the **Privacy Key** field.

Result

The unit will only accept scripts that have been encrypted with this privacy key. The privacy key also ensures that the files are encrypted when using unsecure transfer mode (HTTP,TFTP,FTP).

14.1.2.2 Importing a Configuration Script Using a File Server

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) In the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import.

Note: The file name is case sensitive and may be replaced by a macro. For more details on macros, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg. file extension.

- 3) From the **Transfer Protocol** selection list, select the type of protocol you wish to use to transfer your configuration script.

Note: This must be consistent with the file server you have configured.

- 4) In the **Host Name** field, enter the file server IP address or FQDN.
- 5) In the **Location** field, enter the path relative to the root of the file server where the configuration script is saved.
- 6) If your server requires authentication, enter your username and password.

- 7) If the files are encrypted, provide the privacy key in the **Privacy Key** field.

Note: The privacy key must match the privacy key used to encrypt the file.

- 8) Make sure the file server is started.
- 9) Depending on your use case, set the **Allow Repeated Execution** field to **Enable** or **Disable**. This parameter defines if the Mediatrix unit will execute a script or not, when it is the same as the last executed script."
- 10) Click **Apply & Execute**.

Result

The configuration script will be imported from the file server, and any changes to the script will be applied to the running configuration. Keep in mind that if you import a generic and a specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion ---
Specific File Name:	%mac%.cfg	--- Suggestion ---
Transfer Protocol:	HTTPS	
Host Name:	0.0.0.0:0	
Location:	Downloads	
User Name:	username	
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	
Automatic Script Execution		
Execute On Startup:	Disable	
Execute Periodically:	Enable	
Time Unit:	Hours	
Period:	1	
Time Range:	3:00:00	
Allow DHCP to Trigger Scripts Execution:	Enable	
		Apply Apply & Execute

14.1.2.3 Executing a Configuration Script from the Unit File Management System

Before you start

A configuration script must have been imported to the unit's file management system. Refer to [Importing a Configuration Script to the Unit File Management System](#) (p.459).

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.

- 2) In the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import, or use the **Suggestion** selection list.

Note: The file name is case sensitive, and may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg file extension.

- 3) From the **Transfer Protocol** selection list, select **File**.

Note: This option is not available on the Mediatrix 4102S running a firmware version more recent than DGW 2.0.26.451

- 4) If the file is encrypted, complete the **Privacy Key** field.

Note: The privacy key must match the privacy key used to encrypt the file.

- 5) As a best practice, enable the **Allow Repeated Execution** field.

- 6) Click **Apply & Execute**.

Result

The configuration script will be imported from the unit's file management system, and any changes to the script will be applied to the running configuration. Keep in mind that if you import a generic and specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion --- ▾
Specific File Name:	%mac%.cfg	--- Suggestion --- ▾
Transfer Protocol:	File ▾	
Host Name:	0.0.0.0:0	
Location:	Downloads	
User Name:	username	
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable ▾	
Automatic Script Execution		
Execute On Startup:	Disable ▾	
Execute Periodically:	Enable ▾	
Time Unit:	Hours ▾	
Period:	1	
Time Range:	3:00:00	
Allow DHCP to Trigger Scripts Execution:	Enable ▾	
		Apply Apply & Execute

14.1.2.4 Importing a Configuration Script from Your PC

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser**.
- 3) In the **Upload Script Through Web Browser** table, browse to the location of the file you wish to import.
- 4) If the file is encrypted, complete the **Privacy Key** field.

Note: The privacy key must match the privacy key used to encrypt the file.

- 5) Click **Upload and Execute**.
- 6) Located at the top of the page, click **Refresh**.

Result

The configuration script will be imported from your PC and any changes to the script will be applied to the running configuration.

Upload Script Through Web Browser	
Browse... No file selected. (Clear Selection)	
Privacy Key:	
Upload & Execute	

14.1.2.5 Importing a Configuration Script to the Unit File Management System

Before you start

This option is not available on the Mediatrix 4102S running a firmware version more recent than DGW 2.0.26.451

Steps

- 1) Go to **Management/File**.
- 2) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser** located at the top of the page.
- 3) In the **Import File Through Web Browser** table, from the **Path** selection list, select **Conf/**.
- 4) Browse to the location of the configuration file.
- 5) Click **Import**.

Note: A factory reset will remove the file from the Internal file.

Result

The imported configuration file will appear in the **Internal files** table, under **Management/File**.

Import File Through Web Browser	
Path	File
conf/	yymmdd_device_name.cfg Browse ... Import

14.1.2.6 Exporting a Configuration Script Using a File Server

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Steps

- 1) Go to **Management/Configuration Scripts/Export**.

- 2) In the **Export Script** table, from the **Content** selection list, choose if you wish to export only what is different from the factory configuration script or the complete configuration.
- 3) From the **Service Name** selection list, choose if you wish to export the configuration script of a specific service or of all services.
- 4) In the **Send To URL** field, enter the `protocol://[user[:password]@]hostname[:port]/[path/]filename` where to export the configuration file.

Note: This must be consistent with the file server you have configured. The file name may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. As a best practice, add the *.cfg extension to the file name.

Note: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your script, the interfaces used, the device model, etc.

- 5) If you wish to use encryption for transfer operations, enter a encryption key in the **Privacy Key** field.

Note: Media5 corp strongly recommends to use encryption to protect certificates and passwords.

- 6) Make sure the file server is started.
- 7) Click **Export and Download**.

Result

The configuration script will be exported to the specified file server.

Export Script	
Content:	Modified Config
Service Name:	All --- Suggestion ---
Send To URL:	ftp://file.server.com/folder/yymmdd_device_name.cfg
Privacy Key:	

14.1.2.7 Exporting a Configuration Script to Your PC

Steps

- 1) Go to **Management/Configuration Scripts/Export**.
- 2) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser** located at the top of the page.
- 3) In the **Download Script From Web Browser** table, from the **Content** selection list, choose if you wish to export only what is different from the factory configuration script or the complete configuration.
- 4) If you wish to use encryption for transfer operations, complete the **Privacy Key** field.

Note: Media5 strongly recommends to use encryption to protect certificates and passwords.

5) Click **Export and Download**.

Result

The configuration script will be exported to your PC in the Downloads folder. The system generates a macAddress.cfg file name.

Download Script From Web Browser	
Content:	All Config ▼
Privacy Key:	
Export & Download	

14.1.2.8 Executing Configuration Scripts from a File Server Periodically

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Mediatrrix units do not all include a real time clock allowing them to maintain accurate time when they are shutdown. You must have a time server SNTP that is accessible and properly configured or the automatic configuration update feature may not work properly. Refer to [Configuring the Mediatrrix Unit to Use an SNTP Server](#) (p.94).

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) In the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import.

Note: The file name is case sensitive, and may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg. file extension.

- 3) From the **Transfer Protocol** selection list, select the type of protocol you wish to use to transfer your script.

Note: This must be consistent with the file server you have configured.

- 4) In the **Host Name** field, enter the file server IP address or FQDN.
- 5) In the **Location** field, enter the path relative to the root of the file server where the script is saved.
- 6) If your server requires authentication, enter your username and password.

- 7) If the files are encrypted, provide the privacy key in the **Privacy Parameters** section.

Note: The privacy key must match the privacy key used to encrypt the file.

- 8) Make sure the file server is started.
- 9) In the **Automatic Script Execution** section, from the **Execute Periodically** selection list, choose **Enable**.
- 10) Complete the **Time Unit**, **Period** and **Time Range** fields according to your needs.

Note: The time range (hh[:mm[:ss]] or hh[:mm[:ss]] - hh[:mm[:ss]]) is based on the **Static Time Zone** field, under the **Network > Host** page.

- 11) As a best practice, enable the **Allow Repeated Execution** field.
- 12) Click **Apply**.

Result

The configuration script will be imported from the file server at the specified time or at a random time within the specified interval and thereafter at the period defined by the **Period** field. Any change to the script will be applied to the running configuration. The unit configuration is only updated if at least one parameter value defined in the imported configuration scripts is different from the actual unit configuration. Keep in mind that if you import a generic and a specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion ---
Specific File Name:	%mac%.cfg	--- Suggestion ---
Transfer Protocol:	HTTPS	
Host Name:	0.0.0.0:0	
Location:	Downloads	
User Name:	username	
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	
Automatic Script Execution		
Execute On Startup:	Disable	
Execute Periodically:	Enable	
Time Unit:	Hours	
Period:	1	
Time Range:	3:00:00	
Allow DHCP to Trigger Scripts Execution:	Enable	
		Apply Apply & Execute

14.1.2.9 Executing Configuration Scripts from the Unit File Management System Periodically

Before you start

You must have a time server SNTP that is accessible and properly configured or the automatic configuration update feature may not work properly. Refer to [Configuring the Mediatrix Unit to Use an SNTP Server](#) (p.94). Configuration scripts files must be available in the unit's file management system. Refer to [Importing a Configuration Script to the Unit File Management System](#) (p.459).

A configuration script must have been imported to the unit's file management system. Refer to [Importing a Configuration Script to the Unit File Management System](#) (p.459).

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) In the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import or use the **Suggestion** selection list.

Note: The file name is case sensitive, and may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg. file extension.

- 3) From the **Transfer Protocol** selection list, select **File**.

- 4) If the files are encrypted, provide the privacy key in the **Privacy Key** field.

Note: The privacy key must match the privacy key used to encrypt the files.

- 5) In the **Automatic Script Execution** section, from the **Execute Periodically** selection list, choose **Enable**.
- 6) Complete the **Time Unit**, **Period** and **Time Range** fields according to your needs.

Note: The time range (hh[:mm[:ss]] or hh[:mm[:ss]] - hh[:mm[:ss]]) is based on the **Static Time Zone** field, under the **Network > Host** page.

- 7) As a best practice, enable the **Allow Repeated Execution** field.
- 8) Click **Apply**.

Result

The configuration script will be imported from the system's file management system at the specified time or at a random time within the specified interval and thereafter at the period defined by the **Period** field. Any change to the script will be applied to the running configuration. The unit configuration is only updated if at least one parameter value defined in the imported configuration scripts is different from the actual unit configuration. Keep in mind that if you import a generic and specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion ---
Specific File Name:	\$mac%.cfg	--- Suggestion ---
Transfer Protocol:	File	
Host Name:	0.0.0.0:0	
Location:		
User Name:		
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	
Automatic Script Execution		
Execute On Startup:	Disable	
Execute Periodically:	Enable	
Time Unit:	Hours	
Period:	1	
Time Range:	3:00:00	
Allow DHCP to Trigger Scripts Execution:	Enable	
		Apply Apply & Execute

14.1.2.10 Executing Configuration Scripts from a File Server Each Time the Unit is Started

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) From the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import.

Note: The file name is case sensitive, and may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg. file extension.

- 3) From the **Transfer Protocol** selection list, select the type of protocol you wish to use to transfer your script.

Note: This must be consistent with the file server you have configured.

- 4) In the **Host Name** field, enter the file server IP address or FQDN.
- 5) In the **Location** field, enter the path relative to the root of the file server where the script is saved.
- 6) If your server requires authentication, enter your username and password.
- 7) If the files are encrypted, provide the privacy key in the **Privacy Parameters** section.

Note: The privacy key must match the privacy key used to encrypt the files.

- 8) Make sure the file server is started.
- 9) In the **Automatic Script Execution** section, from the **Execute on Startup** selection list, choose **Enable**.
- 10) As a best practice, enable the **Allow Repeated Execution** field.
- 11) Click **Apply**.

Result

When the unit is restarted, the configuration script will be imported from the file server, and any changes to the script will be applied to the running configuration. Keep in mind that if you import a generic and a specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion ---
Specific File Name:	%mac%.cfg	--- Suggestion ---
Transfer Protocol:	HTTPS	
Host Name:	0.0.0.0:0	
Location:	Downloads	
User Name:	username	
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	
Automatic Script Execution		
Execute On Startup:	Enable	
Execute Periodically:	Disable	
Time Unit:	Hours	
Period:	1	
Time Range:		
Allow DHCP to Trigger Scripts Execution:	Enable	
		Apply Apply & Execute

14.1.2.11 Executing Configuration Scripts from the Unit File Management System Each Time the Unit is Started

Before you start

A configuration script must have been imported to the unit's file management system. Refer to [Importing a Configuration Script to the Unit File Management System](#) (p.459).

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) From the **Execute Scripts** table, in the **Generic File Name** and/or **Specific File Name** field, indicate the name of the files you wish to import or use the **Suggestion** selection list.

Note: The file name is case sensitive, and may be replaced by a macro. For more details, refer to the [Unit Macros](#) (p.23) section. Make sure to add the *.cfg. file extension.
- 3) From the **Transfer Protocol** selection list, select **File**.
- 4) If the files are encrypted, provide the privacy key in the **Privacy Parameters** section.
- 5) In the **Automatic Script Execution** section, from the **Execute on Startup** selection list, choose **Enable**.
- 6) As a best practice, enable the **Allow Repeated Execution** field.
- 7) Click **Apply**.

Result

When the unit is restarted, the configuration script will be imported from the system's file management system, and any changes to the script will be applied to the running configuration. Keep in mind that if you import a generic and specific file, the commands of the specific file will override the commands of the generic file.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion --- ▾
Specific File Name:	%mac%.cfg	--- Suggestion --- ▾
Transfer Protocol:	File ▾	
Host Name:	0.0.0.0:0	
Location:		
User Name:		
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable ▾	
Automatic Script Execution		
Execute On Startup:	Enable ▾	
Execute Periodically:	Disable ▾	
Time Unit:	Hours ▾	
Period:	1	
Time Range:		
Allow DHCP to Trigger Scripts Execution:	Enable ▾	
		Apply Apply & Execute

14.1.2.12 Configuring the DHCP to Trigger Configuration Script Execution

The Mediatrix unit can be configured to automatically import new configuration scripts upon receiving options 66 (tftp-server) or 67 (bootfile), or vendor-specific option 43 using sub-options 66 and 67 in a DHCPv4 answer. A DHCP answer includes both Bound and Renew.

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Mediatrix units do not all include a real time clock allowing them to maintain accurate time when they are shutdown. If you are using HTTPS, you must have an SNTP server that is accessible and

properly configured or the automatic configuration update feature may not work properly. Refer to [Configuring the Mediatrix Unit to Use an SNTP Server](#) (p.94).

Information

For more details on DHCPv4 Auto-Provisioning, refer to [DHCPv4 Auto-Provisioning](#) (p.454)

Steps

- 1) Go to **Management/Configuration Scripts/Execute**.
- 2) In the **Automatic Script Execution** section, from the **Allow DHCP to Trigger Scripts Execution** selection list, choose **Enable**.
- 3) Click **Apply**.

Result

The instructions sent FROM the DHCP server can be in different formats and will be understood by the Mediatrix unit according to what was chosen for the **ScriptsDhcpOptionsFormat** MIB parameter (not accessible via Web page). Possible values with their respective formats are:

- Fully Qualified: Script=[protocol]://[username] :[password]@[server]/[path]/[file].
- Url: [protocol]:// [username] :[password]@[server]/[path]/[file]
- ServerHost: Allow one DHCP option to specify the IP address or FQDN of a file server. Uses the path and filename specified in the ScriptLocation and ScriptGenericFileName parameters, use the transfer protocol, username and password specified in ScriptTransferProtocol, ScriptTransferUsername and ScriptTransferPassword parameters.
- AutoDetect: A value beginning with "Script=" is considered as "FullyQualified", A value beginning with "[protocol]://" is considered as a URL. A value that looks like an IPv4/IPv6 address or domain name is considered as a "ServerHost". (default value)

When the unit starts, it will receive the location of the config script from the DHCP response, as per the format defined by the **ScriptsDhcpOptionsFormat** parameter. The unit will then import and execute the configuration scripts from the specified location. Any changes to the script will be applied to the running configuration. The unit configuration is only updated if at least one parameter value defined in the imported configuration scripts is different from the actual unit configuration.

Execute Scripts		
Transfer Parameters		
Generic File Name:	%product%.cfg	--- Suggestion ---
Specific File Name:	%mac%.cfg	--- Suggestion ---
Transfer Protocol:	HTTPS	
Host Name:	0.0.0.0:0	
Location:	Downloads	
User Name:	username	
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	
Automatic Script Execution		
Execute On Startup:	Enable	
Execute Periodically:	Enable	
Time Unit:	Hours	
Period:	1	
Time Range:	3:00:00	
Allow DHCP to Trigger Scripts Execution:	Enable	
		Apply Apply & Execute

14.1.3 Advanced Configuration Scripts Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#). The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

Scripts Transfer Certificate Validation

Refer to **Conf. ScriptsTransferCertificateValidation**.

Scripts Transfer Certificate Trust Level

Refer to **Conf. ScriptsTransferCertificateTrustLevel**.

Scripts Transfer Cipher Suite

Refer to **Conf. ScriptsTransferCipherSuite**.

Scripts Transfer Tls Version

Refer to **Conf. ScriptsTransferTlsVersion**.

Scripts Dhcp Options Format

Refer to **Conf. ScriptsDhcpOptionsFormat**.

Scripts Transfer Retries Number

Refer to **Conf. ScriptsTransferRetriesNumber**.

14.2 Backup/Restore

14.2.1 Basic Backup and Restore Concepts

14.2.1.1 Configuration Backup and Restore

Performing a configuration backup allows you to have a copy of the entire configuration at the time the backup was performed.

The configuration backup can be used:

- to revert the running configuration to a valid configuration when the running configuration generates error messages or no longer works;
- to deploy a valid configuration on other units;
- to revert to a known configuration when too many changes were made to the running configuration;
- to deploy a backup configuration on a replacement unit.

The configuration backup includes every aspects of the configuration, i.e.

- the status and configuration parameters;
- the certificates;
- the Rulesets.

But the configuration backup does not include the File service files, except for the Rulesets.

The configuration backup is an XML file and can, if necessary, be encrypted.

Note: Media5 corp strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

IMPORTANT: Do not edit the configuration image file as it may no longer work.

IMPORTANT: You can use a backup file on a unit with a newer or same firmware version than what is was taken from. A backup file can not be restored on an older firmware version than the one it was taken from.

IMPORTANT: The configuration image can only be restored on the same platform it was taken from.

Backup made on firmware version vX	Unit firmware version	Possible
Backup.v3	Firmware version 3	YES
Backup.v1	Firmware version 3	YES
Backup.v1	Firmware version 1	YES
Backup.v3	Firmware version 1	NO

The Configuration Back and Restore performed on Dgw v2.0.31 includes all Rulesets. However, starting on Dgw v.2.0.32 only the Rulesets modified by the user will be included in the configuration backup and restore. If a configuration backup is performed on Dgw v2.0.31 and restored on a newer version of DGW, all Rulesets existing in v2.0.31 will be copied as custom Rulesets i.e the system will not use the factory Rulesets of the newer version even if they were not modified.

14.2.2 Basic Backup Tasks

14.2.2.1 Performing a Configuration Backup to a File Server

Before you start

Note: Only FTP and TFTP can be used to backup a configuration to a file server.

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)

Steps

- 1) Go to **Management/Backup and Restore**.
- 2) In the **Image Configuration** table, in the **File Name** field, indicate the name of your backup.

Note: The file name is case sensitive. As a best practice, add the *.xml extension. Make sure to indicate the firmware version the backup was made from because a backup file can not be restored on an older firmware version than the one it was taken from.

Note: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your backup, the interfaces used, the device model, etc.

- 3) From the **Transfer Protocol** selection list, select the type of protocol you wish to use to transfer your backup.

Note: This must be consistent with the file server you have configured.

- 4) In the **Host Name** field, enter the file server IP address or FQDN.
- 5) In the **Location** field, enter the path relative to the root of the file server where the backup will be saved.
- 6) If your server requires authentication, enter your username and password.
- 7) From the **Content** selection list, choose the elements you wish to include to the backup.
- 8) If you wish to use encryption for backup operations, complete the **Privacy Parameters**.

Note: Media5 corp strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

- 9) Make sure the file server is started.
- 10) Click **Apply and Backup Now**.

Result

The configuration will be saved on the selected file server.

Note: In all cases, the configuration image file must not be edited by the user.

Image Configuration	
Transfer Parameters	
File Name:	yymmdd_device_name.xml --- Suggestion ---
Transfer Protocol:	FTP
Host Name:	file.server.com
Location:	configuration folder
User Name:	username
Password:	•••••
Backup Parameters	
Content:	Config And Certificates
Privacy Parameters	
Privacy Algorithm:	None
Privacy Key:	

14.2.2.2 Performing a Configuration Backup to the Unit File Management System

Steps

- 1) Go to **Management/Backup and Restore**.

- 2) In the **File Name** field, indicate the name of your backup.

Note: The file name is case sensitive. As a best practice, add the .xml extension. Make sure to indicate the firmware version the backup was made from because a backup file can not be restored on an older firmware version than the one it was taken from.

Note: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your backup, the interfaces used, the device model, etc.

- 3) From the **Transfer Protocol** selection list, select **File**.
- 4) From the **Content** selection list, choose the elements you wish to include to the backup.
- 5) If you wish to use encryption for backup operations, complete the **Privacy Parameters**.

Note: Media5 corp strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

- 6) Click **Apply and Backup Now**.

Result

The configuration will be saved in the unit file management system. The backup file will appear at the end of the list of the **File** page, under **Management/File**.

Image Configuration	
Transfer Parameters	
File Name:	yymmdd_device_name.xml --- Suggestion --- ▼
Transfer Protocol:	File ▼
Host Name:	file.server.com
Location:	configuration folder
User Name:	username
Password:	••••••
Backup Parameters	
Content:	Config And Certificates ▼
Privacy Parameters	
Privacy Algorithm:	None ▼
Privacy Key:	

14.2.3 Basic Restore Tasks

14.2.3.1 Restoring a Configuration From a File Server

Before you start

Depending on the type of transport protocol used, one of the following procedures must be completed:

- [Configuring the FTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)

Steps

- 1) Go to **Management/Backup and Restore**.
- 2) In the **File Name** field, indicate the name of your backup or use the **Suggestion** selection list.

Note: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from. The configuration image can only be restored on the same platform it was taken from.

- 3) From the **Transfer Protocol** selection list, select the type of protocol you wish to use to transfer your backup.

Note: This must be consistent with the file server you have configured.

- 4) In the **Host Name** field, enter the file server IP address or FQDN.

- 5) In the **Location** field, enter the path relative to the root of the file server where the backup will be saved.
- 6) If your server requires authentication, enter your username and password.
- 7) Make sure the file server is started.
- 8) If the backup file is encrypted, complete the **Privacy Parameters**.

Note: The privacy key must match the privacy key used to encrypt the backup file.

- 9) Click **Apply and Restore Now**.

Note: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result

The unit will be restarted. The configuration will be restored from the configured file server, and used as the running configuration.

Image Configuration	
Transfer Parameters	
File Name:	yymmdd_device_name.xml --- Suggestion --- ▼
Transfer Protocol:	FTP ▼
Host Name:	file.server.com
Location:	configuration folder
User Name:	username
Password:	••••••
Backup Parameters	
Content:	Config And Certificates ▼
Privacy Parameters	
Privacy Algorithm:	None ▼
Privacy Key:	

14.2.3.2 Restoring a Configuration from the Unit File Management System

Steps

- 1) Go to **Management/Backup and Restore**.
- 2) In the **File Name** field, indicate the name of your backup or use the **Suggestion** selection list.

Note: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from. The configuration image can only be restored on the same platform it was taken from.

- 3) From the **Transfer Protocol** selection list, select **File**.

- 4) If the backup file is encrypted, complete the **Privacy Parameters**.

Note: The privacy key must match the privacy key used to encrypt the backup file.

- 5) Click **Apply and Restore Now**.

Note: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result

The unit will be restarted. The configuration will be restored from the system's file management system, and used as the running configuration.

Image Configuration	
Transfer Parameters	
File Name:	yymmdd_device_name.xml --- Suggestion --- v
Transfer Protocol:	File v
Host Name:	file.server.com
Location:	configuration folder
User Name:	username
Password:	*****
Backup Parameters	
Content:	Config And Certificates v
Privacy Parameters	
Privacy Algorithm:	None v
Privacy Key:	

14.2.3.3 Restoring a Configuration from Your PC

Steps

- 1) Go to **Management/Backup and Restore**.
- 2) If the Web pages are not encrypted (HTTPS), click **Activate unsecure file importation from the Web browser**, located at the top of the tables.
- 3) In the **Transfer Scripts Through Web Browser** table, browse to the location of the file you wish to restore.

Note: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from. The configuration image can only be restored on the same platform it was taken from.

- 4) Click **Upload & Restore**.

Note: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result

The unit will be restarted. The configuration will be restored from your PC, and used as the running configuration.

Transfer Images Through Web Browser	
Upload Parameters (Clear Selection)	Upload & Restore
C:\Files\Backup\yymmdd_device_name.xml	Browse ...
Privacy Key:	

14.2.4 Advanced Backup and Restore Configuration Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

Image Transfer Cipher Suite

For more details on the following parameters refer to [DGW Configuration Guide - Configuration Reference Guide](#) published on the [Media5 Documentation Portal](#). Refer to **Conf.ImageTransferCipherSuite**.

Image Transfer Tls Version

Refer to **Conf.ImageTransferTlsVersion**.

14.3 Firmware

14.3.1 Basic Firmware Concepts

14.3.1.1 Single File Upgrade

The single file used to upgrade DGW is a binary file (.bin) that contains the modules and the features to install on your Mediatrix unit when a new release is available.

The single file is uploaded to the Mediatrix using the transfer protocols HTTP, HTTPS, FTP, and TFTP.

14.3.2 Basic Upgrade Tasks

14.3.2.1 Adding the Single File to the Server

Before you start

Your file server must be configured. One of the following procedures must first be completed.

- [Configuring the FTP Server](#) (p.27)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the HTTPS Server](#) (p.28)
- [Configuring the TFTP Server](#) (p.28)

Steps

- 1) Copy the Single File .bin to your server. (FTP, HTTP, HTTPS, or TFTP)
- 2) You may rename the file with a shorter name. This will make it easier to type the URL in the **Mfp Url** field in the [Installing Another Firmware Version Using a Single File](#) (p.479) step.

14.3.2.2 Installing Another Firmware Version Using a Single File

Before you start

Make sure to make a backup of your configuration and save the configuration script before proceeding to the next step. For more details, refer to [DGW -Configuration Guide - Configuration Backup/Restore](#) and [DGW Configuration Guide - Configuration Scripts Import and Export](#) documents published on the [Media5 Documentation Portal](#).

Note: Our QA tests cover five (5) major releases back for each new release. If you are upgrading from a load older than five (5) major releases back, you must install an intermediate version before upgrading to the newest one.

Depending on the type of protocol you will use, the following procedures must be completed.

- [Configuring the FTP Server](#) (p.27)
- [Configuring the HTTP Server](#) (p.27)
- [Configuring the TFTP Server](#) (p.28)
- [Configuring the HTTPS Server](#) (p.28)

Steps

- 1) Go to **Management/Firmware**.

- 2) In the **Firmware Update Configuration** table, in the **Firmware URL** field, enter the complete URL for the Single File.

Note: For example, `http://www.myserver.com/firmware.bin` or `tftp://myserver/myfolder/firmware.bin`

- 3) If your server requires authentication, in the **Transfer Credentials** section, enter your username and password.
- 4) If you wish the unit to automatically restart immediately after the upgrade, select **Enable** from the **Automatic Restart Enable** selection list of the **Installation Configuration** table.

Note: If you choose **Disable**, the unit must be manually restarted in order to complete the upgrade. A message will be displayed to restart the unit.

- 5) **Apply Install Now.**

Note: When the firmware pack update fails, the Mediatrix unit tries to download the firmware three times.

Note: All LEDs will cycle from left to right.

- 6) Click **Latest FPU status**, located at the top of the page.
- 7) Click **Restart the Unit**, located at the top of the page.

Note: You will be redirected to the Reboot page.

- 8) Click **Restart**.

Result

All LEDs will cycle from left to right. The upgrade process should take less than 3 minutes and the unit will be restarted a few times. Once the upgrade will be completed, the new firmware pack version will appear in the **Installed Firmware** table (Management/Firmware).

❖ Firmware

Status	
Firmware Updater Status:	Idle
Last Installation Result:	Success
Last Successful Installation:	2019-04-10 08:43:40

Installed Firmware				
Name	Version	Profile	Bank	
Dgw	44.1.1605	STNL-MX-D2000-267	Main - In Use	<button>Factory Reset</button>
Dgw	44.1.1592	STNL-MX-D2000-267	Recovery	<button>Rollback</button>

Firmware Update Configuration	
Firmware URL:	URL of upgrade file
Transfer Credentials	
User Name:	
Password:	

Installation Configuration	
Automatic Restart Enable:	Enable ▾
Default Settings On Restart:	Disable ▾
Automatic Restart Grace Delay (minutes):	0

14.3.3 Basic Downgrade Tasks

14.3.3.1 Reverting to the Previous Firmware Version from DGW v.44.1 or newer

Before you start

It is only possible to revert to a previous version of the firmware if a previous version is available in the recovery bank.

Information

This feature does not apply to the Mediatrix 4102S model.

Steps

- 1) Go to **Management/Firmware**.

2) In the **Installed Firmware** table, click **Rollback**.

Note: The **Rollback** button is only available if there is a previous version available in the recovery bank.

Note: Any configuration changes performed after the installation of the current firmware version will be lost.

Note: Configuration parameters previous to the firmware upgrade will be restored.

Result

Your system will be restarted on the previously installed version.

14.3.4 Advanced Firmware Upgrade Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#). The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

- **Fpu. MfpTransferTlsVersion**
- **Fpu. MfpTransferCipherSuite**
- **Fpu. MfpTransferCertificateValidation**
- **Fpu. MfpTransferCertificateTrustLevel**

14.4 Certificates

14.4.1 Certificates Concepts

14.4.1.1 Certificates

The Mediatrix unit uses digital certificates, which are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates such as:
 - TlsClient: The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
 - TlsServer: The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a Certification Authority (CA)

Although certificates are factory-installed new ones can also be added. Since TLS certificates are validated in terms of time (certificate validation/expiration date, etc.), the use of NTP (Network Time Protocol) is mandatory when using the security features.

The Mediatrix unit uses two types of certificates:

- Host Certificates: used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
- Others: Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

The Conf, Cwmp, Eth, Fpu, Nlm, Sbc, and SipEp services are considered secure as they require certificate validation to establish a secure connection to a remote host. The following parameters, available by the CLI, are used to determine whether or not the connection to the remote host should be validated with the service certificate. By default, the parameters are always set to a value requiring validation.

- Conf.ScriptsTransferCertificateValidation
- Cwmp.TransportCertificateValidation
- Eth.Eap.CertificateValidation

- Fpu.MfpTransferCertificateValidation
- Nlm.PcCaptureTransferCertificateValidation
- Sbc.CertificateValidation
- SipEp.InteropTlsCertificateValidation (also available in the DGW Web page under SIP/Interop)

The certificates must be uploaded to the Mediatrix units. They define how a Mediatrix unit will certify the remote host in order to mark it as secure and suitable for a TLS connection. If the Mediatrix unit does not trust the remote certificate (i.e. does not authenticate it with either one of the 3 methods: HostName, trustedCertificate, DnsSrv), then the Mediatrix unit will not establish the connection.

By default it is not possible to upload a Host certificate without first clicking on Activate unsecure certificate transfer. This is because the certificate upload will be done in clear text, which means the private key will be susceptible to interception. Establishing a connection without certificate validation, i.e. establishing an unsecure connection, should only be used :

- for testing purpose,
- if one cannot identify the required CA cert, or
- the CA cert has mismatched Common Name/Subject Alternate Name. (In this case there is no fallback, it will fail if the name does not match)

Certificates are used to secure the following connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x)

One common use of the host certificate is to allow HTTPS Web access to the unit (which in this case, the device is the TLS server). For more details refer to the [Technical Bulletins - Creating a Media5 Host Certificate with Open SSL](#) document on the [Media5 Documentation Portal](#).

14.4.2 Certificates Tasks

14.4.2.1 Importing a Trusted CA or SIP Server Certificate through the Web Page

Before you start

You must have an SNTP server for time tracking.

Steps

- 1) Go to **Management/Certificates**.
- 2) Click **Activate unsecure certificate transfer**.
- 3) In the **Certificate Import Through Web Browser** table, from the **Type** selection list, select **Other**.

- 4) Click **Browse** and select your certificate.

Note: The name of the certificate cannot have more than 50 characters.

- 5) Click **Import**.
- 6) Click **Apply**.
- 7) Click **restart required services** located at the top of the page.

Result

Host Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	
0090f80b1b9a_thomas_new.pem	0090f80b1b9a	Mediatix Units CA	2019-06-30 20:00:00	2069-06-30 20:00:00	TlsClient, TlsServer	—
sentinel.pem	s400.media5corp.com	ThomasNG CA Authority	2017-08-08 22:22:09	2027-08-08 22:22:09	TlsClient, TlsServer	—

Other Certificates							
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA	
CAMedia5.crt	prod_ca.media5corp.com	prod_ca.media5corp.com	2014-08-07 15:29:47	2058-05-28 15:29:47		Yes	—
DigiCertGlobalCAG2.crt	DigiCert Global CA G2	DigiCert Global Root G2	2013-08-01 08:00:00	2028-08-01 08:00:00		Yes	—
DigiCertGlobalRootG2.crt	DigiCert Global Root G2	DigiCert Global Root G2	2013-08-01 08:00:00	2038-01-15 07:00:00		Yes	—
DigiCertHighAssuranceEVRootCA.crt	DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	2006-11-09 19:00:00	2031-11-09 19:00:00		Yes	—
Mediatix_IntermediateCA.crt	Mediatix Units CA	Media5 Corporation Root CA	2019-02-21 16:27:12	2043-11-26 11:25:46	TlsClient, TlsServer	Yes	—
RootCA.pem.cer	DigiCert Global Root CA	DigiCert Global Root CA	2006-11-09 19:00:00	2031-11-09 19:00:00		Yes	—
Symantec_SHA1_rootCA.cer			1996-01-28 19:00:00	2028-08-01 19:59:59		No	—
ThomasNg_CA.crt	ThomasNG CA Authority	ThomasNG CA Authority	2017-08-08 22:06:46	2044-12-24 21:06:46	TlsClient, TlsServer	Yes	—
Virtual_Root_CA.pem	Media5 Corporation Root CA	Media5 Corporation Root CA	2018-11-26 11:15:47	2043-11-26 11:25:46		Yes	—
verisign_G5_primary_intermediate.cer	VeriSign Class 3 Public Primary Certification Authority - G5		2006-11-07 19:00:00	2021-11-07 18:59:59	TlsClient, TlsServer	Yes	—

Host Certificate Associations											
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	SBC	CWMP	
0090f80b1b9a_thomas_new.pem	☒	☒	☒	☒	☒	☒	☒	☒	☐	☒	
sentinel.pem	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	

Note: Make sure to associate the certificate to the appropriate service. If you are using SBC service, only 1 certificate should be associated to it.

14.4.2.2 Trusted CA Certificate Content Example

```
-----BEGIN CERTIFICATE-----
```

```

MIICNTCCA6AwIBAgIJANYsw8F6ocdbMA0GCSqGSIb3DQEBBQUAMEQxEzARBgoJ
kiaJk/IsZAEZFgNjb20xGTAXBgoJkiaJk/IsZAEZFglZWRpYXRyaXgxZjAQBgNV
BAMTCU1lZGlnNWRLdjAeFw0wODA4MzExNzQwMTBaFw0xODA4MzExNzQwMTBaMEQx
EzARBgoJkiaJk/IsZAEZFgNjb20xGTAXBgoJkiaJk/IsZAEZFglZWRpYXRyaXgx
ZjAQBgNVBAMTCU1lZGlnNWRLdjCBnzANBghkqhkiG9w0BAQEFAA0BjQAwgYkCgYEA
3TJm6UbpfidGJ/kURz3/kwr8lOLY+Fe280/Iq9Klq5m5G0NEbl8aF3+EbSPTV8GU
YlnzXdHHRaVDP5f3gPJU2+obWxbmQSLqvjx6QdxAhNcGTdPv7UGatQapCmQe1/Ct
2qtLqXrxG/bTPv+Vt/WKPMFEA+hjKvJ1hQgQLAUpD2MCAwEAAAMvMC0wDAYDVR0T
BAUwAwEB/zAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcN
AQEFBQADgYEALhFUMWUOV7UTf/Zy3hmZDwyjd8YcuAkb+TrdvK7yHJHTqC0DdvB
L10REHz6Ch7WCiydR8JLj0fAK+kXGYj9VdWj+qvlTnV4PBEvNzA3bbHBqVo0upJM
aDT7atCeNRJ8ipcy7MHN00FRbEW0XKhwnDxQnX2tz0myAeAnDHe5bsQ=
-----END CERTIFICATE-----

```

14.4.2.3 Generating a Private Key

Steps

- 1) Enter **openssl genrsa -aes256 -out your_device.key 2048**

Note: The following step is optional.

- 2) Enter **cp your_device.key your_device.key.orig**
- 3) Enter **openssl rsa -in your_device.key.orig -out your_device.key** to remove the passphrase.

Example

```

[root@localhost mycert]# cp 192.168.1.31.key 192.168.1.31.key.orig
[root@localhost mycert]# openssl rsa -in 192.168.1.31.key.orig -out
192.168.1.31.key
Enter pass phrase for 192.168.1.31.key.orig:
writing RSA key

[root@localhost mycert]#

```

Result

A private key is generated with:

- a length of 2048 bits
- encryption with a 256 bit AES algorithm.

The output filename is **your_device.key**.

14.4.2.4 Creating a Certificate Signing Request (CSR) from a Private Key

Steps

Enter **openssl req -new -key your_device.key -out your_device.csr -sha256**

Result

A CSR is generated from the private key created in the [Generating a Private Key](#) (p.486) procedure with a SHA256 signature algorithm. This is a result example.

```
[root@localhost mycert]# openssl req -new -key 192.168.1.31.key -out
192.168.1.31.csr -sha256
Enter pass phrase for 192.168.1.31.key:
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank. For some fields
there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CA
State or Province Name (full name) []:Quebec
Locality Name (eg, city) [Default City]:Montreal
Organization Name (eg, company) [Default Company Ltd]:Media5
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:192.168.1.31
Email Address []:tac@media5corp.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []
:An optional company name []:
[root@localhost mycert]#
```

14.4.2.5 Signing the CSR file by Your Own Certificate Authority (CA)

Use this procedure if your certificates are signed by a Certificate Authority you have access to.

Steps

Enter **openssl x509 -req -extfile host_ext.cnf -extensions host_ext -sha256 -days 3652 -in your_device.csr -CA CA.crt -CAkey CA.key -CAserial CA.srl -out your_device.crt**

Note:

- **CA.key** is the private key of your CA
- **CA.crt** is the CA's public certificate
- **CA.srl** is the serial number file
- 3652 days is the validity period of the certificate
- **host_ext.cnf** defines the usage of the certificate. It contains:

```
[ host_ext ]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
```

```
extendedKeyUsage = serverAuth, clientAuth
```

Result

This is a result example.

```
[root@localhost mycert]# openssl x509 -req -extfile host_ext.cnf -
extensions host_ext -sha256 -days
3652 -in 192.168.1.31.csr -CA CA.crt -CAkey CA.key -CAserial CA.srl -out
192.168.1.31.crt
Signature ok
subject=/C=CA/ST=Quebec/L=Montreal/O=Media5/OU=TAC/CN=192.168.1.31/
emailAddress=tac@media5corp.com
Getting CA Private Key
Enter pass phrase for CA.key:
root@localhost mycert]#
```

When the certificate will be imported to the Mediatix unit, the information defined for the keyUsage of the host_ext.cnf file will be displayed in **Management>Certificates/Host Certificates** table, under the **Usage** column.

14.4.2.6 Signing the CSR by a Third Party Certificate Authority (CA)

Use this procedure if your certificates are signed by a Certificate Authority you do not have access to.

Steps

Send your CSR to the Third Party Certificate Authority agency responsible for signing your Certificate Signing Request.

Note: VeriSign or Entrust are examples of Third Party Certificate Authority Agencies.

14.4.2.7 Self-signing the CSR File

Use this procedure if your certificates are self-signed, i.e. security is not an issue.

Steps

Enter **openssl x509 -req -extfile host_ext.cnf -extensions host_ext -sha256 -days 3652 -in your_device.csr -signkey your_device.key -out your_device.crt**

IMPORTANT: The command must be entered on a single line, otherwise it will not work.

Note:

host_ext.cnf is a file containing the following which defines the usage of the certificate:

```
[ host_ext ]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
```



```
extendedKeyUsage = serverAuth, clientAuth
```

14.4.2.8 Combining the Private Key and the Signed Certificate

Information

The host certificate required by the Mediatrix contains two parts: the private key and the signed certificate.

Steps

Enter **cat your_device.key your_device.crt > your_device.pem**

Result

This is a result example:

```
[root@localhost mycert]# cat 192.168.1.31.key 192.168.1.31.crt >
192.168.1.31.pem
[root@localhost mycert]# more 192.168.1.31.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAuxKD066oK0igcHQ1r1lnXLiQT9R0oQkE/pp0Do9vXZVsc8D6
uyFldRoDnm6wBHbbrhLgBfsZ5nVHwZ2KCSjJB2THehDXUskLS/4EWMveLcrzGygH
+qjHARwYmYQdEQrYrd/RqkDgnR2j9gocZBRXBfAWYtLgacJe4xLPy317JyR7YrLL
Qfv2hZAXqSdutmYJCys0405oEv1Dv7kfIDQvxP74Qsh0JgmW4Kq0eQdkfo+Xkwlp
pIdYyIHi+5TgWz4YoMRbZHZfKF+VdwOGAeSy2X+QCmHP81GR+SPefHzzn9oUk0Ha
DpjAPgKWUaaJPHrC8k+gsu6Wi0+dCRcUWnX47QIDAQABAoIBAQCnEMFia3iCED44
L5BCKPXGOI2ovXPq3MM5HVTYbABO8ykHtzA0Ln8NNU5GD1PiqMNHkL0/A6D9z39l
yeud9fKSR85dl0y3YhRUqWX4ZxjkjHrPpdB6aoBQU0snLnVG4wjfPyNfiNEPf4k0
EbmJJyEqjHlxiCiIUROsfM5mTInPSZ3Glgm9l3gRZCBBLLf6js+NiLYYi2ASyw6i
F1+KxwOKTvxKa1TR0HYH35urPW528dFyZp8/f2QUUSM4aN5uQrKj8jDwEOIORsw6
+ybzMOpIbbS2I+cbmtDgr5KjjlE1+7dMY3K/hUmUkE+FPZiJf3v8vFFsRucAQcxq
1lg33ogBAoGBAOjZLXyIiz10RC/poRyMEhQ8xRUQaZiI279/J7N426F1G4An8yUL
8Qcmj2PXraLwnl6kX08Mmul7DN78BD0C7LSKK17PIFMH3NV8vWM8ewaE7nP9EqAJ
l0Lt0gN2t+weNL/Mc551XeBCCG9Ifg+pfnjF8kDPjqTe+8U4BEt4dYQxAoGBAM2s
K9vLoXoxJ50ay+ojTMYSuqPfeIND9WuzUJvLAjtgJGKUJsXYUnk5zVZ2IYRMt2EV
nCuAsemwComgDfLimcAEhUzGURG6t0pB7u2FWYiLm+ZJquCxl66p7zrQ/3hc2Q+Y
61mJ3lEay/IIRksS807Pck/k8q9tmGOYg7mQcP19AoGATzg8coceIFB1gHuTFdxN
9laqkr0PwBan90H1BumSh78JCTQOVFAxTcZ/uG9TowEMUJTJ3GIkflUgDuldI8jP
8aikktATZkxhhLy4zn9vqkKFwi6S3KIGtX1yZGVKsbN+rNaJa5rwwnCU4A+g3AFF
hx+JiSVUmaFhtVSWmXq10LECgYAomyRmauA33GL39UAngWLWalFr0WoV00AZv+0
Mol3RY0JdwyORR5LVtEmj94gK7FM1qJlqFv34kzCTTPtyM9ILNxQgxsAYBfN7mSI
unopzj5yYfr9r7Jdxqk3uImnrUgEjXtEJ427w5y86nNoqks1w2XJoGPhxi+GR9w
pIbaVQKBgBX/k9qc/wXf8uI6R650Jn8HiFFI0nr6brscnmd00D7bJPf2b4tKv1ap
CwSwj/BxYt9agncCXYEG8vHVLCTJYNYHJ/+OwID0ttN9dLE2fLPV1sgigMSY9oP
R9KrLT+LPKL1V11s033vuLcD6j0knH2kLKNRSNyxjGt+of0YxRaw
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIJA0cfW0xpBWD+MA0GCSqGSIb3DQEBCwUAMIGLMQswCQYD
VQQGEwJDQTEPMA0GA1UECAwGUXVlYmVjMREwDwYDVQQHDAhNb250cmVhbDEPMA0G
A1UECgwGTWVkaWE1MQwwCgYDVQQLDANUQUxhZjAUBG9NVBAMMDTE5Mi4xNjguMS4y
MjYxITAFBgkqhkiG9w0BCQEWEnRuZ0BtZWVjYjB3JwLnNvbTAeFw0xNTEyMDEx
media5corp.com
```

```
MTQ4MThaFw0yNTEzMzAxMTQ4MThaMIGKMQswCQYDVQQGEwJDQTEPMA0GA1UECAwG
UXVLYmVjMREwDwYDVQQHDAhNb250cmVhbDEPMA0GA1UECgwGTWVkaWE1MQwwCgYD
VQQLDANUQUxFTATBgNVBAMMDDE5Mi4xNjguMS4zMTEhMB8GCSqGSIb3DQEJARYS
dGFjQG1lZGlnNWVncnAuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAuxKD066oK0igcHQ1r1lnXLIQT9R0oQkE/pp0Do9vXZVsc8D6uyFldRoDnm6w
BHbbrhLgBfsZ5nVHwZ2KCsJJB2ThehDXUskLS/4EWMveLcrzGygH+qjHArwYmYQd
EQrYrd/RqkDgnR2j9gocZBRXBfAWYtLgacJe4xLPy317JyR7YrLLQfv2hZAXqSdu
tmYJCys0405oEv1Dv7kfIDQvxP74Qsh0JgmW4Kq0eQdkfo+XkwLppIdYyIHi+5Tg
Wz4YoMRbZHZfKF+VdwOGAeSy2X+QCmHP81GR+SPefHzzn9oUk0HaDpjAPgKWUaaJ
PHrC8k+gsu6wi0+dCRcUwnX47QIDAQABozkwNzAJBgNVHRMEAjAAMAsGA1UdDwQE
AwIESDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEL
BQADggEBAEX1sxk/Ad4aV0rPk2oE/dz0mFmq4LeucYw9uJ6F7SdewAU8pghXMvBu
c0wvToFdEmRTvPmsDghsPmxSgTyL4DBwfJ2YbPfoFK6BDnZAmU3gw37+WXy0w7tW
1ea+kWN4v6Dv/Ga0uBxQ4pAN2lQaDc99fMSP3G3TCFW4lh0lBEeBxvZ0pHwuLrcd
1IbdPNy7z13Ko0639B935Lj1CRGpzEvgSgGtcMhkLifLAL7dhLVcU7fLIA0z5Kov
A70ESnlj8V8DuVirBTNUKGqgY/36g87e7n8g84Xse86vEFhppKzCcZtDIKQ5KvTv
+iLgQLs9mjHAUruNV9+JJx1spv8FZp0=
-----END CERTIFICATE-----
```

14.4.2.9 Importing a Host Certificate through the Web Page

Before you start

You must have an SNTP server for current date and time.

Steps

- 1) Go to **Management/Certificates**.
- 2) Click **Activate unsecure certificate transfer**.
- 3) From the **Type** selection list, select **Host**.
- 4) Click **Browse** and select the Host certificate.
- 5) Click **Apply**
- 6) In the **Host Certificate Associations** table, select the services that Host Certificate should be associated with.

Note: A Host certificate is by default associated with all services. Several Host Certificates can be imported and associated with one or several services.

- 7) Click **Import**.
- 8) Click **Apply**.

Result

This is an example of the result of a Host Certificate imported and associated with all services.

Certificates

Host Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	
FQDN_Unit192.168.27.103.pem	192.168.27.103	192.168.1.27	2017-03-15 13:36:13	2027-03-15 13:36:13	TlsClient, TlsServer	

Other Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA
Cert_MxDefault001.der	Media5 Corporation - Mediatrix Primary CA	Media5 Corporation - Mediatrix Primary CA	2015-03-06 15:06:40	2065-03-06 15:06:40	TlsClient, TlsServer	Yes

Host Certificate Associations											
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	SBC	CWMP	
FQDN_Unit192.168.27.103.pem	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	

Certificate Authorities	
File Name	Override the OCSP URL for issued Certificates
Cert_MxDefault001.der	

Certificate Import Through Web Browser	
Type	Path
Host	Parcourir... FQDN_Unit192.168.27.103.pem Import

14.5 SNMP Configuration

14.5.1 SNMP Basic Concepts

14.5.1.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) can be used to configure all the parameters available in the Mediatrix CPE, to perform firmware updates, to import a configuration and to monitor the Mediatrix CPE.

To configure the Mediatrix CPE parameters with the SNMP, a secure SNMPv3 or a non-secure SNMPv1 connexion can be used. The CPE does not grant an SNMPv3 access without authentication and privacy. Because the connexion is initiated by the Management Server, the communication is usually unable to go through the NAT Firewall.

Unit monitoring is possible with SNMP because it provides access to all the status parameters of the CPE. Furthermore, the CPE can send notifications, called traps, to the Management Server, that will allow the administrator to monitor specific events. Because it is the CPE that sends the notifications, the communication is usually able to go through the NAT Firewall however the SNMP protocol, based on UDP, does not insure reliable delivery of notifications.

The Mediatrix CPE supports the following SNMP methods:

- GetRequest
- SetRequest
- GetResponse

- SetResponse
- Trap
- GetWalk

The following Management Servers are certified to be used with our Mediatrix units:

- UMN
- HP Openview

The [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#) provides the list of all available parameters.

14.5.2 SNMP Basic Tasks

14.5.2.1 Securing SNMP Interface

Steps

- 1) Go to **Management/SNMP**.
- 2) In the **SNMP Configuration** table, set the following parameters:
 - a) Set **Enable SNMP V1** to **Disable**.
 - b) Set **Enable SNMP V2** to **Disable**.
 - c) Set the **Privacy Protocol**.
 - d) In the **Privacy Password** field, enter a password of your choosing.
- 3) Click **Apply**.

Result

SNMP Configuration	
General Configuration	
SNMP Port:	161
SNMP Protocol	
Enable SNMP V1:	Disable
Enable SNMP V2:	Disable
Enable SNMP V3:	Enable
Authentication Protocol:	MD5
Privacy Protocol:	DES
Privacy Password:	
Community:	public
SNMP Trap	
Enable SNMP Trap:	Disable
Trap Destination(s):	192.168.10.10:162

14.6 CWMP

14.6.1 Basic CWMP Concepts

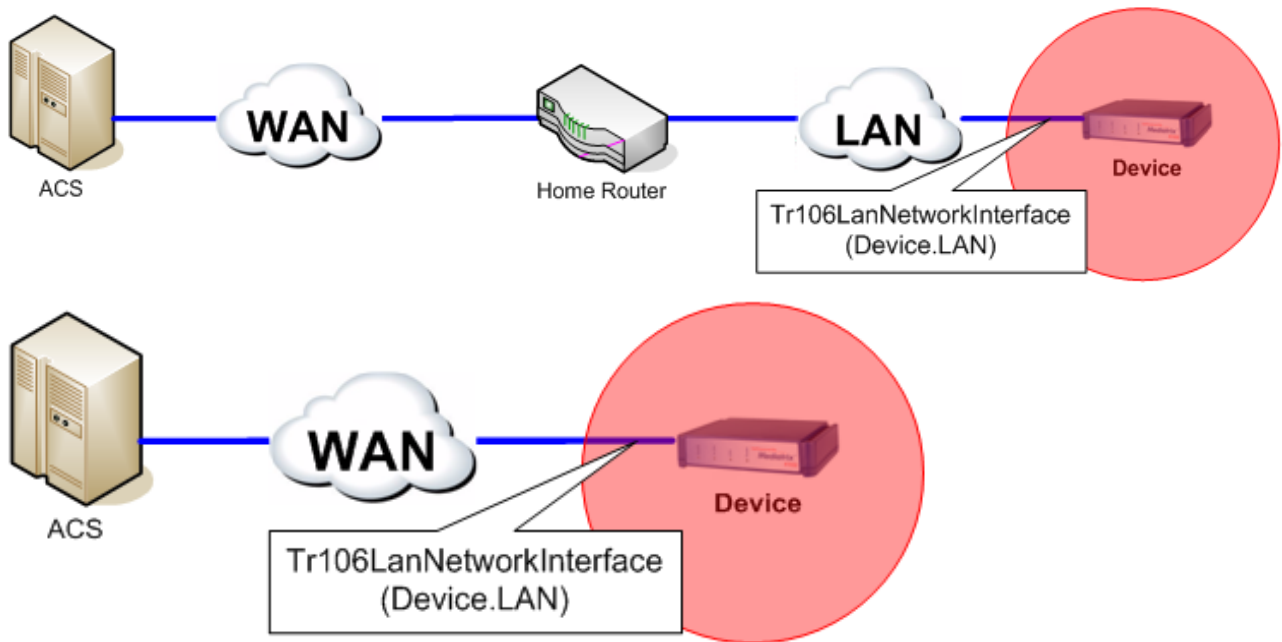
14.6.1.1 Data Model

The Data model is a hierarchical structure of supported device parameters.

Broadband Forum publishes its data model standards, with complete information about each parameter value, the type and the meaning. For more details refer to <https://www.broadband-forum.org/standards-and-software/technical-specifications/tr-069-files-tools>. Each manufacturer uses parts of this standard in his implementation, but can include proprietary parameters.

14.6.1.2 Device Profile

The Cwmp service supports the data model template for device (TR-106) if the RootElement is set to 'Device'



A TR-106 device is a CPE device residing in the home network. This device has a single network interface connected on the LAN side of the home router or directly on the Internet. The **Tr106LanNetworkInterface** parameter identifies that network interface.

- Supported data model for the Device:1 object:
 - Baseline:1
 - LAN:1
 - Time:1
 - VoiceService:1 (Partial Support)
 - GatewayInfo:1

14.6.1.3 Services Parameters

Unless otherwise specified, {i} = 1

Name		Access	Notification
VoiceService.{i}.³		Present	N/A
	The top-level object for a CPE with voice capabilities. {i} is limited to '1' in current implementation.		
VoiceServiceNumberOfEntries		Read-only	None
	The number of entries in the VoiceService table. Returns '1'.		
VoiceService.{i}.Capabilities.		Present	N/A
	The overall capabilities of the VoIP CPE. {i} is limited to 1 in current implementation.		
MaxProfileCount		Read-only	None
	Maximum supported number of distinct profiles. Returns '1'.		
MaxLineCount		Read-only	None
	Maximum supported number of lines for all profiles. Returns the number of ports on the CPE device.		
SignalingProtocols		Read-only	None
	List of supported signaling protocols. Returns 'SIP/2.0' value.		
VoiceService.{i}.Capabilities.SIP.		Present	N/A
	SIP-specific capabilities. {i} is limited to '1' in current implementation.		
Role		Read-only	None
	The role of this VoIP CPE. Returns 'UserAgent' value.		
Transports		Read-only	None
	List of supported SIP transport protocols. Returns 'UDP, TCP, TLS' value.		
URISchemes		Read-only	None

³ This object and its parameters are only available if the TR-104 option is enabled.

Name		Access	Notification
	List of supported URI schemes beyond the URI schemes required by the SIP specification. Returns 'sip' value.		
VoiceService.{i}.VoiceProfile.{i}		Present	N/A
	Object associated with a collection of voice lines with common characteristics. Both {i}s are limited to 1 in current implementation.		
Reset		Read/Write	None
	When the value is set to 'true', all lines of the profile are forced to be reset, causing the unit to be reinitiatlised and all start-up actions, such as registration, to be performed. This restarts SipEp service. Always returns false, i.e '0'.		
VoiceService.{i}.VoiceProfile.{i}.SIP.		Present	N/A
	Voice profile parameters that are specific to SIP user agents. Both {i}s are limited to '1' in current implementation.		
ProxyServer		Read/Write	None
	Host name or IP address of the SIP proxy server. An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. 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. Returns and sets the host part of the SipEp.DefaultStaticProxyHomeDomainHost parameter. Setting a new value to this parameter triggers a non-graceful service restart.		
ProxyServerPort		Read/Write	None
	Destination port to be used when connecting to the SIP server. Returns and sets the port of the SipEp.DefaultStaticProxyHomeDomainHost parameter. Setting a new value to this parameter triggers a non-graceful service restart.		
RegistrarServer		Read/Write	None

Name	Access	Notification
	Host name or IP address of the SIP registrar server. A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. Returns and sets the host part of the SipEp.DefaultStaticRegistrarServerHost parameter. Setting a new value to this parameter triggers a non-graceful service restart.	
RegistrarServerPort	Read/Write	None
	Destination port to be used in connecting to the SIP registrar server. An empty string or '0' indicates that the CPE will use the default value, i.e '5060'. Returns and sets the port of the SipEp.DefaultStaticRegistrarServerHost parameter. Setting a new value to this parameter triggers a non-graceful service restart.	
UserAgentDomain	Read/Write	None
	CPE domain string. This value is saved in an internal database. The value is initially set to an empty string and reset to an empty string on a factory default reset. If an empty string is specified, the SIP listening IP address is used. This value is set to the SipEp.UserAgent.ContactDomain parameter when no specific URI domain is specified by the ACS (see .VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.URI). Returns the last value set by the ACS. Setting a new value to the UserAgentDomain parameter triggers a registration refresh.	
UserAgentPort	Read/Write	None
	Port used for incoming call control signaling. Returns the value of the SipEp.Gateway[name=default].Port parameter. Sets the value of the SipEp.Gateway[name=default].Port and SipEp.Gateway[name=default].SecurePort parameters Setting a new value to the UserAgentPort parameter triggers a non-graceful service restart.	
UserAgentTransport	Read/Write	None

Name	Access	Notification
	Returns the enable transports in this priority: 'TLS', 'UDP' and 'TCP'. • If TLS is enabled, 'TLS' will be reported. • If UDP is enabled, 'UDP' will be reported. • If TCP is enabled, 'TCP' will be reported. • If all 3 are enabled, 'TLS' will be reported. • If two are enabled, only the highest priority will be reported. When set, disables all transports except the one being set. If 'TCP' is set, TLS and UDP will be disabled and TCP will be enabled. Maps to the following parameters: • SipEp.TransportConfig.TransportConfig[GatewayName=default].UdpEnable parameter. • SipEp.TransportConfig.TransportConfig[GatewayName=default].TcpEnable parameter. • SipEp.TransportConfig.TransportConfig[GatewayName=default].TlsEnable parameter. Setting a new value to the UserAgentTransport parameter triggers a non-graceful service restart.	
OutboundProxy	Read/Write	None

Name	Access	Notification
	Host name or IP address of the outbound proxy. To disable the outbound proxy, use '0.0.0.0'. 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 UA 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 will contain 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). Returns and sets the host part of the SipEp.DefaultStaticProxyOutboundHost parameter. Setting a new value to the OutboundProxy parameter triggers a non-graceful service restart.	
OutboundProxyPort	Read/Write	None
	Destination port to be used in connecting to the outbound proxy. This parameter is ignored unless the value of the OutboundProxy parameter is not empty. Returns and sets the port of the SipEp.DefaultStaticProxyOutboundHost parameter. Setting a new value to the OutboundProxyPort parameter triggers a non-graceful service restart.	
ConferenceCallURI	Read/Write	Passive
	URI used in the request-URI of the INVITE sent to the conference server. This parameter only has an effect when the conference type is 'ConferenceServer'. See the EpServ.DefaultConferenceType parameter. Please refer to the documentation shipped with your device for more details regarding this parameter's semantics. If a specific configuration is set in the GwSpecificConference.ServerHost parameter and the GwSpecificConference.EnableConfig parameter is set to 'Enable', then it overrides the current default configuration. Returns and sets the SipEp.DefaultStaticConferenceServerUri parameter.	
VoiceService.{i}.VoiceProfile.{i}.Line.		
	Object associated with a distinct voice line. At most, one enabled entry in this table can exist with a given value for the DirectoryNumber parameter. Both {i}s are limited to 1 in current implementation.	

Name		Access	Notification
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.		Present	N/A
	First two {i}s are limited to 1 in current implementation. The Line.{i} starts from 1 up to the number of ports on the device, also represented by the VoiceService.{i}.Capabilities.MaxLineCount parameter. If the CPE device has different types of lines, the numerical index follows this order: FXS, FXO, E1T1, and BRI lines.		
Enable		Read/Write	Passive

Name	Access	Notification
	Enables or disables this line, or places it into a quiescent state. Returns the value of the EpAdm[i].InitialAdminStateConfig parameter: • Returns 'Disabled' when the value of the InitialAdminStateConfig parameter is 'Locked'. • Returns 'Enabled' when the value of the InitialAdminStateConfig parameter is 'Unlocked'. Set the Enable parameter has the following effect: • Enabled: • Issues the <code>EpAdm.Endpoint[i].Unlock</code> command. • Sets the value of the EpAdm.Endpoint[i].InitialAdminStateConfig parameter to 'Unlocked'. • Disabled: • Issues the <code>EpAdm.Endpoint[i].ForceLock</code> command. • Sets the value of the EpAdm.Endpoint[i].InitialAdminStateConfig parameter to 'Locked'. • Quiescent: • Issues the <code>EpAdm.Endpoint[i].Lock</code> command • Sets the value of the EpAdm.Endpoint[i].InitialAdminStateConfig parameter to 'Locked'.	
DirectoryNumber	Read/Write	Passive

Name	Access	Notification
	Directory number associated with this line. Returns and sets the value of the SipEp.UserAgent.FriendlyName parameter. Setting a new value to the DirectoryNumber parameter triggers a registration refresh.	
Status	Read-only	Passive
	Indicates the status of this line. Returned value is based on the following parameters: • EpAdm.Endpoint.AdminState parameter. • EpAdm.Endpoint.UsageState parameter. • SipEp.RegistrationStatus parameter. Detailed mapping is as follows: • If AdminState == 'Locked' then Status = 'Disabled' • If UsageState == Idle Active Busy and AdminState == 'Shuttingdown' then Status = 'Quiescent' • If UsageState == Idle Active Busy then Status = 'Up' • If RegistrationStatus[endpoint == i].State == Unregistering then Status = 'Unregistering' • If RegistrationStatus[endpoint == i].State == Registering Refreshing then Status = 'Registering' • Otherwise Status = 'Error'	
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.		Present N/A
	Voice line parameters that are specific to SIP call signaling. First two {i}s are limited to 1 in current implementation. The last {i} takes all values from 1 to the value of the VoiceService.{i}.Capabilities.MaxLineCount parameter.	
AuthUserName	Read/Write	Passive

Name	Access	Notification
	Username used to authenticate the connection to the server. Returns and sets the value of the SipEp.Authentication.Username parameter. Also sets the value of the SipEp.UserAgent.Username parameter if the value of the VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.URI parameter is empty Configures the SipEp.Authentication[].CriteriaSelection and SipEp.Authentication[].Endpoint parameters. Setting a new value to the AuthUserName parameter triggers a registration refresh. Mapping between index i of Line{i} and the index of the SipEp.Authentication table behaves differently from the other internal tables. The numerical value of i is directly used as the index of the SipEp.Authentication table. If i = 2, index of the SipEp.Authentication table is 2. Therefore, any modification to this table made by other means must follow this convention.	
AuthPassword	Write	None
	Password used to authenticate the connection to the server. Set value of proper columnar SipEp.Authentication.Password parameter. Configures the SipEp.Authentication[].CriteriaSelection and SipEp.Authentication[].Endpoint parameter. Setting a new value to the AuthPassword parameter triggers a registration refresh. Mapping between index i of Line{i} and the index of the SipEp.Authentication table works the same as for the AuthUserName parameter. Returns an empty string.	
URI	Read/Write	Active
	URI by which the user agent will identify itself for this line. Returns the SIP URI used by the device (formed with the SipEp.UserAgent.Username@SipEp.UserAgent.ContactDomain parameter). This value is saved in an internal database. The value is initially set to an empty string and reset to an empty string on a factory default reset. Sets the value of the SipEp.UserAgent.Username parameter and, if an optional host part is given, sets the value of the SipEp.UserAgent.ContactDomain parameter. Setting a new value to the URI parameter triggers a registration refresh.	
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Stats.	Present	N/A

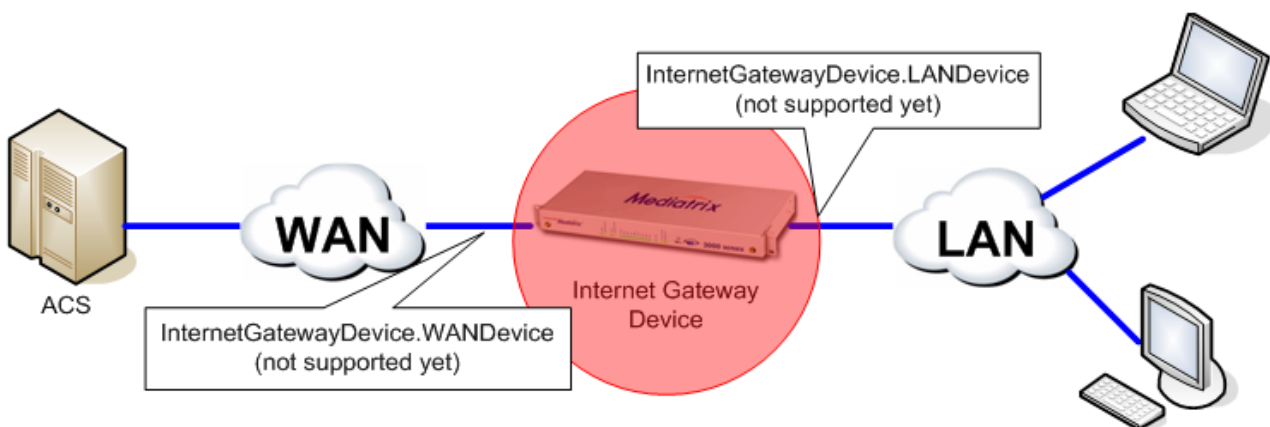
Name	Access	Notification
	Statistics for this voice line instance. First two {i}s are limited to 1 in current implementation. The last {i} takes all values from 1 to the value of VoiceService.{i}.Capabilities.MaxLineCount parameter Note: These statistics are from the IP network standpoint. If a call is directly established between two telephony interfaces (between two local FXS lines for instance), statistics are not cumulated. Note: Unless otherwise stated, these statistics are updated each time the processing of a call terminates. Note: These statistics are cleared when the service they originate from is started or restarted. Note: These statistics are cumulative for all the calls on the line. They are updated at the end of each call. Note: The Line statistics are obtained from the EpServ and Mipt services. Lines in TR-104 are mapped to endpoints of the device. The CWMP service builds an internal map to convert between the numerical index {i} used as the 'Line' number and the textual endpoint indexes used in the tables of the EpServ and Mipt services. When statistics are reported for multi-channel endpoints, they cover all the channels of the endpoint. For instance, the number of received packets for a 'Line' is the number of packets received for all the channels of the related endpoint. Note: The media statistics are only available for FXS and FXO lines. The call statistics are only available for FXS lines.	
ResetStatistics	Write	None
	When set to one, resets the statistics for this voice line. Always returns 'false'. Maps to the Mipt.EndpointStatistics[i].Reset and EpServ.CallStatistics[i].Reset parameters.	
PacketsSent	Read-only	Passive
	Returns the total number of RTP packets sent for this line. Maps to the Mipt.EndpointStatistics[i].PacketsSent parameter.	
PacketsReceived	Read-only	Passive
	Returns the total number of RTP packets received for this line. Maps to the Mipt.EndpointStatistics[i].PacketsReceived parameter.	

Name		Access	Notification
BytesSent		Read-only	Passive
	Returns the total number of RTP payload bytes sent for this line. Maps to the Mipt.EndpointStatistics[i].BytesSent parameter.		
BytesReceived		Read-only	Passive
	Returns the total number of RTP payload bytes received for this line. Maps to the Mipt.EndpointStatistics[i].BytesReceived parameter.		
IncomingCallsReceived		Read-only	Passive
	Returns the total number of incoming calls received. Maps to the EpServ.EndpointStatistics[i].IncomingCallsReceived parameter.		
IncomingCallsAnswered		Read-only	Passive
	Returns the total number of incoming calls answered by the local user. Maps to the EpServ.EndpointStatistics[i].IncomingCallsAnswered parameter.		
IncomingCallsConnected		Read-only	Passive
	Returns the total number of incoming calls that successfully completed call setup signaling. Maps to the EpServ.EndpointStatistics[i].IncomingCallsConnected parameter.		
IncomingCallsFailed		Read-only	Passive
	Returns the total number of incoming calls that failed to successfully complete call setup signaling. Maps to the EpServ.EndpointStatistics[i].IncomingCallsFailed parameter.		
OutgoingCallsAttempted		Read-only	Passive
	Returns the total number of outgoing calls attempted. Maps to the EpServ.EndpointStatistics[i].OutgoingCallsAttempted parameter.		
OutgoingCallsAnswered		Read-only	Passive
	Returns the total number of outgoing calls answered by the called party. Maps to the EpServ.EndpointStatistics[i].OutgoingCallsAnswered parameter.		
OutgoingCallsConnected		Read-only	Passive
	Returns the total number of outgoing calls that successfully completed call setup signaling. Maps to the EpServ.EndpointStatistics[i].OutgoingCallsConnected parameter.		

Name		Access	Notification
OutgoingCallsFailed		Read-only	Passive
Returns the total number of outgoing calls that failed to successfully complete call setup signaling. Maps to the EpServ.EndpointStatistics[i].OutgoingCallsFailed parameter.			
CallsDropped		Read-only	Passive
Returns the total number of calls that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination. Maps to the EpServ.EndpointStatistics[i].CallsDropped parameter.			
TotalCallTime		Read-only	Passive
Returns the cumulative duration of all IP calls on the endpoint since service start, in seconds. Maps to the EpServ.EndpointStatistics[i].TotalCallTime parameter.			
AverageReceiveInterarrivalJitter		Read-only	Passive
Average received interarrival jitter, in microseconds. This value is based on the average interarrival jitter of each call ended during the collection period. The value is weighted by the duration of the calls. Maps to the Mipt.EndpointStatistics[i].AverageReceiveInterarrivalJitter parameter.			

14.6.1.4 Gateway Profile

The Cwmp service supports the data model template for internet gateway device (TR-98) if the RootElement is set to 'InternetGatewayDevice'.



The Internet Gateway Device is a CPE device at the frontier of the home network and the public Internet. It normally implements at least 2 network interfaces, one for the WAN and one for the LAN.

14.6.1.5 TR-069 or CPE WAN Management Protocol (CWMP)

The Technical Report 069 (TR-069), also known as CWMP, is a Broadband Forum technical specification. This protocol can be used to monitor and update the Mediatrix unit configurations and firmware. In other words, when using TR-069, the Mediatrix unit can get in contact with an Auto Configuration Server (ACS) to initiate a configuration script transfer/execution and a firmware upgrade.

The first time the Mediatrix unit is connected to the network, it will attempt to contact the Auto Configuration Server (ACS), which is the entry point for the administrator. The Mediatrix unit will obtain the URL of the ACS using either the DHCP server with option 43 or by retrieving the information directly from the Customer's Profile. Therefore, upon start-up, the Mediatrix unit will contact the ACS, which in return will send the required configuration files and initiate, if necessary, a firmware update. This automated sequence is what is referred to as zero-touch, as the Mediatrix unit is automatically configured by the ACS according to the instructions given by the administrator without manual intervention on the unit.

The administrator can determine a schedule for the Mediatrix unit to periodically contact the ACS. These contacts will allow the Mediatrix unit to:

- verify if new configurations are available,
- verify if a new firmware update is available and
- send notifications for monitoring purposes.

Monitoring is achieved by regularly sending notifications to the ACS, through the mean of "Inform" requests, which can be:

- Passive: the information is sent according to the schedule.
- Active: the information is sent immediately when a parameter status changes, regardless of the periodic schedule.

Because the Periodic Informs are initiated by the Mediatrix unit, they have no problem passing through residential or enterprise NAT and firewalls.

Furthermore, the administrator can initiate a connection to the Mediatrix unit to perform immediate maintenance or monitoring. This will only be possible if the NAT firewall has been configured to allow communications initiated by the ACS.

The TR-069 protocol can be activated on units that are already deployed with a licence key (For more details on licences refer to the [Technical Bulletin - How to activate a licence on a Mediatrix unit](#) published on the [Media5 Documentation Portal](#)). However, it can be enabled/disabled for a specific configuration via the Management interface.

TR-069 methods supported by the Mediatrix unit include:

- SetParameterValues
- GetParameterValues
- AddObject

- DeleteObject
- Download
- Reboot
- Upload
- FactoryReset

14.6.1.6 TR-104

The Technical Report 104 (TR-104) describes the data model for provisioning of a voice-over-IP (VoIP) CPE device by an Auto Configuration Server (ACS) using the mechanism defined in TR-069. Configuring the TR-104 parameters in DGW allows you to enable or disable the provisioning parameters for VoIP CPE, such as calls statistics.

- The Media5 implementation of TR-104 is limited to the SIPEndpoint profile.
- Active notifications are not supported for all objects except when explicitly mentioned. (for more details request the Supported TR-069 Methods and Parameters document from your representative).
- Only FXS lines can be managed by the TR-104 profile.
- BRI, PRI or FXO lines are not supported by the TR-104 profile.
- A single voice profile is supported, it is instantiated by default. No creation or deletion of voice profile is allowed.
- Only a subset of parameters is currently supported.
- When TR-104 is used, it is highly recommended not to use other means of configuration (since TR-104 assumes some configuration).

14.6.1.7 TR-106

Technical Report 106 (TR-106) is the Data Model Template for TR-069-Enabled Devices. The configuration of the TR-106 Network Interface parameter in DGW allows you to specify the network interface to be used for the TR-106 LAN profile to report network statistics.

- If no network interface is configured for TR-106, i.e. the field is left empty under **Management/Misc/CWMP**, the Mediatrix unit will use the network interface configured under **Management/Misc/System Management/Network Interface**.
- If the network interface configured for TR-106 is set to **All**, the Mediatrix unit will use the network interface configured for contacting the ACS in the **TR-106 Configuration** section of the **CWMP Configuration** table. The TR-106 Data Model template can only be used if **Root Element** is set to **Device**. Refer to [Configuring the Report Network Statistics \(Through the TR-106 Data Model\)](#).

Note: This parameter can also be set via Cwmp.RootElement.

The TR-106 Data Model template can only be used if the **Cwmp.RootElement** parameter value is **Device**.

14.6.1.8 TR-111

Technical Report 111 (TR-111) allows the remote management of home networking devices through NAT traversal mechanisms, as defined in TR-069 Annex G (formerly in TR-111).

The TR-111 parameters defined in DGW allows the activation and configuration of a STUN server, so devices behind a NAT can be reached .

14.6.1.9 Special Consideration for TR-104 Parameters

Some parameters under VoiceService tree requires some parameters to be configured in a defined way to work. The default values of the Mediatrix profiles interfere with TR-104 functionality. Here is a table that summarizes what needs to be configured for each parameter.

Device.Services.VoiceService.{i} . ⁴	{i} is limited to '1' in current implementation.
Device.Services.VoiceService.{i}.VoiceProfile.{i} .	Both {i}s are limited to 1 in current implementation.
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i} .	The Line.{i} starts from 1 up to the number of ports on the device, also represented by the VoiceService.{i}.Capabilities.MaxLineCount parameter.
Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP .	
AuthUserName / AuthPassword	The realm must be manually set or disabled.
URI	Setting the CRout.AutoRoutingCriteriaType to 'SipUsername' for auto routing might be required to work with the proper SIP URIs received in INVITE. SipEp.UserAgent[].Register MUST be set to 'Enable' if registration is required. This can not be enabled by TR-104 parameters (but can be by a configuration script).

⁴ This object and its parameters are only available if the TR-104 option is enabled.

14.6.2 Basic CWMP Tasks

14.6.2.1 Configuring the Access to the Auto Configuration Server (ACS)

Before you start

The CPE WAN Management Protocol (CWMP) service must be started (under **System/Services**).

Steps

- 1) Go to **Management/CWMP**.
- 2) In the **CWMP Configuration** table, under the **ACS Configuration** section, set the following parameters:
 - **ACS URL Config Source**
 - **ACS Static URL**
 - **username**
 - **Password**

Note: The **username** and **Password** fields are not accessible if you have the User or Observer access right. Also, the **ACS Static URL** field is only editable if the **ACS URL Config Source** field has been configured to **Static**.

- 3) Click **Apply**.

Result

ACS Configuration	
ACS Status:	No URL configured
ACS URL:	
ACS URL Config Source:	DHCP
ACS Static URL:	
Username:	
Password:	

14.6.2.2 Configuring the CWMP Establishment (TR-069)

Before you start

The CPE WAN Management Protocol (CWMP) service must be started (under **System/Services**).

Steps

- 1) Go to **Management/CWMP**.

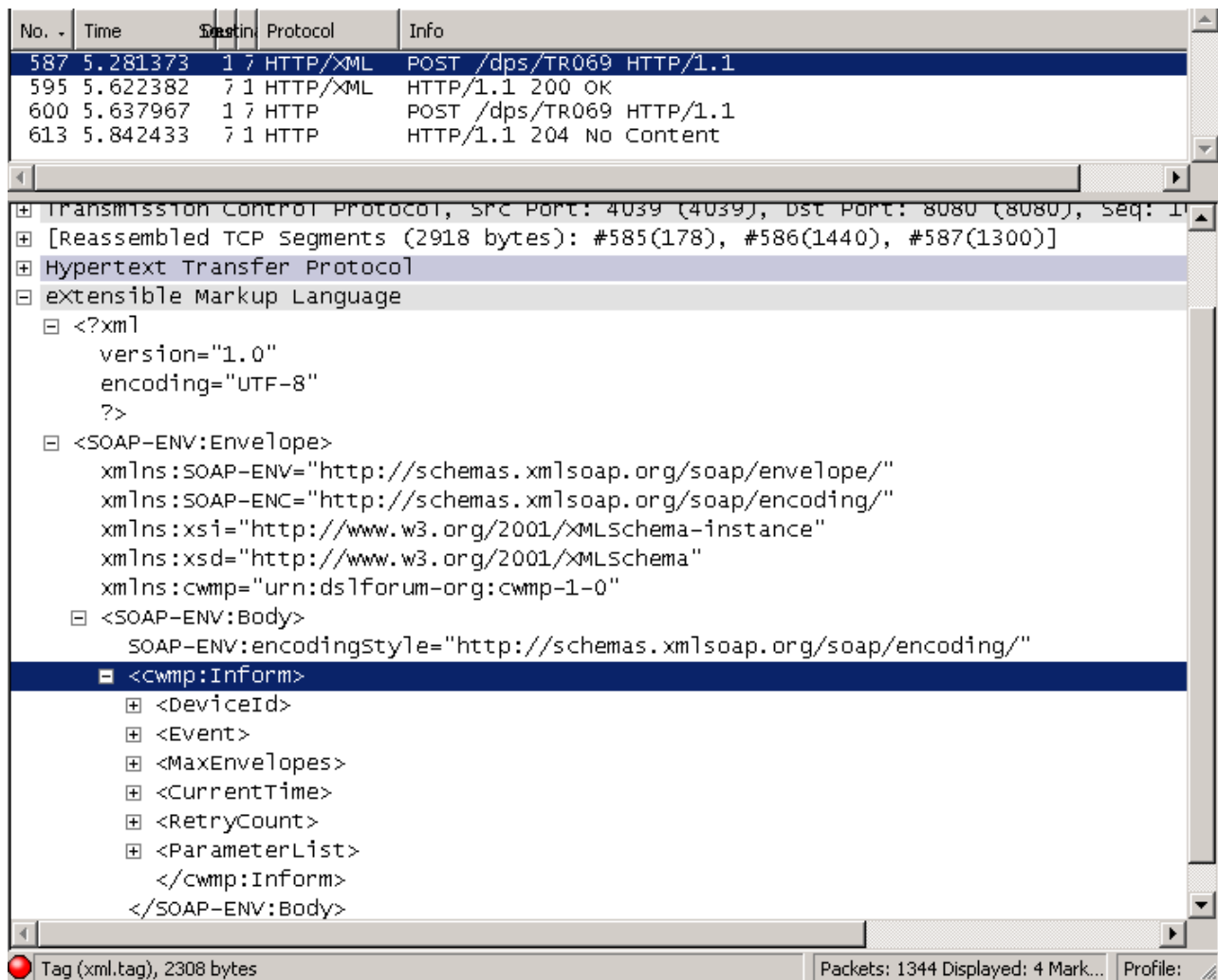
- 2) In the **CWMP Configuration** table, set the following parameters:
 - a) Set **Root Element** to **Device** or **Internet Gateway Device**, depending on your configuration.
 - b) Configure the **Listening Port** to reflect your configuration.
 - c) Set **ACS URL Config Source** to reflect your configuration.

Note: If you chose **Static**, configure the **ACS Static URL**. HTTP and HTTPS are supported.

- d) Under **TR-069 Configuration** section, set **Annex F** to **Enable**.
- e) If using authentication, configure **User Name** and **Password** to reflect your configuration.

Result

If everything is configured correctly, you should see a TCP connection being established between your Mediatrix unit and the TR-069 server (from now on simply ACS). After the TCP connection has been established, the unit will send its first "Inform" message to the ACS, as seen below. Note that there will be more HTTP POST messages sent to the ACS (those can be empty) until the server returns a "204 No Content" message.



14.6.2.3 Configuring VoIP Provisioning (TR-104 Data Model)

Before you start

The CPE WAN Management Protocol (CWMP) service must be started (under **System/Services**).

Steps

- 1) Go to **Management/CWMP**.
- 2) In the **CWMP Configuration** table, under the **TR-104 Configuration** section, from the drop down list, select **Enable**.
- 3) Click **Apply**.

Result

The **Device.Services.VoiceService** parameters, listed in the *Tr069DataModelSupport-Functional_Specification.pdf*, will be enabled.

CWMP Configuration	
General Configuration	
Root Element:	Device
Listening Port:	0
ACS Configuration	
ACS Status:	No URL configured
ACS URL:	
ACS URL Config Source:	DHCP
ACS Static URL:	
Username:	
Password:	
Periodic Inform Configuration	
Periodic Inform:	Disable
Periodic Inform Interval:	3600
Periodic Inform Time:	0001-01-01T00:00:00Z
TR-069 Configuration	
Annex F:	Disable
TR-104 Configuration	
TR-104:	Enable
TR-106 Configuration	
Network Interface:	
TR-111 Configuration	
STUN Status:	Disabled
STUN:	Disable
NAT Detected:	No
STUN Server:	

14.6.2.4 Configuring the Access to the STUN Server TR-111

Before you start

The CPE WAN Management Protocol (CWMP) service must be started (under **System/Services**).

Steps

- 1) Go to **Management/CWMP**.

- 2) In the **CWMP Configuration** table, under the **TR-111 Configuration** section, complete the fields as required.
- 3) Click **Apply**.

Result

CWMP Configuration	
General Configuration	
Root Element:	Device
Listening Port:	0
ACS Configuration	
ACS Status:	No URL configured
ACS URL:	
ACS URL Config Source:	DHCP
ACS Static URL:	
Username:	
Password:	
Periodic Inform Configuration	
Periodic Inform:	Disable
Periodic Inform Interval:	3600
Periodic Inform Time:	0001-01-01T00:00:00Z
TR-069 Configuration	
Annex F:	Disable
TR-104 Configuration	
TR-104:	Disable
TR-106 Configuration	
Network Interface:	
TR-111 Configuration	
STUN Status:	Disabled
STUN:	Enable
NAT Detected:	No
STUN Server:	Host name of IP address of STUN server

14.6.2.5 Configuring the Report Network Statistics (Through the TR-106 Data Model)

Before you start

The CPE WAN Management Protocol (CWMP) service must be started (under **System/Services**).

The TR-106 Data Model template can only be used if the **Cwmp.RootElement** parameter value is **Device**.

Steps

- 1) Go to **Management/CWMP**.
- 2) In the **CWMP Configuration** table, under the **TR-106 Configuration** section, in the **Network Interface** field indicate the network interface referred by the TR-106 LAN profile.
 - If left empty, use the network interface configured in the Hoc.ManagementInterface parameter.
 - If the Hoc.ManagementInterface parameter is set to **All**, use the network interface used for contacting the ACS.
- 3) Click **Apply**.

Result

The network statistics of the network interface are advertised to the ACS through a TR-106 Data Model.

CWMP Configuration	
General Configuration	
Root Element:	Device
Listening Port:	0
ACS Configuration	
ACS Status:	No URL configured
ACS URL:	
ACS URL Config Source:	DHCP
ACS Static URL:	
Username:	
Password:	
Periodic Inform Configuration	
Periodic Inform:	Disable
Periodic Inform Interval:	3600
Periodic Inform Time:	0001-01-01T00:00:00Z
TR-069 Configuration	
Annex F:	Disable
TR-104 Configuration	
TR-104:	Disable
TR-106 Configuration	
Network Interface:	TR-106 LAN profile network interface
TR-111 Configuration	
STUN Status:	Disabled
STUN:	Disable
NAT Detected:	No
STUN Server:	

14.6.3 Advanced CWMP Parameters

14.6.3.1 Advanced CPE WAN Management Protocol (CWMP) Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#). The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

For ACS

- To set the parameter type validation when the ACS assigns a value to a parameter
Cwmp.interopParameterTypeValidation
- To set the access mode to the local log table from the ACS: **Cwmp.NlmLocalLogLogEnable**
- To define the username to authenticate an ACS making a connection request to the CPE:
Cwmp.ConnectionRequestUsername
- To define the password to authenticate an ACS making a connection request to the CPE:
Cwmp.ConnectionRequestPassword

Note: Enabling access will require significant CPU resources and impact performance of your unit when notifications are sent frequently to the local log.

For TR-069 (CWMP) establishment

- To set the HTTPS transport cipher suite configuration for TR-069 (CWMP):
Cwmp.TransportHttpsCipherSuite .
- To set the HTTPS Transport Tls Version configuration for TR-069 (CWMP):
Cwmp.TransportHTTPSTlsVersion.
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

For TR-111

- To set the period range, in seconds, at which STUN Binding Requests must be sent by the unit for the purpose of maintaining the STUN connection: **Cwmp.tr111StunKeepAlivePeriod**. The current implementation does not allow a range. The minimum and maximum values must be the same.
- To set the value of the STUN username attribute to be used in Binding Requests:
Cwmp.tr111StunUsername
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

For the MAC address

- To set the MAC address format: **Cwmp.InteropMacAddressFormat**.

14.6.3.2 Supported Parameters for the GatewayDevice Object

Note: Parameters not present are not supported.

Note: When Write parameters are read, an empty value is returned.

Note: The **Notification** column refers to the maximum level of notification allowed for the parameter. Unless stated otherwise, the parameter notifications are turned off by default.

Name	Access	Notification
InternetGatewayDevice.	Present	N/A
	The top-level object for an Internet Gateway Device.	
DeviceSummary	Read-only	Passive
	Explicit summary of the top-level data model of the device, including version and profile information. Returns the 'InternetGatewayDevice:1.0[] (Baseline:1)' value.	
LANDeviceNumberOfEntries	Read-only	Not supported
	Number of instances of the LANDevice object. Returns '0'.	
WANDeviceNumberOfEntries	Read-only	Not supported
	Number of instances of the WANDevice object. Returns '0'.	
InternetGatewayDevice.DeviceInfo	Present	N/A
	This object contains general device information.	
Manufacturer	Read-only	Passive
	The manufacturer of the CPE. Returns the value of the HiddenManufacturer hidden parameter.	
ManufacturerOUI	Read-only	Passive
	Organisation unique identifier of the device manufacturer. Represented as a six hexadecimal digit value, using all upper-case, and including any leading zeros. Returns the '0090F8' string.	
ModelName	Read-only	Passive
	Model name of the CPE. Returns the value of the Dcm.UnitInfoProductName parameter.	
Description	Read-only	Passive

Name	Access	Notification
	A full description of the CPE device. Returns the value of the concatenation (separated by spaces) of the following parameters: • Dcm.UnitInfoProductName. • Fpu.MfpInstalledInfo.MfpVersion (first row). • Fpu.MfpInstalledInfo.MfpProfileName (first row). This is the same value as the system description in SNMP.	
ProductClass	Read-only	Passive
	Identifies the class of product for which the serial number applies to. Returns the value of the Dcm.UnitInfoProductName parameter.	
SerialNumber	Read-only	Passive
	Serial number of the CPE. Returns the value of the Dcm.UnitInfoSerialNumber parameter.	
HardwareVersion	Read-only	Always Passive
	Identifies the particular CPE model and version. Returns the value of the concatenation (separated by a space) of the following parameters: • Dcm.UnitInfoProductName parameter. • Dcm.UnitInfoHardwareRevision parameter.	
SoftwareVersion	Read-only	Always Active
	Identifies the software version currently installed on the CPE. Returns the value of the Fpu.MfpInstalledInfo.MfpVersion parameter (first row).	
SpecVersion	Read-only	Passive

Name	Access	Notification
	Represents the version of the specification implemented by the device. Returns '1.0'.	
ProvisioningCode	Read/Write	Active
	Identifies the primary service provider and other provisioning information. Returns the last value set by the ACS. This value is saved in an internal database. The value is initially set to an empty string and also reset to an empty string on a factory default reset.	
UpTime	Read-only	Passive
	Time in seconds since the CPE was last restarted. Returns the system uptime in seconds. Uses the same time source as the SNMP and Web system uptime.	
VendorLogFileNumberOfEntries	Read-only	Passive
	Returns the number of entries of the DeviceInfo.VendorLogFile.{i} table.	
InternetGatewayDevice.DeviceInfo {i} .	Present	N/A
	Table of log files. This table is informational only and does not allow the ACS to operate on these files in any way. Returns the vendor log files table, each table entry represents a Vendor log file.	
Name	Read-only	None
	Returns the Vendor log file name.	
MaximumSize	Read-only	None
	The maximum size of the log file in bytes. When the maximum file size is not defined, the value is '0'.	
Persistent	Read-only	None
	When the value is 'true', the log file contents are preserved when the device is restarted. When the value is 'false', the log file contents are deleted when the device is restarted.	

Name	Access	Notification
InternetGatewayDevice.Management	Present	N/A
	This object contains parameters relating to the CPE's association with an ACS.	
URL	Read/Write	Passive
	URL used to connect the CPE to the ACS using the CPE WAN Management Protocol. This parameter supports only a valid HTTP or HTTPS URL. Returns the value of the AcsStaticUrl parameter if the value of the AcsUrlConfigSource parameter is set to 'Static'. Otherwise, returns an empty string. When receiving a SetParameterValues command: • If the value is empty, the value of the AcsStaticUrl parameter is set to empty and the value of the AcsUrlConfigSource parameter is set to 'Dhcp'. • When the value is not empty, the value of the AcsStaticUrl parameter is set to the new value and the AcsUrlConfigSource parameter is set to 'Static'.	
Username	Read/Write	Passive
	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is only used for HTTP-based authentication of the CPE. Returns and sets the value of the Username parameter.	
Password	Write	Passive
	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is only used for HTTP-based authentication of the CPE. Returns an empty string. Sets the value of the Password parameter.	
PeriodicInformEnable	Read/Write	Passive

Name	Access	Notification
	Whether or not the CPE must periodically send CPE information to the ACS by calling the Inform method. Returns and sets the value of the PeriodicInformEnable parameter.	
PeriodicInformInterval	Read/Write	Passive
	The duration in seconds of the interval for which the CPE will attempt to connect with the ACS and call the Inform method. Applicable only if the value of the PeriodicInformEnable parameter is 'Enable'. Returns and sets the value of the PeriodicInformInterval parameter.	
PeriodicInformTime	Read/Write	Passive
	An absolute time reference in UTC to determine when the CPE will initiate the Inform method. When the Inform method is called, it occurs at this reference time plus or minus an integer multiple of the PeriodicInformInterval parameter. The Unknown Time value indicates that no particular time reference is specified. That is, the unit locally chooses the time reference and only needs to follow the specified PeriodicInformInterval parameter. If absolute time is not available to the unit, its periodic Inform behavior is the same as if the PeriodicInformTime parameter was set to the Unknown Time value, i.e. '0001-01-01T00:00:00Z'. Returns and sets the value of the PeriodicInformTime parameter.	
ParameterKey	Read-only	Always
	Returns the last value set by the ACS in the last SetParameterValues, AddObject, or DeleteObject method call. This value is saved in an internal database. The value of the ParameterKey parameter is initially set to an empty string and reset to an empty string on a factory default reset.	
ConnectionRequestURL	Read-only	Always Active

Name	Access	Notification
	The HTTP URL used by the ACS to make a Connection Request notification to the CPE. Returns the 'http://[host]:[port]' value where: • host: The IP address of the management interface. If listening on all interfaces, the IP address of the interface used when contacting the ACS. • port: The value of the ListeningPort parameter.	
ConnectionRequestUsername	Read/Write	Active
	Username used to authenticate an ACS making a Connection Request to the CPE. Returns the value of the Cwmp.ConnectionRequestUsername parameter.	
ConnectionRequestPassword	Write	Passive
	Password used to authenticate an ACS making a Connection Request to the CPE. Returns an empty string. Sets the value of the Cwmp.ConnectionRequestPassword parameter.	
UpgradesManaged	Read/Write	Passive
	Indicates whether or not the ACS will manage upgrades for the CPE. The parameter is supported, but the functionality is not implemented. Returns the last value set by the ACS. This value is saved in an internal database. The value is initially set to 'false' and reset to 'false' on a factory default reset.	
UDPConnectionRequestAddress	Read-only	Active
	The public IP address and port of the unit to use for external UDP connection requests. This address is found in the STUN binding response.	
STUNEnable	Read/Write	Active

Name	Access	Notification
	Enables or disables the use of STUN by the CPE. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests. Returns the value of the Cwmp.Tr111StunEnable parameter.	
STUNServerAddress	Read/Write	Active
	Host name or IP address of the STUN server used by the CPE to send Binding Requests if STUN is enabled via the STUNEnable parameter. If the value of the STUNServerAddress parameter is empty and the value of the STUNEnable parameter is 'Enable', then the CPE uses the address of the ACS extracted from the host portion of the ACS URL. Otherwise, the value of the STUNServerAddress parameter is used by the CPE to send Binding Requests. Returns the address part of the Cwmp.Tr111StunServerHost parameter.	
STUNServerPort	Read/Write	Active
	Port number of the STUN server used by the CPE to send Binding Requests if STUN is enabled via the STUNEnable parameter. By default, this is 3478, i.e. the default STUN port. Returns the port part of the Cwmp.Tr111StunServerHost parameter.	
NATDetected	Read-only	Active
	When STUN is enabled, this parameter indicates whether or not the CPE has detected the address and/or the port mapping in use. A 'True' value indicates that the received MAPPED-ADDRESS in the most recent Binding Response differs from the CPE's source address and port. Returns 'True' if the value of the Cwmp.Tr111NatDetected parameter is set to 'yes'. Returns 'False' otherwise or when the STUN is disabled.	
STUNMinimumKeepAlivePeriod	Read/Write	Active

Name	Access	Notification
	Configures the first session retry wait interval, in seconds. If STUN is enabled, the minimum period, in seconds, during which the STUN Binding Requests may be sent by the CPE for the purpose of maintaining the STUN connection. Returns the minimal value of the Cwmp.Tr111StunKeepAlivePeriod parameter.	
STUNUsername	Read/Write	Active
	The value of the STUN USERNAME attribute to be used in Binding Requests when STUN is enabled. If the value of the STUNUsername parameter is empty, the CPE sends the STUN Binding Requests without the STUN USERNAME attribute. Returns and sets the value of the Cwmp.Tr111StunUsername parameter.	
InternetGatewayDevice.Time.	Present	N/A
	This object contains parameters relating to the NTP or SNTP time client on the CPE.	
NTPServer1	Read/Write	Active
	First NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=1].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=1].HostName parameter and sets the value of the Hoc.SntpConfigSource parameter to 'Static'.	
NTPServer2	Read/Write	Active
	Second NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=2].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=2].HostName parameter.	
NTPServer3	Read/Write	Active

Name	Access	Notification
	Third NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=3].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=3].HostName parameter.	
NTPServer4	Read/Write	Active
	Fourth NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=4].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=4].HostName parameter.	
CurrentLocalTime	Read-only	Passive
	The current date and time in the CPE's local time zone. Returns the value of the Hoc.SystemTime parameter	
InternetGatewayDevice.Services.	Present	N/A
Refer to the Services Parameters (p.494) table.		

14.6.3.3 Supported Parameters for the GatewayDevice Object

Note: Parameters not present are not supported.

Note: When Write parameters are read, an empty value is returned.

Note: The **Notification** column refers to the maximum level of notification allowed for the parameter. Unless stated otherwise, the parameter notifications are turned off by default.

Name	Access	Notification
Device.	Present	N/A
	The top-level object for a Device.	
DeviceSummary	Read-only	Always Passive
	Explicit summary of the top-level data model of the device, including version and profile information. Returns the 'Device:1.0[] (Baseline:1)' value.	
Device.DeviceInfo.	Present	N/A
Manufacturer	Read-only	Passive
	The manufacturer of the CPE. Returns the value of the HiddenManufacturer hidden parameter.	
ManufacturerOUI	Read-only	Passive
	Organisation unique identifier of the device manufacturer. Represented as a six hexadecimal digit value, using all upper-case, and including any leading zeros. Returns the '0090F8' string.	
ModelName	Read-only	Passive
	Model name of the CPE. Returns the value of the Dcm.UnitInfoProductName parameter.	
Description	Read-only	Passive
	A full description of the CPE device. Returns the value of the concatenation (separated by spaces) of the following parameters: • Dcm.UnitInfoProductName. • Fpu.MfpInstalledInfo.MfpVersion (first row). • Fpu.MfpInstalledInfo.MfpProfileName (first row). This is the same value as the system description in SNMP.	
ProductClass	Read-only	Passive

Name	Access	Notification
	Identifies the class of product for which the serial number applies to. Returns the value of the Dcm.UnitInfoProductName parameter.	
SerialNumber	Read-only	Passive
	Serial number of the CPE. Returns the value of the Dcm.UnitInfoSerialNumber parameter.	
HardwareVersion	Read-only	Always Passive
	Identifies the particular CPE model and version. Returns the value of the concatenation (separated by a space) of the following parameters: • Dcm.UnitInfoProductName parameter. • Dcm.UnitInfoHardwareRevision parameter.	
SoftwareVersion	Read-only	Always Active
	Identifies the software version currently installed on the CPE. Returns the value of the Fpu.MfpInstalledInfo.MfpVersion parameter (first row).	
DeviceStatus	Read-only	Passive
	Current operational status of the device. Returns the 'UP' string when the device is up.	
UpTime	Read-only	Passive
	Time in seconds since the CPE was last restarted. Returns the system uptime in seconds. Uses the same time source as the SNMP and Web system uptime.	
VendorLogFileNumberOfEntries	Read-only	Passive
	Returns the number of entries of the DeviceInfo.VendorLogFile.{i} table.	

Name	Access	Notification
Device.DeviceInfo.VendorLogFile. {}.	Present	N/A
	Table of log files. This table is informational only and does not allow the ACS to operate on these files in any way. Returns the vendor log files table, each table entry represents a Vendor log file.	
Name	Read-only	None
	Returns the Vendor log file name.	
MaximumSize	Read-only	None
	The maximum size of the log file in bytes. When the maximum file size is not defined, the value is '0'.	
Persistent	Read-only	None
	When the value is 'true', the log file contents are preserved when the device is restarted. When the value is 'false', the log file contents are deleted when the device is restarted.	
Device.GatewayInfo.⁵	Present	N/A
	This object contains information associated with a connected Internet Gateway Device.	
ManufacturerOUI	Read-only	Active
	Organizationally unique identifier of the associated Internet Gateway Device. An empty string indicates that there is no associated Internet Gateway Device that has been detected. Returns the GatewayManufacturerOui value received via the suboption 4 of the 'Vendor-Specific Information'. Returns an empty value if the contents of the suboption is not present or incorrect.	
ProductClass	Read-only	Active

⁵ The GatewayInfo object and all its parameters are only available if the TR-069 annex F option is enabled.

Name	Access	Notification
	Identifier of the product class of the associated Internet Gateway Device. An empty string indicates either that there is no associated Internet Gateway Device that has been detected, or the Internet Gateway Device does not support the use of the ProductClass parameter. Returns the GatewayProductClass value received via the suboption 6 of the 'Vendor-Specific Information'. Returns an empty value if the contents of the suboption is not present or incorrect.	
SerialNumber	Read-only	Active
	Serial number of the associated Internet Gateway Device. An empty string indicates that there is no associated Internet Gateway Device that has been detected. Returns the value of GatewaySerialNumber parameter received via the suboption 5 of the 'Vendor-Specific Information'. Returns an empty value if the contents of the suboption is not present or incorrect.	
Device.Time.	Present	N/A
	This object contains the parameters related to the NTP or SNTP time client on the CPE.	
NTPServer1	Read/Write	Active
	First NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=1].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=1].HostName parameter and sets the value of the Hoc.SntpConfigSource parameter to 'Static'.	
NTPServer2	Read/Write	Active
	Second NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=2].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=2].HostName parameter.	
NTPServer3	Read/Write	Active

Name	Access	Notification
	Third NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=3].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=3].HostName parameter.	
NTPServer4	Read/Write	Active
	Fourth NTP timeserver. Either a host name or IP address. Returns the value of the Hoc.SntpServersInfo[Priority=4].HostName parameter. Sets the value of the Hoc.StaticSntpServers[Priority=4].HostName parameter.	
CurrentLocalTime	Read-only	Passive
	The current date and time in the CPE's local time zone. Returns the value of the Hoc.SystemTime parameter.	
LocalTimeZone	Read/Write	Active
	The local time zone definition. Returns and sets the value of the Hoc.StaticTimeZone parameter.	
Device.LAN.	Present	N/A

Name	Access	Notification
	This object contains parameters related to the IP-based LAN connectivity of a device. Returns the informations of the network interface used by the device for connecting to the ACS. • The CPE uses the network interface configured in Cwmp.TR106LanNetworkInterface parameter if not empty. • Otherwise, the CPE uses the network interface configured in Cwmp.NetworkInterface parameter if not empty. • Otherwise, the CPE uses the network interface configured in Hoc.ManagementInterface parameter. • If the value of the Hoc.ManagementInterface parameter is set to 'All', use the network interface used for contacting the ACS.	
AddressingType	Read-only	Passive
	The method used to assign an address to this interface. Returns 'DHCP' if the value of the Bni.NetworkInterface.ConnectionType parameter is 'ipDhcp'. Returns 'Static' if the value of the Bni.NetworkInterface.ConnectionType parameter is 'ipStatic'. Returns an empty string if the Bni.NetworkInterface.ConnectionType parameter contains any other value.	
IPAddress	Read-only	Always Active

Name	Access	Notification
	The current IP address set on this interface. Returns the IP address from the Bni.NetworkInterfacesStatus.IpAddr parameter.	
SubnetMask	Read-only	Passive
	The current subnet mask set to this interface. Returns the IP address mask from the Bni.NetworkInterfacesStatus.IpAddr parameter.	
DefaultGateway	Read-only	Passive
	The IP address of the current default gateway for this interface. Returns the default gateway from the Hoc.DefaultRouterInfo parameter.	
DNSServers	Read-only	Passive
	List of DNS server IP addresses for this interface. Returns the list of DNS server IP addresses, separated by a coma, defined in the Hoc.DnsServersInfo parameter.	
MACAddress	Read-only	Always Active
	The physical address of this interface. Returns the value of the Dcm.unitInfoMacAddress parameter.	
Device.LAN.Stats.	Present	N/A
	This object contains statistics for the network interface used for connecting the device to the ACS.	
ConnectionUpTime	Read-only	Passive

Name	Access	Notification
	The time in seconds during which this network interface has been connected. - If the network interface is using DHCP, this is the time that the DHCP client has been only in the Bound or Renewing states and the lower-layer interface has continuously maintained a link. - If the network interface is using static addressing, this is the time that the lower-layer interface has continuously maintained a link. Returns the value of the Bni.NetworkInterfacesStatus.ConnectionUptime parameter.	
TotalBytesSent	Read-only	Passive
	Total number of IP payload bytes sent over this interface since the device was last restarted, as specified in the DeviceInfo.UpTime parameter. Returns the value of the Bni.InterfaceStatistics.TxBytes parameter.	
TotalBytesReceived	Read-only	Passive
	Total number of IP payload bytes received over this interface since the device was last restarted, as specified in the DeviceInfo.UpTime parameter. Returns the value of the Bni.InterfaceStatistics.RxBytes parameter.	
TotalPacketsSent	Read-only	Passive
	Total number of IP packets sent over this interface since the device was last restarted, as specified in the DeviceInfo.UpTime parameter. Returns the value of the Bni.InterfaceStatistics.TxPackets parameter.	
TotalPacketsReceived	Read-only	Passive

Name	Access	Notification
	Total number of IP packets received over this interface since the device was last restarted, as specified in the DeviceInfo.UpTime parameter. Returns the value of the Bni.InterfaceStatistics.RxPackets parameter.	
Device.ManagementServer.	Present	N/A
	This object contains parameters relating to the CPE's association with an ACS.	
URL	Read/Write	Passive
	URL used to connect the CPE to the ACS using the CPE WAN Management Protocol. This parameter supports only a valid HTTP or HTTPS URL. Returns the value of the AcsStaticUrl parameter if the value of the AcsUrlConfigSource parameter is set to 'Static'. Otherwise, returns an empty string. When receiving a SetParameterValues command: • If the value is empty, the value of the AcsStaticUrl parameter is set to empty and the value of the AcsUrlconfigSource parameter is set to 'Dhcp'. • When the value is not empty, the value of the AcsStaticUrl parameter is set to the new value and the AcsUrlConfigSource parameter is set to 'Static'.	
Username	Read/Write	Passive
	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is only used for HTTP-based authentication of the CPE. Returns and sets the value of the Username parameter.	
Password	Write	Passive

Name	Access	Notification
	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is only used for HTTP-based authentication of the CPE. Returns an empty string. Sets the value of the Password parameter.	
PeriodicInformEnable	Read/Write	Passive
	Whether or not the CPE must periodically send CPE information to the ACS by calling the Inform method. Returns and sets the value of the PeriodicInformEnable parameter.	
PeriodicInformInterval	Read/Write	Passive
	The duration in seconds of the interval for which the CPE will attempt to connect with the ACS and call the Inform method. Applicable only if the value of the PeriodicInformEnable parameter is 'Enable'. Returns and sets the value of the PeriodicInformInterval parameter.	
PeriodicInformTime	Read/Write	Passive
	An absolute time reference in UTC to determine when the CPE will initiate the Inform method. When the Inform method is called, it occurs at this reference time plus or minus an integer multiple of the PeriodicInformInterval parameter. The Unknown Time value indicates that no particular time reference is specified. That is, the unit locally chooses the time reference and only needs to follow the specified PeriodicInformInterval parameter. If absolute time is not available to the unit, its periodic Inform behavior is the same as if the PeriodicInformTime parameter was set to the Unknown Time value, i.e. '0001-01-01T00:00:00Z'. Returns and sets the value of the PeriodicInformTime parameter.	
ParameterKey	Read-only	Always

Name	Access	Notification
	Returns the last value set by the ACS in the last SetParameterValues, AddObject, or DeleteObject method call. This value is saved in an internal database. The value of the ParameterKey parameter is initially set to an empty string and reset to an empty string on a factory default reset.	
ConnectionRequestURL	Read-only	Always Active
	The HTTP URL used by the ACS to make a Connection Request notification to the CPE. Returns the 'http://[host]:[port]' value where: • host: The IP address of the management interface. If listening on all interfaces, the IP address of the interface used when contacting the ACS. • port: The value of the ListeningPort parameter.	
ConnectionRequestUsername	Read/Write	Active
	Username used to authenticate an ACS making a Connection Request to the CPE. Returns the value of the Cwmp.ConnectionRequestUsername parameter.	
ConnectionRequestPassword	Write	Passive
	Password used to authenticate an ACS making a Connection Request to the CPE. Returns an empty string. Sets the value of the Cwmp.ConnectionRequestPassword parameter.	
UpgradesManaged	Read/Write	Passive
	Indicates whether or not the ACS will manage upgrades for the CPE. The parameter is supported, but the functionality is not implemented. Returns the last value set by the ACS. This value is saved in an internal database. The value is initially set to 'false' and reset to 'false' on a factory default reset.	

Name	Access	Notification
UDPConnectionRequestAddress	Read-only	Active
	The public IP address and port of the unit to use for external UDP connection requests. This address is found in the STUN binding response.	
STUNEnable	Read/Write	Active
	Enables or disables the use of STUN by the CPE. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests. Returns the value of the Cwmp.Tr111StunEnable parameter.	
STUNServerAddress	Read/Write	Active
	Host name or IP address of the STUN server used by the CPE to send Binding Requests if STUN is enabled via the STUNEnable parameter. If the value of the STUNServerAddress parameter is empty and the value of the STUNEnable parameter is 'Enable', then the CPE uses the address of the ACS extracted from the host portion of the ACS URL. Otherwise, the value of the STUNServerAddress parameter is used by the CPE to send Binding Requests. Returns the address part of the Cwmp.Tr111StunServerHost parameter.	
STUNServerPort	Read/Write	Active
	Port number of the STUN server used by the CPE to send Binding Requests if STUN is enabled via the STUNEnable parameter. By default, this is 3478, i.e. the default STUN port. Returns the port part of the Cwmp.Tr111StunServerHost parameter.	
NATDetected	Read-only	Active

Name	Access	Notification
	When STUN is enabled, this parameter indicates whether or not the CPE has detected the address and/or the port mapping in use. A 'True' value indicates that the received MAPPED-ADDRESS in the most recent Binding Response differs from the CPE's source address and port. Returns 'True' if the value of the Cwmp.Tr111NatDetected parameter is set to 'yes'. Returns 'False' otherwise or when the STUN is disabled.	
STUNMinimumKeepAlivePeriod	Read/Write	Active
	Configures the first session retry wait interval, in seconds. If STUN is enabled, the minimum period, in seconds, during which the STUN Binding Requests may be sent by the CPE for the purpose of maintaining the STUN connection. Returns the minimal value of the Cwmp.Tr111StunKeepAlivePeriod parameter.	
STUNUsername	Read/Write	Active
	The value of the STUN USERNAME attribute to be used in Binding Requests when STUN is enabled. If the value of the STUNUsername parameter is empty, the CPE sends the STUN Binding Requests without the STUN USERNAME attribute. Returns and sets the value of the Cwmp.Tr111StunUsername parameter.	
Device.Services.	Present	N/A
Refer to the Services Parameters (p.494) table.		

14.6.3.4 Transport Layer Security (TLS) Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#). The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

For certificate transfert

- To set the HTTPS transfer cipher suite for certificate transfer: **Cert.TransferHttpsCipherSuite**
- To set the HTTPS transfer Tls Version for certificate transfer:: **Cert.TransferHttpsTlsVersion**
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

For file transfer

- To set the HTTPS transfer cipher suite for file transfer: **File.TransferHttpsCipherSuite**
- To set the HTTPS transfer Tls Version configuration for file transfer: **File.TransferHttpsTlsVersion**

For DGW Web access

- To set the Https Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**.
- To set the Http Mode used for DGW Web access: **Web.HttpMode**
- To select the Secure Server Port used to access the DGW Web interface: **Web.SecureServerPort**
- To set the HTTPS Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**
- To set the Tls Version used for secure DGW Web access: **Web.TlsVersion**

For SIP TLS transport

- To set the TLS transport cipher suite used for secure SIP transport: **SipEp.TransportTlsCipherSuite**
- To set Transport Tls Version used for secure SIP transport: **SipEp.TransportTlsVersion**
- To set TLS client authentication: **SipEp.InteropTlsClientAuthenticationEnable**

For TR-069 (CWMP) establishment

- To set the HTTPS transport cipher suite configuration for TR-069 (CWMP): **Cwmp.TransportHttpsCipherSuite**
- To set the HTTPS Transport Tls Version configuration for TR-069 (CWMP): **Cwmp.TransportHTTPSTlsVersion**
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

14.7 Access Control

14.7.1 Basic Access Control Concepts

14.7.1.1 Important Information

- The **Management/Access Control** page is only accessible if you have **admin** Access Rights.
- A maximum of 10 users can be added in the **Users** table.
- When a partial reset is triggered,
 - the default accounts are restored, with their default values and access rights.
 - the Radius authentication is disabled.
- The password is case sensitive. All characters are allowed.
- The username is case sensitive.
- The Mediatrix unit's Radius server settings do not support IPv6.

14.7.1.2 Access Right Permissions

Access Right	Observer	User	Admin
Read Configuration Parameters	√	√	√
Modify Configuration Parameters		√	√
Read/Write Passwords, Secrets, Secret Keys			√
Change Access Rights			√
Execute Configuration Scripts		√	√
Export Configuration		√	√
Backup/Restore Configuration			√
Firmware Updates and Rollback			√

14.7.1.3 Protection Against Brute Force Login Attempts

Mediatrix units have a protection against brute force login attempts.

When this protection is enabled, a user account is temporarily locked after repetitive login failures. The protection is enabled by default. The maximum number of login attempts before locking the user's account and the duration of the lock are configurable.

14.7.1.4 Service Access Control Type

It is possible to define the type of authentication and accounting to use for the CLI, SNMP, and Web services. In other words, it is possible to decide if authentication or accounting requests are sent to a RADIUS server or validated against the username and password stored locally in the **Users** table of DGW.

- Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted.
- Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session.

14.7.1.5 Radius Servers used For Authentication

A radius server can be used for Authentication for the CLI and the Web services

The first authentication attempt is sent to the Radius server with the highest priority. When authentication fails or the request reaches the timeout set in the **Server Request Timeout** field, the next server with the highest priority is used.

Note: As long as there are Radius servers available to try, they are tried, even if one of the servers has rejected authentication.

When all servers have failed to reply because the request has reached the timeout set in the **Server Request Timeout** field or when no servers are configured for the service asking for authentication, authentication is attempted against local user names and passwords as a fallback strategy.

Note: If one of the servers in the list of Radius servers rejects the authentication, the fallback strategy will not occur.

14.7.1.6 Radius Servers used For Accounting

A radius server can be used for Accounting Requests for the CLI, Snmp, and Web services

It is possible to use up to three Accounting Radius servers for each of the CLI, the Snmp, and Web services.

The first accounting attempt is sent to:

- the Priority #1 Radius server. If the accounting fails or the request reaches the timeout, the accounting request is sent to:
- the Priority #2 Radius server. If the accounting request fails or the request reaches the timeout, the accounting request is sent to:
- Priority #3 Radius server. If the accounting request fails or the request reaches the timeout, the accounting request is dropped.

14.7.1.7 Advanced Access Control Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on advanced parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- To set the maximum login attempts allowed before locking the account: **Aaa.LoginLockedMaxRetry**
- To set how much time the account will remain locked: **Aaa.LoginLockedTimeout**

14.7.2 Basic Access Control Tasks

14.7.2.1 Adding a User to DGW

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, complete the **User Name** and **Password** fields.

Note: The user name is case sensitive.

Note: Passwords are not exported to a configuration script, unless the user has admin access rights

- 3) Click 
- 4) From the **Access Rights** selection list, choose the appropriate rights.
- 5) From the **Lock Protection**, enable de protection, if required.

6) Click **Apply**.

Result

Users					
User Name	Password	Access Rights	Lock Protection		
NewUser	*****	Observer ▾	Enable ▾	—	
admin	*****	Admin ▾	Enable ▾	—	
public	*****	Admin ▾	Enable ▾	—	
				+	

14.7.2.2 Changing the Rights of a DGW User

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, from the **Access Rights** selection list, choose the appropriate rights.
- 3) Click **Apply**.

Result

The user will have the selected DGW access rights.

14.7.2.3 Changing the Login Password

Before you start

You must have administrator rights.

Information

For security reasons, it is a best practice to change the Default Login Password.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, enter a new password for the user.

Note: The password is case sensitive. All characters are allowed.

- 3) Click **Apply**.

14.7.2.4 Deleting a User from DGW

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, click  next to the user to delete.

Note: If all users are deleted from the **Users** table, the profile's default user(s) will be used upon unit restart.

- 3) Click **Apply**.
- 4) Click **Reboot**.

Result

The current activities of the deleted user are terminated only once the system has been restarted.

Users					
User Name	Password	Access Rights	Lock Protection		
admin	*****	Admin ▾	Enable ▾		
public	*****	Admin ▾	Enable ▾		
NewUser	(Deleted on next reboot)				
					

14.7.2.5 Protecting User Accounts Against Brute Force Attacks

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, from the **Lock Protection** selection list, choose **Enable**.

Note: For more details, refer to [Protection Against Brute Force Login Attempts](#) (p.544) and the [Advanced Access Control Parameters](#) (p.545) parameters.

- 3) Click **Apply**.

14.7.2.6 Setting the Access Control Type of the CLI Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Authentication Type** selection list, choose the appropriate type of authentication.
- 3) From the **Accounting Type** selection list, choose the appropriate type of Accounting.
- 4) If you chose to use Radius servers for authentication and/or accounting, from the **Select a Service** selection list, choose CLI.
- 5) In the **CLI Radius Server** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default, many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 6) Click **Apply**.

Result

For example:

Services Access Control Type			
Service	Authentication Type	Accounting Type	
Cli	Radius ▾	Radius ▾	
Snmp	Local ▾	Radius ▾	
Web	Radius ▾	Radius ▾	

Select a Service: Cli ▾

Cli Radius Servers			
	Priority #1	Priority #2	Priority #3
Authentication			
Host:	hostname1:port	hostname2:1812	hostname3:1645
Server Secret:			
Accounting			
Host:	hostname1:port	hostname2:181	hostname3:1646
Server Secret:			
General (Applied to all services)			
Server Request Timeout (s)	5		
Radius Users Access Rights	Admin ▾		

14.7.2.7 Setting the Access Control Type of the Snmp Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Accounting Type** selection list, choose the appropriate type of Accounting.

Note: The use of a Radius server for Authentication is not allowed for the Snmp Service

- 3) If you chose to use Radius servers for accounting, from the **Select a Service** selection list, choose **SNMP min**.
- 4) In the **SNMP Radius Servers** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default, many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 5) Click **Apply**.

Result

For example:

Services Access Control Type		
Service	Authentication Type	Accounting Type
Cli	Radius ▾	Radius ▾
Snmp	Local ▾	Radius ▾
Web	Radius ▾	Radius ▾

Select a Service: Snmp ▾

Snmp Radius Servers			
	Priority #1	Priority #2	Priority #3
Authentication			
Host:			
Server Secret:			
Accounting			
Host:	hostname1:port	hostname2:1813	hostname3:1646
Server Secret:			
General (Applied to all services)			
Server Request Timeout (s)	5		
Radius Users Access Rights	Admin ▾		

14.7.2.8 Setting the Access Control Type of the Web Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Authentication Type** selection list, choose the appropriate type of authentication.
- 3) From the **Accounting Type** selection list, choose the appropriate type of Accounting.
- 4) If you chose to use Radius servers for authentication and/or accounting, from the **Select a Service** selection list, choose **Web**.
- 5) In the **Web Radius Servers** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default , many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 6) Click **Apply**.

Result

For example:

Services Access Control Type			
Service	Authentication Type	Accounting Type	
Cli	Radius ▾	Radius ▾	
Snmp	Local ▾	Radius ▾	
Web	Radius ▾	Radius ▾	

Select a Service: Web ▾

Web Radius Servers			
	Priority #1	Priority #2	Priority #3
Authentication			
Host:	hostname1:port	hostname2:1812	hostname3:1645
Server Secret:			
Accounting			
Host:	hostname1:port	hostname2:1813	hostname3:1646
Server Secret:			
General (Applied to all services)			
Server Request Timeout (s)	5		
Radius Users Access Rights	Admin ▾		

14.8 File

14.8.1 File Basic Concepts

14.8.1.1 File Manager

The DGW file manager allows for the importation of data files used by DGW.

When a DGW Mediatrix unit is purchased, several preset files are already present in the **Internal files** table (**Management/File**). these can be the default rulesets, a configuration script, etc.

However, it is possible to import and export files (for example to import the configuration scripts that are applied on similar units).

Note: The file manager is not available on the Mediatrix 4102S

The file manager system supports the importation and exportation of the following types of files:

Path	Type of File	Platforms
moh/	MP3 files for Music On Hold (MOH)	All except the Mediatrix 4102S
conf/	Configuration scripts and backup files	All except the Mediatrix 4102S
sbc/rulesets/	Session Border Controller rulesets	Sentinel 100 and 400
vm/drives/	Virtual Machine images	Sentinel 400
vm/images/	Bootable ISO images	Sentinel 400

The file manager system supports the exportation only of the following types of files:

Path	Type of File	Platforms
nlm/diag	Log files generated by System/Diagnostic (Nlm service)	All except the Mediatrix 4102S
nlm/logs	Notification files generated by System/Event Log (Nlm service)	All except the Mediatrix 4102S and Mediatrix C7 Series
nlm/pcaptures	Network capture files generated by System/ Packet Capture (Nlm service)	All except the Mediatrix 4102S
sbc/logs	SIP/RTP traffic logged by the Log received traffic action in Call Agent Rulesets (Sbc service)	Sentinel 100 and 400

It is possible to import a file either by using an URL or through a Web browser.

Note: Media5 strongly recommends to use an HTTPS access.

14.8.1.2 Large Files - Important Information

Remember, when importing a very large file:

- Closing the unit Web page will stop the transfer.
- Web Browsers do not always display a progress indicator, be cautious not to accidentally abort the file transfer.
- Transfer speed depends on connection speed, therefore transfer can take several minutes.
- Free disk space in computer must be at least equivalent to the size of the imported file.
- Anti-virus programs sometimes abort large file transfers; consider closing it.

14.8.2 File Basic Tasks

14.8.2.1 Importing an ISO image to the Unit File Management System

Information

If the ISO Image is larger than 10mb, use the [Importing an ISO Image Larger than 10mb to the Unit File Management System](#) (p.553).

Steps

- 1) Go to **Management/File**.
- 2) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser** located at the top of the page.
- 3) In the **Import File Through Web Browser** table, from the **Path** selection list, select **vm/drives/**.
- 4) Browse to the location of the ISO file containing the operating system (OS) to install on the virtual machine.
- 5) Click **Import**.

Note: A factory reset will remove the file from the **Internal filestable**.

Result

The imported ISO file will appear in the **VM Files** table, under **Management/File**.

Import File Through Web Browser	
Path	File
vm/drives/	Browse... yymmdd_OS.iso Import

14.8.2.2 Importing an ISO Image Larger than 10mb to the Unit File Management System

Before you start

Only the http and https protocols are supported to import the large files.

Steps

- 1) Go to **Management/File**.
- 2) In the **Import File Through URL** table, from the **Destination** selection list, select the destination directory on the unit where to save the file.
- 3) In the **URL** field, indicate the file server's URL where the iso image to import is located.

Note: For larger files you must use the http or https protocols. For example <http://www.myserver.com/myfile>

- 4) Complete the **User Name** and **Password** fields if the file server requires authentication.
- 5) Click **Import**.

Result

The ISO image file will be displayed in the **VM Files** table, under **Management/File**.

Import File Through URL	
Last Import File Result:	None
Import File Parameters Import	
Destination:	Choose directory
URL:	http://www.myserver.com/ myfile
Username:	username
Password:	

14.8.2.3 Deleting a File from DGW

Before you start

This option is not available on the Mediatrix 4102S.

Steps

- 1) In the Web interface of DGW, go to **Management/File**.
- 2) Click  located on the same line of the file you wish to remove.
- 3) Click **OK**.
- 4) A message will be displayed asking: **Are you sure you want to delete this file?**, click **OK**.

Result

The file will no longer appear in the table.

Internal files		
Name	Description	Size
conf/conf_and_certs.txt	Automatically generated on 25/05/2018 10:58:34.	136 KB 
conf/Gateway_Configuration.cfg	Configures the Sentinel with Gateway-style default settings.	10 KB 
conf/PRI_China-DSS1.cfg	China DSS1	3 KB 
conf/PRI_Default.cfg	PRI default configuration	3 KB 
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB 
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB 
conf/Survivability.cfg	Configures the DGW unit to use the SipProxy service for	1 KB 
nlm/diag/logs_0090f80b0848_2018-04-05_115327.tgz	Mon Jan 28 08:18:17 2019	10 KB 
8 file(s)		Total: 169 KB / Available: 26.4 GB

VM files		
Name	Description	Size
vm/images/test.cfg	Virtual Machine configuration file	1 KB 
vm/images/test.img	Virtual Machine image file	192 KB 
2 file(s)		Total: 193 KB / Available: 52.9 GB

14.8.2.4 Importing an MP3 File from a Web Browser

Steps

- 1) Go to **Management/File**.
- 2) Click **Activate unsecure file importation from the Web browser**, located at the top of the page .
- 3) In the **Import File Through Web Browser** table, from the **Path** drop-down list, select **moh/**.
- 4) Select the MP3 file.
- 5) Click **Import**.
- 6) Validate that the MP3 file appears in the **Internal files** table.
- 7) Go to **Telephony/Music on Hold**.
- 8) From the **Transfer Configuration** table, enter the URL of the MP3 file to use in the URL field.

Note: For example: file:///myfile.mp3.

- 9) Leave the **User Name**, **Password** and **Reload Interval** fields empty.
- 10) Click **Apply & Transfer Now**.

14.8.2.5 Importing a Virtual Machine Image to the Unit File Management System

Steps

- 1) Go to **Management/File**.

- 2) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser** located at the top of the page.
- 3) In the **Import File Through Web Browser** table, from the **Path** selection list, select **vm/images/**.
- 4) Browse to the location of the file containing the virtual machine image to install on the unit.
- 5) Click **Import**.

Note: A factory reset will not remove the vm files from the **Internal file** table.

Result

The imported image file will appear in the **Internal files** table, under **Management/File**.

14.8.2.6 Downloading a Local Capture File From the Mediatrix Unit to Your PC

Steps

- 1) Go to **Management/File**.
- 2) In the **Internal files** table, click the name of the file you have given to your capture.
- 3) Save your capture file.

Result

The capture will be saved at the chosen location.

14.9 Misc

14.9.1 Disabling the Rescue Interface

Information

By default the Rescue interface is disabled. However, after a partial reset the rescue interface is enabled.

IMPORTANT: The Rescue interface is bound to the unit's WAN port (wan for the Mediatrix 4102S, and ETH1 for all other Mediatrix units). The IP address of the Rescue interface is 192.168.0.1 (IPv4) or an IPv6 Link Local address.

Steps

- 1) Go to **Management/Misc**.

- 2) From the **Network Interface** drop-down menu, select the interface that will be used to manage the unit.

IMPORTANT: If you keep the **Rescue Interface** selected, you will not be able to get into the management interface after disabling it.

- 3) Click **Apply**
- 4) Go to **Network/Interfaces**.
- 5) In the **Rescue Interface** table, from the **Activation** selection list, select **Disable**.
- 6) Click **Apply**.

IMPORTANT: Make sure to reconfigure at least the user's authentication and firewall rules (if applicable), otherwise it may leave the unit unsecure.

Result

The unit will be reachable either on the new configured static IP address or on the DHCP .

Rescue Network Configuration			
Family	Link	IP Address	Activation
IP version 4	eth1	192.168.0.1/24	Disable ▼
IP version 6	All	fe80::0290:f8ff:fe09:b3db	

15 Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

16 Acronyms

3G

3rd Generation cellular data network

4G

4th Generation cellular data network

A

Aaa

Authentication, Authorization and Accounting

AC

Access Concentrator

ACS

Auto Configuration Server

ADSL

Asymmetric Digital Subscriber Line

AES

Advanced Encryption Standard

AGC

Automatic Gain Control

ANI

Automatic Number Identification

AOC-E

Advice of Charge End-of-Call

B

BER

Basic Encoding Rules

Bni

Basic Network Interfaces

BRI

Basic Rate Interface

C

CA

Certification Authority

CAS

Channel Associated Signalling

CC

Country Code

[CCBS](#)

Completion of Call to Subscriber

[CCNR](#)

Completion of Calls on No Reply

[Cdr](#)

Call Detail Record

[CDR](#)

Call Detail Record

[Cert](#)

Certificate Manager

[CHAP](#)

Challenge Handshake Authentication

[Cli](#)

Command Line Interface

[CLIP](#)

Calling Line Information Presentation

[CLIR](#)

Calling Line Information Restriction

[CNG](#)

Comfort Noise Generator

[CNIP](#)

Calling Name Identity Presentation

[COLP](#)

Connected Line Identification Presentation

[COLR](#)

Connected Line Identification Restriction

[Conf](#)

Configuration Manager

[CRout](#)

Call Routing

[CS-ACELP](#)

Conjugate Structure-Algebraic Excited Linear Prediction

[Cwmp](#)

CPE Wan Management Protocol

D

[Dcm](#)

Device Control Manager

[DER](#)

Distinguished Encoding Rules

[Dhcp](#)

Dynamic Host Configuration Protocol Server

[DHCP](#)

Dynamic Host Configuration Protocol

[Dhcp](#)

Dynamic Host Configuration Protocol

[DNIS](#)

Dialed Number Identification Service

[DNS](#)

Domain Name Server

[DSCP](#)

Differentiated Services Code Point

[DSL](#)

Digital Subscriber Lines

[DSS1](#)

Digital Subscriber Signalling System No.1

[DST](#)

Daylight Saving Time

[DTMF](#)

Dual Tone Multi-Frequency

E

[E1](#)

European PRI digital signal carrier. 32 channels (30 voice channels + synchronization and signaling)

[Eam](#)

E and M Channel Associated Signaling

[EMS](#)

Element Management System

[EpAdm](#)

Endpoint Administration

[EpServ](#)

Endpoint Services

[ETH](#)

Ethernet Manager

F

FCC

Federal Communication Commission

FILE

File Manager

Fpu

Firmware Pack Updater

FQDN

Fully Qualified Domain Name

FSK

Frequency Shift Keying

FXO

Foreign Exchange Office

FXS

Foreign Exchange Service/Station

G

GMT

Greenwich Mean Time

H

HDSL

High-bit-rate Digital Subscriber Line

Hoc

Host Configuration

HTML

Hyper Text Markup Language

HTTP

Hyper Text Transfer Protocol

HTTPS

HTTP over the Transport Layer Security

Hz

Hertz

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IETF

Internet Engineering Task Force

IMS

IP Multimedia Core Network Subsystem

IP

Internet Protocol

IP PBX

Internet Protocol Private Branch eXchange

IpRouting

IP routing

IpSync

IP Synchronisation

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

ISDN

Integrated Services Digital Network

Isdn

Integrated Services Digital Network

ITC

Information Transfer Capability

ITSP

Internet Service Provider

ITU

International Telecommunication Union

K

kbps

KiloBits Per Second

L

LAN

Local Area Network

LED

Light Emitting Diode

Lfw

Local Firewall

LNP

Local Number Portability

LLPD-MED

Link Layer Discovery Protocol-Media Endpoint Discovery

[LLPD](#)

Link Layer Discovery Protocol

[Lldp](#)

Link Layer Discovery Protocol

[LQos](#)

Local Quality of Service

[M](#)

[MAC](#)

Media Access Control

[MFC](#)

Multi-Frequency Code

[MIB](#)

Management Information Base

[MIKEY](#)

Multimedia Internet KEYing

[Mipt](#)

Media IP Transport

[Moh](#)

Music on Hold

[MSN](#)

Multiple Subscriber Number

[MTU](#)

Maximum Transmission Unit

[MWI](#)

Message Waiting Indicator

[N](#)

[NT](#)

Network Termination. The endpoint on the telephone switch side.

[NAT](#)

Network Address Translation

[Nat](#)

Network Address Translation

[Nfw](#)

Network Firewall

[Nlm](#)

Notifications and Logging Manager

[Ntc](#)

Network Traffic Control

[NTP](#)

Network Time Protocol

O

[OCSP](#)

Online Certificate Status Protocol

P

[PAP](#)

Password Authentication Protocol

[PBX](#)

Private Branch eXchange

[PCM](#)

Pulse Code Modulation

[Pcm](#)

Process Control Manager

[PEM](#)

Privacy Enhanced Mail

[PI](#)

Presentation Indicator

[PISN](#)

Private Integrated Services Network

[POSIX](#)

Portable Operating System Interface

[POTS](#)

Plain Old Telephony System

[Pots](#)

Plain Old Telephony System Line

[PPP](#)

Point-to-Point Protocol

[PPPoE](#)

Point-to-Point Protocol over Ethernet

[PRACK](#)

Provisional Response Acknowledgement

[PRI](#)

Primary Rate Interface

[PSTN](#)

Public Switched Telephony Network

Q

[QoS](#)

Quality of Service

R

[R2](#)

R2 Channel Associated Signaling

[Radius](#)

Remote Authentication Dial-In User Service

[RADSL](#)

Rate-adaptive Digital Subscriber Line

[RFC](#)

Request For Comment

[RTCP](#)

Realtime Control Protocol

[RTP](#)

Real Time Transport Protocol

S

[Sbc](#)

Session Border Controller

[SBC](#)

Session Border Controller

[Scm](#)

Service Controller Manager

[SCN](#)

Switched Circuit Network

[SDES](#)

Secure Description

[SDP](#)

Session Description Protocol

[SHA](#)

Secure Hash Algorithm

[SI](#)

Screening Indicator

[SIP](#)

Session Initiation Protocol

[SipEp](#)

SIP Endpoint

[SLA](#)

Service Level Agreement

[SNMP](#)

Simple Network Management Protocol

[Snmp](#)

Simple Network Management Protocol

[SNTP](#)

Simple Network Time Protocol

[SRTCP](#)

Secure Real-Time Transport Control Protocol

[SRTP](#)

Secure Real-Time Transport Protocol

[SSH](#)

Secure Socket Shell

[SSL](#)

Secure Socket Layer

[STD](#)

Standard Saving Time

[STP](#)

Spanning Tree Protocol

T

[TBRL](#)

Terminal Balance Return Loss

[TCP](#)

Transmission Control Protocol

[TCP/IP](#)

Transmission Control Protocol/Internet Protocol

[TDM](#)

Time-division multiplexing

[TE](#)

Terminal Equipment, the endpoint on the customer side

[TEI](#)

Terminal Endpoint Identifier

[TelIf](#)

Telephony Interface

[TFTP](#)

Trivial File Transfer Protocol

[TLS](#)

Transport Layer Security

[TON](#)

Type of Number

U

[UDP](#)

User Datagram Protocol

[UMN](#)

Unit Manager Network

[UNI](#)

User-Network Interface

[URI](#)

Uniform Resource Identifier

[UTC](#)

Universal Time Coordinated

V

[VAD](#)

Voice Activity Detector

[VLAN](#)

Virtual Local Area Network

[VoIP](#)

Voice Over IP

[VPN](#)

Virtual Private Network

W

[WAN](#)

Wide Area Network

[Wi-Fi](#)

Wireless IEEE802.11 a, b or g network

[Web](#)

Web

[WLAN](#)

Wireless Local Area Network

[WINS](#)

Windows Internet Name Service

17 Glossary

3G

3rd Generation cellular data network. A technology used for mobile devices and mobile telecommunications use services and networks. It is based on a set of standards that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.

4G

4th Generation cellular data network. A technology used for mobile devices and mobile telecommunications use services and networks. It is based on a set of standards that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.

10 Base T

An Ethernet local area network that works on twisted pair wiring. 10 indicates the transmission speed of 10 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

100 Base T

A version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet. 100 indicates the transmission speed of 100 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

1000 Base T

A version of Ethernet that operates at 10 times the speed of a 100 BaseT Ethernet. 1000 indicates the transmission speed of 1,000 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

A

Authentication, Authorization and Accounting (AAA)

System service that authenticates a user and grants rights to perform specific tasks on the system.

Access Device

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

Accounting

Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilisation, and capacity planning activities.

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 μ -law standard. See also [mu \(\$\mu\$ \)-law](#).

ANI (Automatic Number Identification)

In Channel Associated Signaling, the sending of the calling numbers is known as Automatic Number Identification.

AOC

In ISDN signaling, an Advice Of Charge (AOC-D) message is sent to advise of the current charge (D)uring a call or an AOC-E message is sent to advise of the total charge at the (E)nd of a call.

Area Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line.

Authentication

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials do not match, authentication fails and network access is denied.

B

Basic Rate Interface

Basic Rate Interface or Basic Rate Access is an Integrated Services Digital Network (ISDN) configuration defined in the physical layer standard I.430 produced by the ITU. This configuration consists of two 64 kbit/s “bearer” channels (B channels) and one 16 kbit/s “data” channel (D channel). The B channels are used for voice or user data, and the D channel is used for any combination of: data, control/signalling and X.25 packet networking. The two B channels can be bonded together giving a total data rate of 128 kbit/s. BRI is the kind of ISDN interface most likely to be found in a residential service.

Basic Network Interfaces (Bni)

User service managing the layer 3 network interfaces.

C

Call Detail Record (Cdr)

User service allowing the administrator to generate custom call notifications with information such as endpoints, point of origin, duration, etc.

Call Routing

Calls through the unit can be routed based on a set of routing criteria.

Call Routing (CRout)

User service manipulating properties and routing calls between the telephony interfaces and the SIP endpoints.

Certificate Management (Cert)

System service that manages the security certificates used for the authentication of the unit and its peers before establishing a secure connection.

Channel Associated Signaling (CAS)

With this method of signaling, each traffic channel has a dedicated signaling channel. In other words the signaling for a particular traffic circuit is permanently associated with that circuit. Channel-

associated call control is still widely used today mostly in South America, Africa, Australia and in Europe.

Command Line Interface (Cli)

User service allowing the administrator to manage the unit using the SSH or TELNET protocols.

Configuration Manager (Conf)

System service executing configuration scripts as well as performing backup/restore of the unit's configuration.

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.

CPE WAN Management Protocol (Cwmp)

User service allowing the administrator to manage the unit using the TR-069 protocol.

D

Device Control Manager (Dcm)

System service managing the auto-detection and identification of unit hardware components as well as the licence activation keys.

Dynamic Host Configuration Protocol Server (Dhcp)

User service managing a DHCP server on each network interface.

Dialed Number Identification Service (DNIS)

DNIS is a telephone service that identifies for the receiver of a call the number that the caller dialed. It's a common feature of 800 and 900 lines. If you have multiple 800 or 900 numbers to the same destination, DNIS tells which number was called. DNIS works by passing the touch tone digits (dual tone multi frequency or MF digits) to the destination where a special facility can read and display them or make them available for call center programming.

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.

Distinguished Encoding Rules (DER)

DER for ASN.1, as defined in ITU-T Recommendation X.509, is a more restrictive encoding standard than the alternative BER (Basic Encoding Rules) for ASN.1, as defined in ITU-T Recommendation X.209, upon which DER is based. Both BER and DER provide a platform-independent method of encoding objects such as certificates and messages for transmission between devices and applications

Domain Name Server (DNS)

Internet service that translates domain names into IP addresses. 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 signaling 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.

[E](#)

[E1](#)

European PRI digital signal carrier. 32 channels (30 voice channels + synchronization and signaling).

[Echo Cancellation](#)

Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.

[E and M Channel Associated Signaling \(Eam\)](#)

Service managing the E and M CAS telephony interfaces.

[Endpoint Administration \(EpAdm\)](#)

User service allowing for high-level management of telephony endpoints.

[Endpoint Services \(EpServ\)](#)

User service managing the telephony services of each endpoint.

[Ethernet Manager \(Eth\)](#)

System service managing the unit's Ethernet link interfaces.

[F](#)

[Failback](#)

The restoration of the original state of a system after failing.

[Failover](#)

An automatic switch to a secondary system on failure of the primary system, used to insure the availability of critical resources, involving a parallel backup system running at all times so that, upon the detection of primary system failure, processing is automatically shifted to the backup.

[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 clear down 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.

[File Manager \(File\)](#)

System service allowing the administrator to manage the files stored on the unit.

[Firewall](#)

A firewall in a networked environment blocks some communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust).

[Foreign Exchange Office \(FXO\)](#)

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 office end of an FX circuit (frequently a PBX).

[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.

[Firmware Pack Updater \(Fpu\)](#)

System service managing firmware upgrade, downgrade and rollback operations.

[Full-Duplex Connection](#)

Refers to a transmission using two separate channels for transmission and reception and that can transmit in both ways at the same time. See also [Half Duplex Connection](#) .

G

[G.703](#)

ITU-T recommendation for the physical and electrical characteristics of hierarchical digital interfaces at rates up to 140Mbit/s.

[G.704](#)

ITU-T recommendation for synchronous frame structures on G.703 interfaces up to 45Mbit/s. The conventional use of G.704 on a 2Mbit/s primary rate circuit provides 30 discrete 64kbit/s channels, with a further 64kbit/s channel available for common channel signaling

[G.711](#)

Algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48 kbps, 56 kbps, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

[G.723.1](#)

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

[G.726](#)

An implementation of ITU-T G.726 standard for conversion linear or A-law or μ -law PCM to and from a 40, 32, 24 or 16 kbit/s channel.

[G.729](#)

A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).

[Gateway](#)

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

H

[Half-Duplex Connection](#)

Refers to a transmission using the same channel for both transmission and reception therefore it can't transmit and receive at the same time. See also [Full Duplex Connection](#).

Host Configuration (Hoc)

System service managing the IP host parameters and other system settings.

Hunt Group

The hunt group hunts an incoming call to multiple interfaces. It accepts a call routed to it by a routing table or directly from an interface and creates another call that is offered to one of the configured destination interfaces. If this destination cannot be reached, the hunt group tries another destination until one of the configured destinations accepts the call. When an interface accepts a call, the interface hunting is complete and the hunt group service merges the original call with the new call to the interface that accepted the call.

I

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.

Information Transfer Capability (ITC)

A request to the network exchange equipment to ask if a particular type of encoding is allowed. It is also called ISDN bearer capability or ISDN service.

Integrated Services Digital Network (ISDN)

A set of digital transmission protocols defined by the international standards body for telecommunications, the ITU-T (formerly called the CCITT). These protocols are accepted as standards by virtually every telecommunications carrier all over the world. ISDN complements the traditional telephone system so that a single pair of telephone wires is capable of carrying voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form.

Integrated Services Digital Network (Isdn)

User service managing the ISDN parameters for BRI and PRI telephony interfaces.

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.

IP Forwarding

Allows the packet to be forwarded to a specific network based on the packet's criteria (source IP address and source Ethernet link).

IP Routing (IpRouting)

User service managing the unit's IP routing table.

IP Synchronisation (IpSync)

User service controlling the IP media synchronization using clock reference signals sent over IP.

[Internet Protocol version 4 \(IPv4\)](#)

IPv4 (Internet Protocol version 4) is a 32-bit address internet protocol.

[Internet Protocol version 6 \(IPv6\)](#)

IPv6 (Internet Protocol version 6) is the successor to the common Internet Protocol (IPv4). IPv6's is a 128-bit address Internet protocol.

J

[Jitter](#)

A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

L

[Light Emitting Diode \(LED\)](#)

A semiconductor diode that emits light when a current is passed through it.

[Link Layer Discovery Protocol \(Lldp\)](#)

User service managing the IEEE 802.1ab protocol used for advertising the unit's capabilities on the network.

[Local Area Network \(LAN\)](#)

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also [WAN](#) .

[Local Firewall](#)

Allows you to dynamically create and configure rules to filter incoming packets with the unit as destination. The traffic is analysed and filtered by all the configured rules.

[Local Firewall \(Lfw\)](#)

User service allowing the administrator to filter incoming packets with the unit as final destination.

[Local Quality Of Service \(LQos\)](#)

System service managing the QOS parameters applicable to the unit.

M

[Management Information Base \(MIB\)](#)

Specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

[Media Access Control \(MAC\) Address](#)

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

[Media Interface](#)

The Media Interface is used for media (RTP, UDPTL) processing.

[Media IP Transport \(Mipt\)](#)

User service managing the voice and data encodings over the IP network.

[Mu \(μ\)-Law](#)

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also [A-Law](#).

[Music on Hold \(MoH\)](#)

User service managing the option to play an audio file when a telephony endpoint is on hold.

N

[Network](#)

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

[Network Address Translation \(NAT\)](#)

NAT, also known as network masquerading or IP masquerading, rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. There are two types of NAT rules:

- Source rules: They are applied on the source address of outgoing packets.
- Destination rules: They are applied on the destination address of incoming packets.

[Network Address Translation \(Nat\)](#)

User service allowing the administrator to change the source or the destination IP address of a packet.

[Network Firewall](#)

Allows dynamically creating and configuring rules to filter packets forwarded by the unit. Since this is a network firewall, rules only apply to packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured.

[Network Firewall \(Nfw\)](#)

User service allowing the administrator to filter traffic that is routed between networks.

[Network Traffic Control \(Ntc\)](#)

User service allowing the administrator to perform traffic shaping on the network interfaces.

[Notification and Logging Manager \(Nlm\)](#)

User service managing the routing and filtering of the unit's event notification messages.

O

[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.

P

[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.

Plain Old Telephone System Line (Pots)

User service managing the FXS and FXO analog telephony interfaces.

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 Dial up 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.

Primary Rate Interface (PRI)

A telecommunications standard for carrying multiple DS0 voice and data transmissions between two physical locations. All data and voice channels are (ISDN) and operate at 64 kbit/s. North America and Japan use a T1 of 23 B channels and one D channel which corresponds to a T1 line. Europe, Australia and most of the rest of the world use the slightly higher capacity E1, which is composed of 31 B channels and one D channel. Fewer active B channels (also called user channels) can be used for a fractional T1. More channels can be used with more T1's, or with a fractional or full T3 or E3.

Presentation Indicator (PI)

An information element (IE) field that determines whether a caller's CLI can be displayed on a Caller ID device or otherwise presented to the called party.

Private Branch Exchange (PBX)

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Process Control Manager (PCM)

System service managing the start-up and shutdown sequences of the system.

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.

Q

QSIG

QSIG is an ISDN based signaling protocol for signaling between private branch exchanges (PBXs) in a Private Integrated Services Network (PISN). It makes use of the connection-level Q.931 protocol and the application level ROSE protocol. ISDN "proper" functions as the physical link layer.

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).

R

R2 Channel Associated Signaling (R2)

User service managing the E1 CAS telephony interfaces.

Real Time Control Protocol (RTCP)

RTCP is the control protocol designed to work in conjunction with RTP. It is standardised 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 real-time 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 formal document from the IETF that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

S

SBC Session

An SBC session is a SIP call established between two endpoints not including the SBC. A session usually has 2 call legs, one incoming and one outgoing of the SBC.

Screening Indicator (SI)

A service provided by ISDN that can be used to test the trustworthiness of the calling party's number. This signalling-related information element is found in octet 3a of the ISDN SETUP message.

Service Controller Manager (Scm)

System service allowing the administrator to enable or disable services.

Session Border Controller (Sbc)

User service allowing the administrator to perform SIP to SIP normalization, call routing, NAT traversal and survivability.

Session Border Controller (SBC)

A Session Border Controller used in Voice over Internet Protocol (VoIP) networks to control the signaling and media streams involved in establishing, conducting and analysing telephone calls or other interactive media communications.

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.

Signaling Interface

The Signaling Interface is used for SIP signaling.

Simple Network Management Protocol (Snmp)

User service allowing the administrator to manage the unit using the SNMP protocol.

Simple Network Management Protocol (SNMP)

A standard of network management that uses a common software agent to manage local and wide area network equipments 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 synchronisation source and network paths.

SIP Endpoint (SipEp)

User service allowing the administrator to associate telephony endpoints with SIP user agents.

Session Traversal Utilities for NAT (STUN)

Session Traversal Utilities for NAT is a standardized set of methods and a network protocol to allow an end host to discover its public IP address if it is located behind a Network Address Translation (NAT)

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.

Switched Circuit Network (SCN)

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.

T

T1

North-American PRI digital signal carrier. 24 channels (23 voice + 1 signaling)

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.

TDM

Method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern

Telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Telephony Interface (TelIf)

User service managing tone generation and detection on the telephony interfaces.

TR-069

The TR-069 also known as CWMP, is a Broadband Forum technical specification. This protocol can be used for monitoring and updating CPE configurations and firmware.

TR-104

The TR-104 is a part of CWMP, a Broadband Forum technical specification. This specification defines the data model for provisioning a Voice over Internet Protocol (VoIP) CPE device by an Auto-Configuration Server (ACS) using the mechanism defined in TR-069.

TR-106

TR-106 specifies data model guidelines to be followed by all TR-069-enabled devices.

TR-111

This specification extends the mechanism defined in TR-069 for remote management of customer premises equipment to allow a management system to more easily access and manage devices connected via LAN through an Internet gateway.

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.

U

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.

V

Virtual LAN (VLAN)

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Virtual Private Network (VPN)

A private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

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.

W

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.

Web (WEB)

User service allowing the administrator to manage the unit using HTTP(S) web pages.

18 DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

19 Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

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



media5corp.com