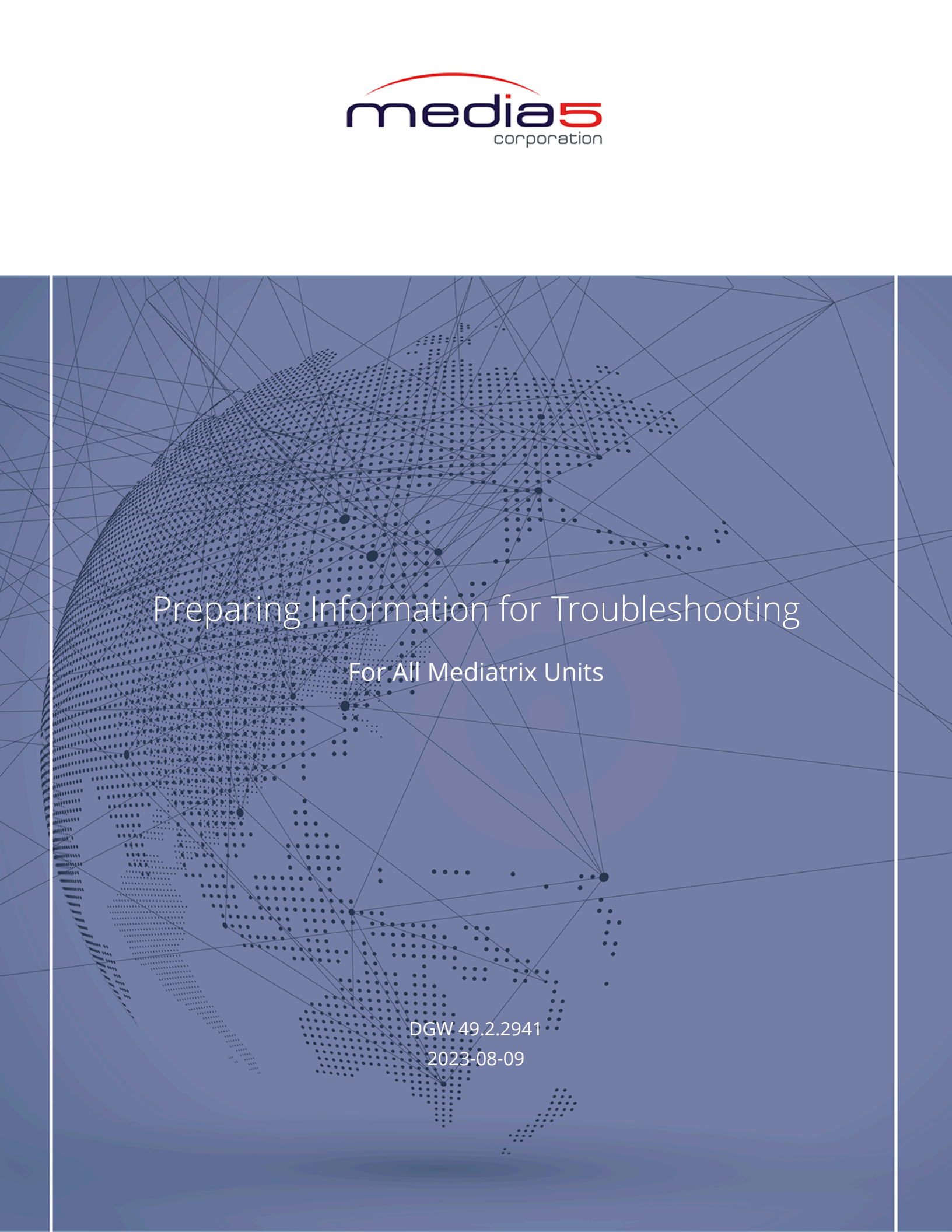


The background of the page is a dark blue gradient with a complex, abstract graphic. It consists of a dense network of thin, light blue lines connecting numerous small, dark blue dots. These dots are arranged in a way that suggests a globe or a network map, with some areas being more densely populated than others. The overall effect is a sense of global connectivity and data flow.

Preparing Information for Troubleshooting

For All Mediatrix Units

DGW 49.2.2941
2023-08-09

Table of Contents

Required Information to Report a Problem	4
Exporting a Configuration Script to Your PC	5
Enabling Syslogs in Debug Mode	6
Packet Captures	7
Starting a Packet Capture	7
Stopping a Packet Capture	8
Remote Packet Capture	9
Starting a Network Capture Remotely On Windows	9
Starting a Network Capture Remotely On MacOS or Linux	11
Capturing a Trace Using Wireshark	14
Enabling the PCM Traces of a Port Using the CLI	16
Enabling PCM Traces of a Port Using the Configuration Script	17
Enabling the PCM Traces of a Port Using UMN	19
Enabling the Automatic Diagnostic Log Dump	21
Manually Starting a Diagnostic Log Dump	21

Table of Contents

Endpoint Examples	22
Online Help	23
DGW Documentation	24
Copyright Notice	25

Required Information to Report a Problem

When reporting a problem and to make sure that all the relevant information is given to the Mediatrix support team at once, the following information is required.

Required information	Checkmark
Mediatrix product name, release and build number.	
Profile name	
Serial number of the Mediatrix unit if a hardware problem is suspected.	
Name/manufacturer/type of other VoIP devices along with their IP addresses.	
Name/manufacturer/software version of the Proxy server (SIP).	
Whenever possible, a diagram of the network or wiring setup.	
Call flow/call scenario to reproduce the problem.	
Is the call going through a NAT, Firewall, Bridge, VPN, Router, Soft switch, etc?	
Export the complete configuration script of the Mediatrix device. Refer to the Exporting a Configuration Script to Your PC instructions.	

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	

Enabling Syslogs in Debug Mode

Information

Although a Syslog server can be used, it is recommended to use Wireshark.

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Remote Host** field, enter the static IP address or domain name and port number of the device that archives the log entries sent by syslog transport.

Note: Specifying no port, or port 0, sends notifications to port 514.

- 3) From the **Diagnostic Traces** field, select **Enable**.
- 4) Click **Edit**.
- 5) In the **Diagnostic Traces** table, select the level of severity an event should have to be reported by the syslog.

IMPORTANT: Enabling all the traces will reduce the performance of the Mediatrix unit and may cause it to no longer respond.

- 6) Click **Apply**.
- 7) Click **Apply** again.

Result

The traces generated by the Mediatrix unit with the selected severity level, will be sent to the specified address.

Syslog Configuration	
Remote Host:	IP address
Technical Assistance Centre	
Diagnostic Traces:	Enable ▾
Filter:	Edit

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**.

Starting a Packet Capture

Steps

- 1) Go to **System/Packet Capture**.
- 2) In the **Packet Capture Configuration** form, complete the fields as required.

Note: The URL format must follow this syntax:

```
protocol://[user[:password]@]hostname[:port]/[path/]filename
```

Note: Available protocols are File, HTTP, and HTTPS but the File protocol is not available on Mediatrix 4102S units.

IMPORTANT: 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) From the **Link Name**, select the link to perform the capture.
- 4) Click **Apply & Start Capture**.

Result

If there are no problems with your configuration, the "Last Capture Result" status will be "Requested". The captured packets will be sent to the specified URL. If the selected URL started with **file://**, then the capture will be sent to the File service.

Packet Capture Configuration	
Max Number Of Frames:	0
Max Number Of Seconds:	0
Filter:	
URL:	protocol://[user[:password]@]hostname[:port]/[path/]filename
Link Name:	v

Stopping a Packet Capture

Steps

- 1) Go to **System/Packet Capture**.
- 2) Click **Apply & Stop Capture**.

Result

If there are no problems with your configuration, the status of the "Last Capture Result" will be "Completed". The captured packets will no longer be sent to the specified URL.

Remote Packet Capture

A remote capture allows a remote Mediatrix unit to capture the traffic on its network interfaces, and forward it through a SSH tunnel, in order to see the traffic live on a local PC running Wireshark.

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.10).

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.

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-antispooof -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-antispooof -pw "administrator" admin@192.168.0.10  
"pcapture -i eth1 host 10.5.128.11 or host 10.5.128.4 " | wireshark -k -i -
```

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.12).

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.

Examples of `pcapture` 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 -
```

Capturing a Trace Using Wireshark

Before you start

You must have downloaded Wireshark at the following link <https://www.wireshark.org/> (Wireshark is a network protocol analyzer. It is an Open Source software released under the GNU General Public Licence. It can decode most VoIP protocols: SIP, MGCP, H.323, RTP, etc.). Select the Windows version. Make sure to install winpcap and read the instructions.

If you are taking a trace on a switch, the port of the switch connected to the PC must be configured to mirror the port connected to the Mediatrix unit. Alternatively, you could use a hub, which should be connected to both the PC running Wireshark and the Mediatrix unit.

Otherwise you will not capture the packets from the unit.

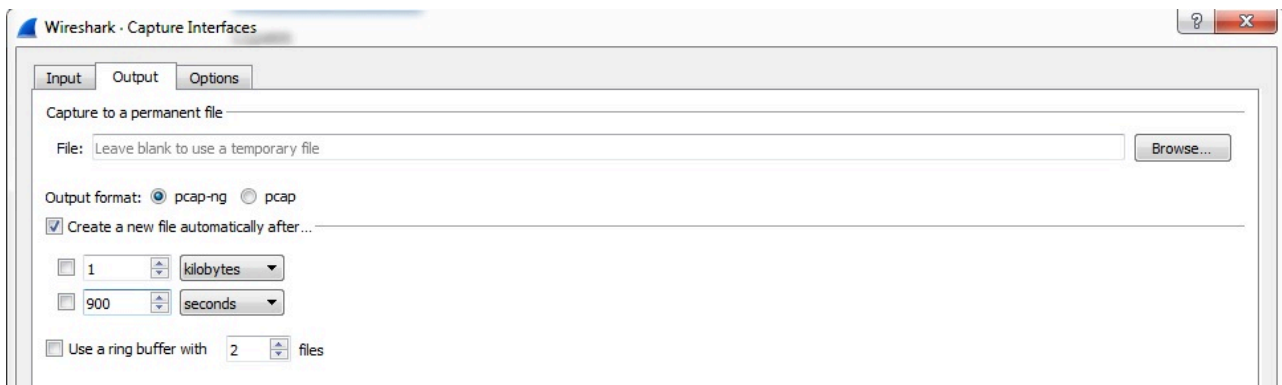
Steps

- 1) In the **Capture** menu, select **Capture Options**.
- 2) In the **Capture** selection list, select the Ethernet network adapters to use.
- 3) In the **(Display) Options** section, select the **Update list of packet in real time** check box.
- 4) Select the **Automatic scrolling in live capture** check box.
- 5) If troubleshooting a random problem happening weekly, select the **Use multiple files** check box.

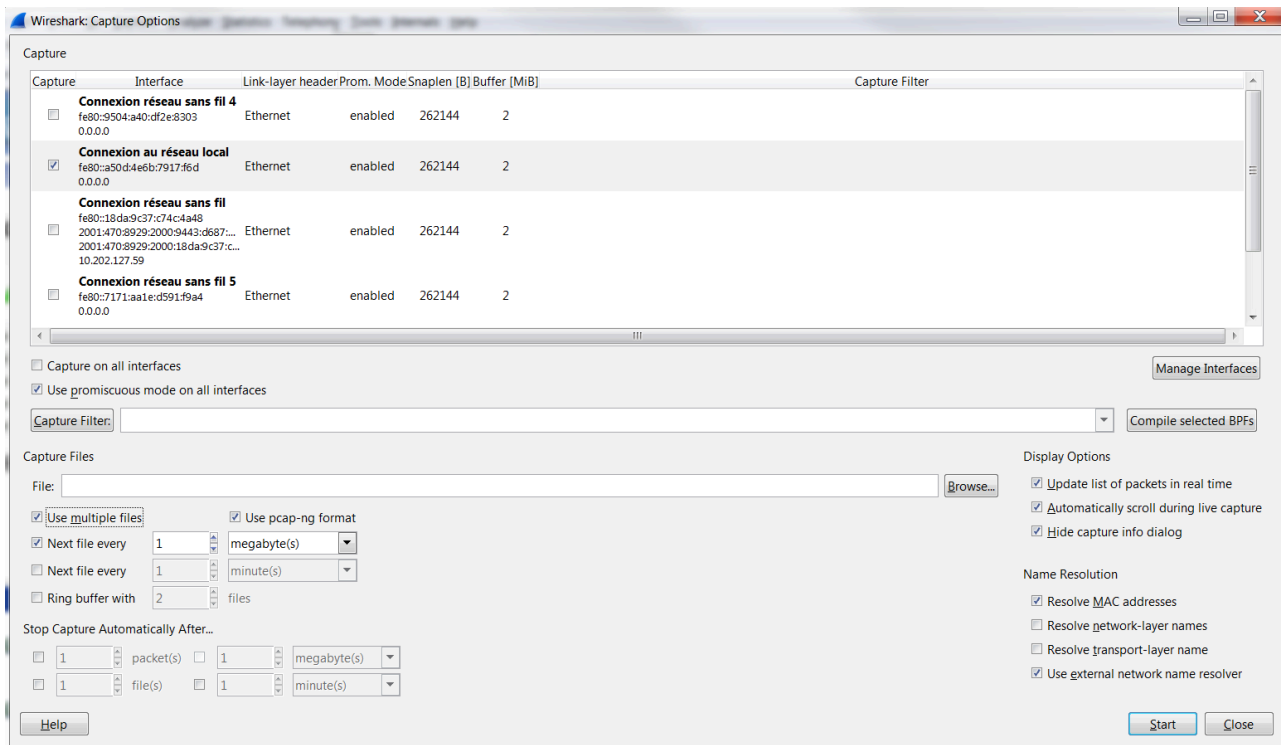
Note: For the latest Wireshark release, this can be configured via **Capture/Options/Output/Create a new file automatically after...**

Result

In Wireshark release 2.2.0



In older Wireshark releases



Enabling the PCM Traces of a Port Using the CLI

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 the CLI, set the **Mipt.PcmCaptureEnable** parameter to **Enable**.

Note: For example **Mipt.PcmCaptureEnable=Enable** or **Mipt.PcmCaptureEnable=1**

- 2) Set the **Mipt.PcmCaptureEndpoint** parameter to the unit's endpoint on which the PCM capture will be taken from. For endpoint examples, refer to [Endpoint Examples](#) (p.22).

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: For example **Mipt.PcmCaptureEndpoint = FXO2**

Note: Port names are case sensitive.

- 3) Set the **Mipt.PcmCaptureIpAddr** MIB parameter to the IP address of the PC running Wireshark.

Note: For example **Mipt.PcmCaptureIpAddr = 192.168.0.17**

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.

- 4) 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** should reflect the values configured.

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.22).

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.

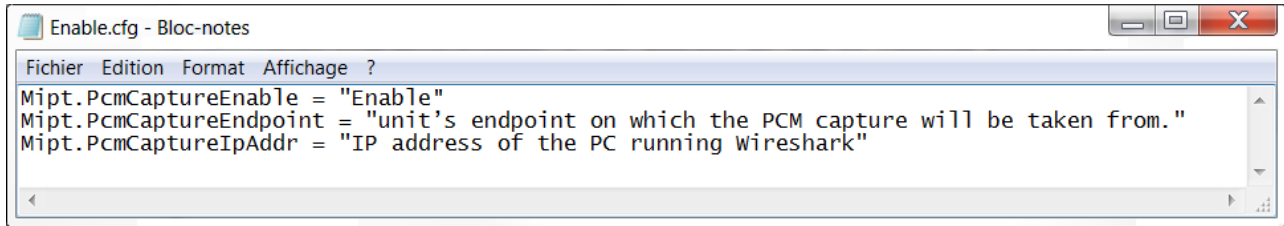
Note: The IP address does not have to be listening on UDP ports, as it is easy to filter out ICMP "port unreachable" messages afterwards.

- 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..



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.22).

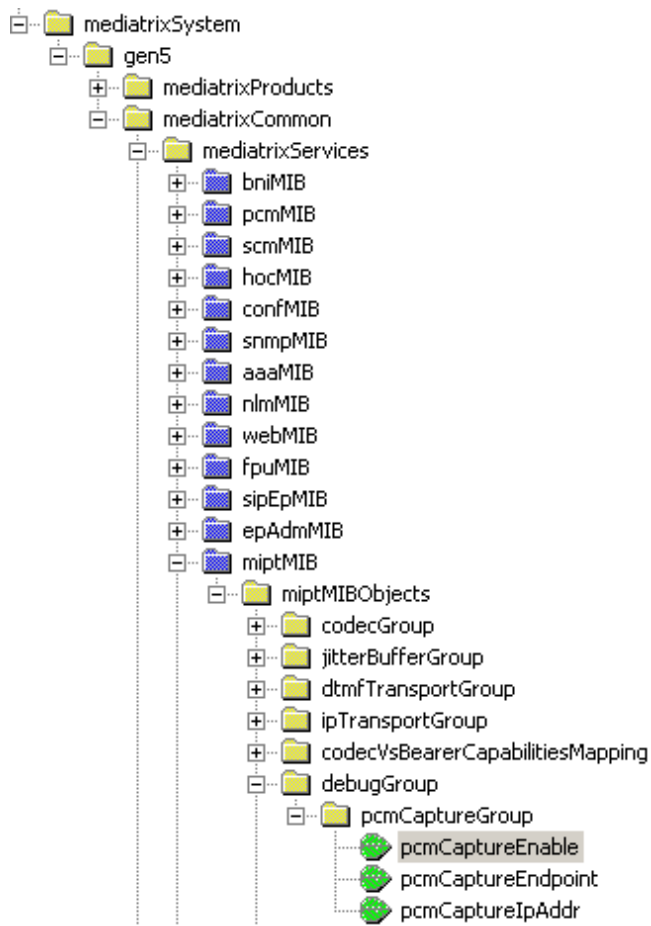
Note: To make sure that you are capturing the appropriate endpoint, please verify its naming by running the following command in CLI: **Epadm.Endpoint**. The output of the command displays a table with the unit's endpoints.

- 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



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.

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.

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 Mediatrix 4108-16-24 unit
Phone-Fax1	Port 1 of a Mediatrix 4102S unit
FXS1	Port 1 of the FXS card of a Mediatrix C7 unit
FXO1	Port 1 of the FXO card of a Mediatrix 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.

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.

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.

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