

Starting a Remote Packet Capture
For All Mediatrix Units

DGW 49.2.2941
2023-08-09

Table of Contents

Packet Captures	3
Starting a Network Capture	3
Starting a Network Capture on a Specific VLAN	5
Starting a Network Capture Remotely On Windows	6
Important Information to Know on Wireshark	8
Starting a Network Capture Remotely On MacOS or Linux	8
Online Help	11
DGW Documentation	12
Copyright Notice	13

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 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.4)
 - 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 through the specified filter will be captured and sent to the specified URL.

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.

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

Starting a Network Capture on a Specific VLAN

Before you start

The VLAN must first be created. Refer to [Creating a VLAN](#) (p.5)

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.

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**

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-antispooof -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-antispooof 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.7).

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 -
```

Important Information to Know on Wireshark

When starting a Network Capture Remotely on windows, two major problems can occur.

- The first time the unit is connected via plink/wireshark, no capture will be displayed in the Wireshark window because plink must first confirm the ssh key. Make sure to toggle to the CMD window to be able to answer **y** to the **Store key in cache? (y/n)** question. Only then will the capture be displayed.
- Only one session at the time must be running. If the **Data written to the pipe is neither in a supported pcap format nor in pcapng format**. Wireshark message is displayed, it is usually because either:
 - there is already another plink or putty session running. Make sure to exit all putty/plink sessions, to quit wireshark and to press CTRL-C several times in the CMD session to make sure the program is terminated.
 - there is another user or a script accessing the device on another PC. In that case, restart the CLI service via the DGW Web interface (under **System/Services**) and wait about 30 seconds.

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.9).

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.

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 -
```

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