This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

GVP Troubleshooting Guide

Collecting Packet Traces

5/9/2025

Contents

- 1 Collecting Packet Traces
  - 1.1 Windows
  - 1.2 Linux

Collecting Packet Traces

Windows

Wireshark is a network protocol analyzer that you can use for analyzing network problems. You can download it from Wireshark.org. After installing wireshark on your Microsoft Windows machine, you can perform the following actions.

Capturing Network Traffic

1. Open Wireshark.
2. To start capturing network traffic, go to **Capture** on the menu bar, and then click **Interfaces**. A window will open.
3. Click **Start** on the desired network interface. Wireshark will start capturing network traffic.
4. To stop capturing, go to Capture on the menu bar, and click **Stop**.
5. To save the captured packets, go to **File** on the menu bar, and click **Save As**. A window will open.
6. Enter a file name, and then click **Save** to save the file.

> **Important**
> The **Packet Range** option enables you to select a specific set of packets to save.

Creating a Packet Filter

Wireshark supports packet filters, which enables you to filter out unwanted packets. For example, the `sip || rtp` filter will display only SIP and RTP packets. You can click Expression to see more filter options.

Displaying VoIP Calls

Wireshark can look for VoIP calls from the captured packets. Go to **Statistics** on the menu bar and click **VoIP Calls**. A window will open with the list of VoIP calls.

Linux

1. Use the following command:
   ```
   dumpcap -i <interface-name> -w <output_file>.pcap
   ```

If using RHEL5, use the following command:

```
tcpdump -s 1500 -i eth0 -w /root/filename.pcap
```

2. Press Ctrl + C to stop and exit the capture.
3. You can then transfer the capture file to a Windows machine to view and filter it by using Wireshark software.
   For example—If `eth0` is the active interface on the machine with which the GVP component (such as MCP, CCP, or RM) is associated, the command in Linux would be the following:

   ```
   dumpcap -i eth0 -w gvpcapture.pcap
   ```