

Troubleshoot Network Latency in SDWAN

Contents

[Introduction](#)

[Troubleshoot Network Latency from vManage](#)

[Source and Destination IPs](#)

[Simulate Flows](#)

[Ping and Traceroute](#)

[Tunnel Health](#)

[App Route Visualization](#)

[Packet Capture](#)

[Control Connections](#)

[Interface Utilization and Statistics](#)

Introduction

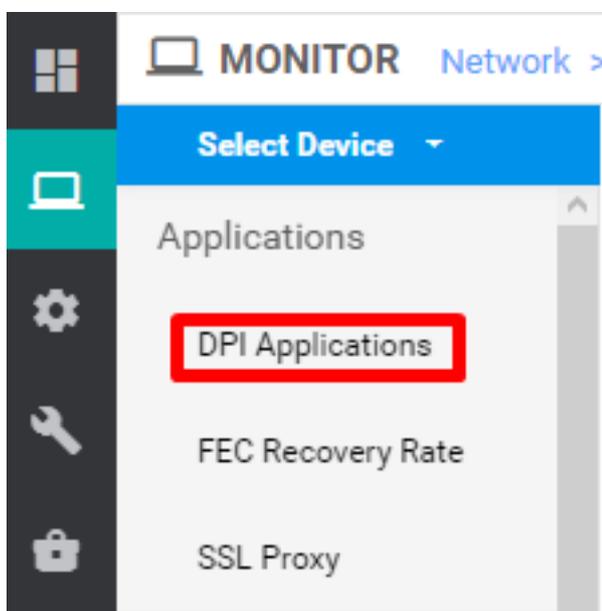
This document describes how to troubleshoot Network Latency (Network 'Slowness') in an SDWAN environment from vManage.

Troubleshoot Network Latency from vManage

Source and Destination IPs

Source and destination IPs are one of the first information to gather. You can provide this information. However, you can always use the DPI Applications tab in vManage, if the issue is application-specific.

Navigate to **Network > Device > DPI Applications**.



Here, you can dive deep into Applications to get the source and destination IPs (provided you have the information about the application in question).

Here is an example of breadcrumbs to find the source and destination IPs for HTTP traffic.

[Network](#) > [Applications - DPI](#) > [web](#) > [https](#)

Simulate Flows

Once you have the source and destination IPs, use SDWANs built-in Simulate Flows to find the next hop for the IPs in question.

Navigate to **Network > Device > Troubleshooting > Simulate flows.**

The image shows a screenshot of the SD-WAN management interface. On the left is a navigation sidebar with categories like WAN, Security Monitoring, and Control Connections. The 'Troubleshooting' option is highlighted in red. The main content area is divided into three panels: 'Connectivity' (with options like Device Bringup, Ping, Trace Route, Speed Test), 'Traffic' (with options like Tunnel Health, App Route Visualization, Packet Capture, and 'Simulate Flows' highlighted in red), and 'Logs' (with Debug Log). Below this is a detailed view of the 'Simulate Flows' tool. It includes a breadcrumb path 'MONITOR > Troubleshooting > Simulate Flows' and a 'Troubleshooting' dropdown. The tool has input fields for 'VPN' (set to VPN-1), 'Source/Interface for VPN-1', 'Source IP', 'Destination IP', 'Application' (Choose), and 'Custom Application (created in CLI)'. A 'Simulate' button is highlighted in red. The 'Output' section shows a diagram of traffic flow from a laptop icon through a tunnel icon to a box representing 'public-internet' and 'Remote System IP Encapsulation IPSec'. The text 'Total next hops: 1 | IPSec: 1' is visible in the bottom right of the output area.

Ping and Traceroute

You can use in-built ping and traceroute tools in vManage to troubleshoot reachability.

Navigate to **Network > Device > Troubleshooting > ping/Traceroute.**

Tunnel Health

The tunnel Health tool comes in handy when you troubleshoot latency between two sites. The tool gives you a comprehensive view of tunnel status over a period of time which you can customize.

You can view statistics about data traffic, traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels.

Navigate to **Network > Device > Troubleshooting > Tunnel Health**.

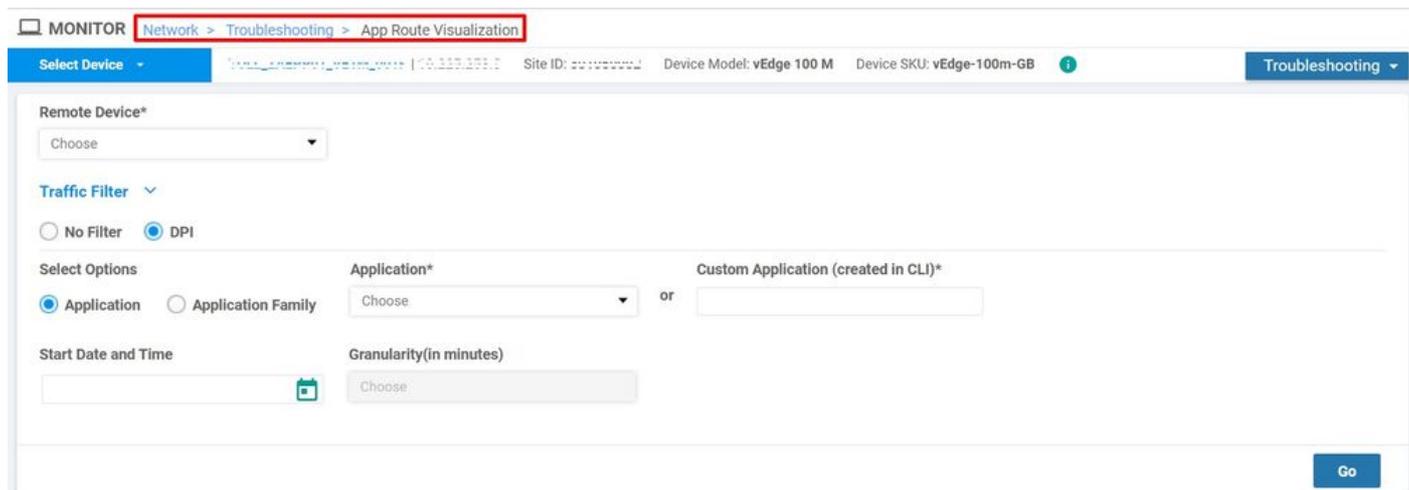


App Route Visualization

This displays the Application-aware routing statistics in graphical format for all tunnels between the two routers. The top graphs display either loss statistics or latency and jitter statistics.

The bottom graphs display the number of packets received and transmitted on the data planetunnel. By default, statistics for the first six tunnels are shown.

Navigate to **Network > Device > Troubleshooting > App Route Visualization**.



Packet Capture

To capture control plane and data plane packets in real-time and to save these packets to a file. Navigate to **Network > Device > Troubleshooting > Packet Capture**.

Control Connections

Check the control connections up-time to verify whether there are any underlying connectivity issues.

From CLI, run **show control connections**.

Interface Utilization and Statistics

Interface utilization and statistics can be viewed from the **Interface** Tab on the left pane. Interface statistics are represented in a graphical view. You can use chart options to filter for specific data.

The time period over which the data to be displayed can be customized.

Navigate to **Network > Device > Interface**.

