Cisco Catalyst SD-WAN Troubleshooting Guide

First Published: 2026-07-01

Last Modified: 2026-07-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Troubleshooting Tools and Methods** 1

- Troubleshooting 1
- Troubleshoot Common Cellular Interface Issues 2
- Troubleshoot WiFi Connections 5
- Troubleshoot a Device 9
  - Check Device Bringup 9
  - Ping a Device 9
  - Speed Test 11
    - Information about speed test 11
    - Restrictions for speed test 12
    - Prerequisites for speed test 12
    - Disable backward-compatible IP for site-to-site speed test 12
    - Verify backward-compatible IP as disabled for site-to-site speed test 12
    - Run Speed Test 13
    - Troubleshooting Speed Test Issues 15
  - Run a Traceroute 15
  - Discover Underlay Paths 16
  - Diagnostic Monitoring Log Capture 16
    - Configure Diagnostic Monitoring Log Capture 16
- BFD Tunnel Troubleshooting 17
- On-Demand Troubleshooting 19
- Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit 24
  - Cisco RADKit in Cisco SD-WAN Manager 25
  - Cisco RADKit Restrictions 25
  - Enable Cisco RADKit service in Cisco SD-WAN Manager 25
  - Use the Cisco RADKit Service APIs 26

Verify Cisco RADKit service in Cisco SD-WAN Manager 27

CHAPTER 2 **Troubleshoot Cisco Catalyst SD-WAN Solution** 31

Support Articles 31

Submit feedback for a support document 33

Disclaimer and caution 34

CHAPTER 3 **Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS** 35

Information About the Unified Debug Condition 35

Restrictions of the Unified Debug Condition 36

Use Cases for the Unified Debug Condition 36

Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI 36

Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS 38

CHAPTER 4 **Collecting System Information in an Admin-Tech File** 43

Feature history: Admin-tech file 43

Collecting system information using an admin-tech file 45

Benefits collecting system information using an admin-tech file 45

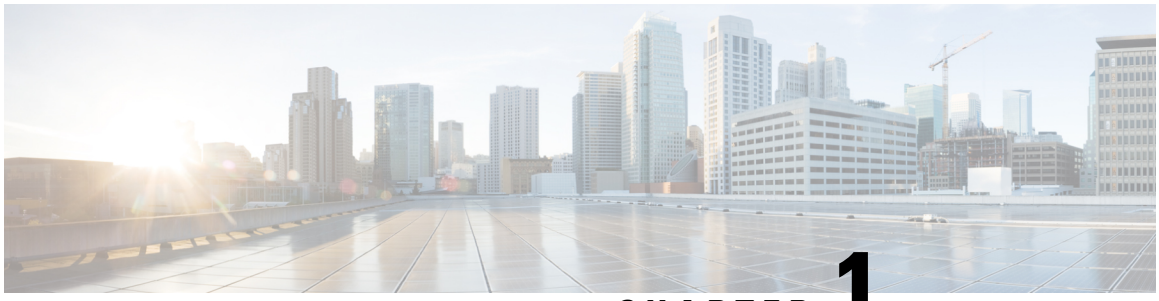
Prerequisites for collecting system information using an admin-tech file 45

Restrictions for collecting system information in an admin-tech file 45

Generate admin-tech files 46

View admin-tech files 48

Upload an admin-tech file to a TAC case 48



CHAPTER 1

Troubleshooting Tools and Methods

- Troubleshooting, on page 1
- Troubleshoot Common Cellular Interface Issues, on page 2
- Troubleshoot WiFi Connections, on page 5
- Troubleshoot a Device, on page 9
- BFD Tunnel Troubleshooting, on page 17
- On-Demand Troubleshooting, on page 19
- Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit, on page 24

Troubleshooting

Table 1: Feature History

Feature Name	Release Information	Description
Improved Access to Troubleshooting Tools in Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	The troubleshooting tools are now easily accessible from the various monitoring pages of Cisco SD-WAN Manager, such as **Site Topology**, **Devices**, **Tunnels**, and **Applications**, thereby providing you with context-based troubleshooting guidance. Earlier, the troubleshooting tools were accessible only from the device dashboard.
Connect to and troubleshoot Cisco Catalyst SD-WAN solution using Cisco RADKit	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Use tools and Python modules from Cisco Remote Automation Development Kit (RADKit) to securely connect to remote terminals, WebUIs, or desktops. Using RADKit, a TAC engineer can request the required information during the troubleshooting process, from the various devices and services, in a secure and controlled way.
Cisco RADKit in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	The Cisco Remote Automation Development Kit (RADKit), a tool for remote automation and troubleshooting, is integrated directly into Cisco SD-WAN Manager. This integration provides the capability to enable or disable the RADKit service using the API in Cisco SD-WAN Manager.

Troubleshoot Common Cellular Interface Issues

Resolve Problems with Cellular Interfaces

This topic describes the most common issues and error messages that occur with cellular connections from the router to the cellular network, and the steps to resolve them.

Insufficient Radio Signal Strength

Problem Statement

The cellular module in the router cannot detect a radio signal from the service provider network.

Identify the Problem

- The signal strength displayed in the Cisco SD-WAN Manager Cellular Status screen or with the **show cellular status** CLI command, or in the Cellular Radio screen or with the **show cellular radio** command is no signal, poor, or good. It should be excellent. The following table lists the ranges of signal strengths:

Table 2:

Signal	Excellent	Good	Fair	Poor
Received signal strength indicator (RSSI)	>= -65 dBm	-65 to -75 dBm	-75 to -85 dBm	<= -85 dBm
Reference signal receive power (RSRP)	>= -80 dBm	–80 to -90 dBm	–90 to -100 dBm	<= -100 dBm
Reference signal receive quality (RSRQ)	>= -10 dBm	-10 to -15 dB	-15 to -20 dB	< –20 dB
Signal-to-noise ratio (SNR)	>= 20 dB	13 to 20 dB	0 to 13 dB	<= 0 dB

Note All parameters must be considered together and not in isolation. For example, a strong RSSI does not mean signal quality is good if RSRP is bad.

- The wireless LED on the router is lit (solid or blinking) and is red, orange or yellow, or it is blinking green. It should be solid green.

Resolve the Problem

1. Examine the router to verify that both basic antennas are correctly installed.
2. Contact the service provider to verify that the location has coverage.
3. Move the router to a new location within the building.
4. Procure an additional external cabled antenna and connect it to the router.

Modem Status Remains in Low-Power Mode

Problem Statement

End users cannot connect to the cellular network, and the modem status remains in low-power mode.

Identify the Problem

- End users cannot connect to the cellular network.
- The error message "Missing or unknown APN" is generated.
- The signal strength is less than excellent.

Resolve the Problem

1. Verify that there is sufficient radio signal strength. If there is not, follow the instructions in the Insufficient Radio Signal Strength section.
2. Verify that the cellular0 interface is operational. When the cellular interface is shut down, the modem status is set to Low Power mode. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   Then click **Real Time**, and from the **Device Options** drop-down list, choose **Interface Detail**.

   To do this from the CLI, use the **show interface** command. Check that the Admin Status and Oper Status values are both Up.
3. Verify that the modem temperature is not above or below the threshold temperatures. To view the modem temperature, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select the router.

   Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Modem**.

   From the CLI, use the **show cellular modem** command.
4. Check that the access point name (APN) in the profile for the cellular0 interface matches the name expected by your service provider. Some service provides required that you configure the APN, and they include configuration instructions in the SIM card package.
   a. To check which APN name is configured, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select the router.

      Cisco vManage Release 20.6.1 and earlier: To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

      Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Profiles**.

      From the CLI, use the ; **show cellular profiles** command. The APN column shows the name of the APN. Each profile specifies an access point name (APN), which is used by the service provider to determine the correct IP address and connect to the correct secure gateway. For some profiles, you must configure the APN.

   b. If the APN is not the one required by the service provider, configure the correct APN. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** and use the **Cellular Profile** feature template.

To configure this from the CLI, use the **cellular cellular0 profile apn** command.

5. If none of the previous steps works, reset the cellular interface.

Error Messages

The following table list the most common error messages that are displayed regarding cellular interfaces:

Table 3:

Error Message	Problem Statement	How Do I Fix the Problem
Authentication failed	End user authentication failed, because the service provider cannot authenticate either the user's SIM card or the Cisco vEdge device SIM card.	Contact the cellular service provider.
Illegal ME	The service provider denied access to an end user, because the end user is blocked from the network.	Contact the cellular service provider.
Illegal MS	The service provider denied access to an end user, because the end user failed the authentication check.	Contact the cellular service provider.
Insufficient resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
IPV4 data call throttled	The SIM card being used in the Cisco vEdge device requires that you configure static APN.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Missing or unknown APN	End users cannot connect to the cellular network, either because an APN is required and is not included in the cellular profile or because the APN could not be resolved by the service provider.	See the profile's APN, as described in Modem Status Remains in Low-Power Mode , above.
MS has no subscription for this service	The service provided denied access to an end user, because the end user has no subscription.	Contact the cellular service provider.
Network failure	The service provider network is experiencing difficulties.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.

Error Message	Problem Statement	How Do I Fix the Problem
Network is temporarily out of resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
Operator has barred the UE	The service provided denied access to an end user, because the operator has barred the end user.	Contact the cellular service provider.
Requested service option not subscribed	The SIM card being used in the Cisco vEdge device requires that you configure a static APN entry.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Service not supported by the PLMN	The Public Land Mobile Network (PLMN) does not support data service.	Contact the cellular service provider.

Troubleshoot WiFi Connections

This topic describes how to check and resolve connection problems between a WiFi client and a WiFi network that is provided by a WiFi router. The procedures described here are applicable to devices that support WiFi only.

Check for WiFi Connection Problems

If a WiFi client is unable to connect to a WiFi network when a router is providing the WiFi network, follow these steps to determine the source of the problem. To perform each step, use a method appropriate for the WiFi client.

1. Verify that the WiFi client can locate the service identifier (SSID) advertised by the router. If the client cannot find the SSID, see the section, SSID Not Located.
2. Verify that the WiFi client can connect to the SSID advertised by the router. If the client cannot connect to the SSID, see the section, SSID Connection Fails.
3. Verify that the WiFi client has been assigned an IP address. If the client cannot obtain an IP address, see the section, Missing IP Address.
4. Verify that the WiFi client can access the Internet. If the client cannot connect to the Internet, see section, Internet Connection Failure.
5. If the WiFi client connection is slow or if you notice frequent disconnects, see section, WiFi Speed Is Slow.

Resolve Problems with WiFi Connections

This section describes the most common issues that occur with WiFi connections between a WiFi client and a router, and it describes steps to resolve the issues.

SSID Not Located

Problem Statement

The WiFi client cannot locate the SSID advertised by the router.

Resolve the Problem

1. Ensure that the basic service set identifier (BSSID) address for the SSID is valid:
   a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   b. Choose a device from the device list that appears.

   c. From the left pane, choose WiFi. The right pane displays information about WiFi configuration on the router.

   d. In the right pane, locate the SSID. Check that the BSSID for this SSID does not have a value of 00:00:00:00:00:00.

   e. If the BSSID is 00:00:00:00:00:00, the WLAN (VAP) interface for this SSID may be misconfigured. Ensure that the WLAN interface has been added to a bridge during the configuration process. To view the running configuration of the device, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. For the desired device, click **...**and choose **Running Configuration**.

      To view the running configuration of the device from the CLI, run the **show running-config** command. To add the WLAN interface to a bridge — from the Cisco SD-WAN Manager, choose **Configuration** > **Templates**.

      Click **Feature Templates**, and choose the **Bridge** feature template.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

2. Eliminate static channels. A static channel is one where you explicitly configure the radio channel rather than allowing the router to automatically select the best radio channel. A slow static channel may appear to be an unreachable SSID.
   a. View the current SSID channel setting for the router. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the list of devices that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose WLAN Clients or WLAN Radios.

      From the CLI, run the **show wlan clients** or **show wlan radios** command.

   b. If the channel is set to a specific number, change the value to "auto". To do this, use the WiFi Radio feature template in Cisco SD-WAN Manager.

      From the CLI, run the **wlan channel auto** command.

3. Ensure that the WiFi client is using the same radio band as the router, either 2.4 GHz (for IEEE 802.11b/g/n) or 5 GHz (for IEEE802.11a/n/ac):
   a. Check which radio band the WiFi client supports.
   b. Check the router's Select Radio setting. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Radios**.

      From the CLI, run the **show wlan radios** command.
   c. If the router and WiFi client radio band settings do not match, either change the WiFi client's radio band or change the settings on the router so that they match. To do this, use the Wifi Radio feature template.

      From the CLI, run the **wlan** command.

SSID Connection Fails

Problem Statement

The WiFi client can locate the SSID advertised by the router but cannot connect to it.

Resolve the Problem

1. If you configure passwords locally on the router, ensure that the WiFi client's password matches the SSID's password.
2. If you are using a RADIUS server, ensure that the RADIUS server is reachable and that the WiFi client's username and password match the RADIUS configuration:
   a. To verify that the RADIUS server is reachable from the router, ping the server. To do this in Cisco SD-WAN Manager, ping a device. From the CLI, run the **ping** command.
   b. Check for matching passwords on the RADIUS server and WiFi client.
3. Ensure that you do not exceed the maximum number of clients for this SSID:
   a. Verify the number of used clients and the maximum number of clients:
      - From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. From the left pane, select WiFi. In the right pane, locate the SSID. Check the No. of Clients field. If the used/maximum values are equal, no more clients can connect to this SSID.
      - From the CLI, run the **show wlan interfaces detail** command.
   b. If needed, increase the maximum clients setting for your SSID. To do this use the WiFi SSID feature template in Cisco SD-WAN Manager.

      From the CLI, run the **max-clients** command.
4. Ensure that the WiFi client supports WPA2 management security:
   a. Check your Management Security setting. To do this, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Interfaces**.

From the CLI, run the **show wlan interfaces** command. If the management security value is set to "required," the WiFi client must support WPA2 security.

b. If necessary, change the Management Security setting for your SSID to "optional" or "none." To do this in Cisco SD-WAN Manager, use the WiFi SSID feature template.

From the CLI, run the **mgmt-security** command.

Missing IP Address

Problem Statement

The WiFi client can connect to the SSID, but cannot obtain an IP address.

Resolve the Problem

Ensure that a DHCP server is reachable and has an available IP address in its address pool:

1. If the router is acting as a DHCP helper (DHCP relay agent), ping the DHCP server to ensure that it is reachable from the router.. From the CLI, run the **ping** command.
2. If you are using a remote DHCP server, check that the remote DHCP server has an available IP address in its address pool.
3. If the router is acting as the local DHCP server:
   a. View the number of addresses being used. From the Cisco SD-WAN Manager menu, **Monitor** > **Devices** and choose a device from the device list that appears. Next, click **Real Time**, and from the **Device Options** drop-down list, choose **DHCP Servers**.

   From the CLI, run the **show dhcp server** command.

   b. Compute the number of IP addresses in the pool based on the configured DHCP address pool size and the number of addresses excluded from the DHCP address pool. To view these values in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. For the desired router, click **...** and choose **Running Configuration**.

   To view them from the CLI, run the **show running-config** command.

   c. If necessary, increase the range of addresses in the router's DHCP address pool using the DHCP-Server feature template in Cisco SD-WAN Manager.

Internet Connection Failure

Problem Statement

The WiFi client is connected to the SSID and has an IP address, but it cannot connect to the Internet.

Resolve the Problem

Ensure that the WiFi client has received the correct default gateway and DNS settings from the DHCP server:

1. If the DHCP server is remote, check the settings on the server.
2. If the router is the DHCP server, ensure that the default gateway and DNS server settings are the same as those on the WiFi client. To view the settings in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device from the device list that is displayed. Click **Real Time,** and in the **Device Options** drop-down list, choose **DHCP Interfaces**.

From the CLI, run the **show dhcp interface** command.

WiFi Speed Is Slow

Problem Statement

The WiFi client can connect to the Internet, but the connection speed is slow.

Resolve the Problem

Allow the router to choose the best WiFi channel:

1. View the current SSID channel setting for the router. To do this in Cisco SD-WAN Manager, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device from the device list that is displayed. Click **Real Time,** and in the **Device Options** drop-down list, choose **WLAN Clients**.

   From the CLI, run the **show wlan clients** or **show wlan radios** command.

2. If the channel is set to a specific number, change the value to "auto". To do this in Cisco SD-WAN Manager, use the WiFi Radio feature template.

   From the CLI, run the **wlan channel auto** command.

Troubleshoot a Device

You can troubleshoot the connectivity or traffic health for all the devices in an overlay network.

Check Device Bringup

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Device Bringup**.

The **Device Bringup** window opens.

Ping a Device

Table 4: Feature History

Feature Name	Release Information	Description
IPv6 Support in Cisco SD-WAN Manager UI Troubleshooting	Cisco Catalyst SD-WAN Manager Release 20.13.1	Added support for using an IPv6 address when pinging a device. Also added support for using an IPv6 address when running a traceroute, configuring packet capture, and simulating flows.

Before You Begin

Ensure that **Device Monitoring** and **Events** features have read and write permissions and **Tools** has read permission. For more information on different permission settings, see Manage Users.

With the set permissions to the usergroup, ensure that you are able to access the required features.

To verify that a device is reachable on the network, ping the device to send ICMP ECHO_REQUEST packets to it:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Ping**.
5. In the **Destination IP** field, enter the IP address of the device to ping.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
6. In the **VPN** field, choose the VPN to use to reach the device.
7. In the **Source/Interface** field, choose the interface to use to send the ping packets.
8. In the **Probes** field, choose the protocol type to use to send the ping packets.
9. In the **Source Port** field, enter the number of the source port.
10. In the **Destination Port** field, enter the number of the destination port.
11. Click **Advanced Options** to specify additional parameters:
    a. In the **Count** field, enter the number of ping requests to send. The range is 1 to 30. The default is 5.
    b. In the **Payload Size** field, enter the size of the packet to send. The default is 64 bytes, which comprises 56 bytes of data and 8 bytes of ICMP header. The range for data is 56 to 65507 bytes.
    c. Enter the **MTU**.

Note The **MTU** option does not apply beginning with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

    d. Click the **Rapid** slider to send five ping requests in rapid succession and to display statistics only for the packets transmitted and received, and the percentage of packets lost.
    e. In the **Type of Service** field, enter the value to be included in the ping packets.
    f. In the **Time to Live** field, enter the round-trip time, in milliseconds, for sending this ping packet and receiving a response.
    g. Click the **Don't Fragment** option to set the **Don't Fragment** bit in the ping packets.

12. Click **Ping**.

From Cisco vManage Release 20.10.1, the **Ping** option can be accessed using one of these methods:

- Choose **Monitor** > **Devices**, click **…** adjacent to the device name, and choose **Ping**.
- In the **Site Topology** page, click a device name or tunnel name, and then click **Ping** in the right navigation pane.

Speed Test

Table 5: Feature History

Feature Name	Release Information	Description
Speed Test	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This feature enables you to carry out speed testing between two edge devices or between a local edge device to a remote iperf3 server.
Speed Test Enhancement	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature allows you to specify your own or preferred iperf3 server for Internet speed test.
Cisco SD-WAN site-to-site speed test with private address	Cisco Catalyst SD-WAN Manager Release 26.1.x	This feature introduces the use of private IP addresses (10.1.x.x) for site-to-site speedtests instead of 11.1.x.x. A new CLI command is provided to disable 11.1.x.x.

Information about speed test

Iperf3 is a network bandwidth test tool used for detecting bandwidth-related network problems.

There are two types of speed test:

- Site-to-site speed test: Cisco SD-WAN Manager tests the network speed and available bandwidth between two devices. Cisco SD-WAN Manager designates one device as the source and the other as the destination.

  From Cisco Catalyst SD-WAN Manager Release 26.1.x, 10.1.x.x (a private IPv4 address) is used as the primary address for the speed test loopback. The 11.1.x.x address is retained as a secondary address to ensure backward compatibility with devices running older software versions.

  You can remove the 11.1.x.x IP address range from the speedtest loopback interface using a CLI command. See the Disable backward-compatible IP address for site-to-site speed test section.

Note After you remove the 11.1.x.x IP address range, the device can no longer perform site-to-site speedtests with peers running older versions that support only the 11.1.x.x range.

- Internet speed test: Cisco SD-WAN Manager tests the network speed and available bandwidth between a device and an iperf3 server reachable by the network. Starting from Cisco vManage Release 20.10.1

and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, users can specify the IP address (or domain name) and port of an iperf3 server to perform Internet speed tests. Cisco SD-WAN Manager designates the device as the client and the iperf3 server as the server.

The speed tests measure upload speed from the source device to the destination device, and measure download speed from the destination device to the source device.

The speed test traffic between edges ignore per-tunnel QoS on hub side and causes impact on the spoke side when WAN interface is congested.

Restrictions for speed test

- Unbound loopback interfaces are not supported for speed test.
- The speed test sends and receives traffic through the control plane, so the test result depends on the router's punt/inject (control plane to data plane communication) efficiency and control plane CPU usage.
- If the `speedtest disable-backward-compatible-ip` command is configured, site-to-site speed test with peer devices on older versions will fail.
- The `speedtest disable-backward-compatible-ip` command is only supported through CLI add-on profile or CLI add-on template.

Prerequisites for speed test

Speed testing requires the system ID and the device host name of the destination device.

Disable backward-compatible IP for site-to-site speed test

To keep only the private IP address (10.1.x.x) for the site-to-site speed test, you can remove the 11.1.x.x IP address range.

Procedure

To remove the 11.1.x.x IP address range from the speed test loopback interface, use the **speedtest disable-backward-compatible-ip** command.

Example:

```
sdwan
speedtest disable-backward-compatible-ip
```

Verify backward-compatible IP as disabled for site-to-site speed test

Procedure

To verify that the backward compatible IP has been disabled for site-to-site speed test, use the **show running-config interface Loopback65529** command.

Example:

The following example shows the configuration before backward compatible ip is disabled:

```
vm5# show running-config interface Loopback65529
interface Loopback65529
 vrf forwarding 65529
 ip address 11.1.85.85 255.255.255.255 secondary
 ip address 10.1.85.85 255.255.255.255
```

The following example shows that only the 10.1.x.x IP address is configured at the loopback interface, implying the compatible IP has been disabled.

```
vm5# show running-config interface Loopback65529
interface Loopback65529
 vrf forwarding 65529
 ip address 10.1.85.85 255.255.255.255
```

Run Speed Test

Perform the following steps to run a speed test.

Run Site-to-Site Speed Test

Before You Begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.
   - **Destination Device**: From the drop-down list, choose the remote device by its device name and system IP address.
   - **Destination Circuit**: From the drop-down list, choose the color of the tunnel interface on the remote device.
6. Click **Start Test**.

The right pane shows the results of the speed test, the download, and upload speed between the source and destination. The download speed shows the speed from the destination to the source, and the upload speed shows the speed from the source to the destination in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table in the lower part of the right pane.

From Cisco vManage Release 20.10.1, the **Speed Test** option is also accessible as follows:

- On the **Monitor** > **Devices** page, click **…** adjacent to the device name and choose **Speed Test**.
- On the **Monitor** > **Applications** page, click **…** adjacent to the application name and choose **Speed Test**.
- On the **Site Topology** page, click a device name, and then click **Speed Test** in the right navigation pane.

Run Internet Speed Test

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.
   - **Destination Device**: From the drop-down list, choose **Internet**.
   - Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a
     - **iPerf3 Server**: (Optional) Enter the hostname or iPer3 server's IP address in IPv4 format.
     - **Server Port Range**: (Optional) Enter the server port or a port range. For example, 5201, 5210, or 5201-5205.
     - Built-in public iperf3 servers list and their port ranges:
       - ping.online.net (5203-5208)
       - iperf.par2.as49434.net (9231-9236)
       - paris.testdebit.info (9201-9240)
       - speedtest.serverius.net(5002)
       - speedtest.uztelecom.uz (5205-5209)
       - iperf.biznetnetworks.com (5201-5203)

Note If you do no provide an iPerf3 server then the built-in iPerf3 servers will be automatically used. The Server Port Range option is only applicable when a user-specified iPerf3 server is entered. If no port range is provided, the system defaults to port 5201. When using the built-in servers, the speed test selects the server with the shortest ICMP ping RTT (Round-Trip Time).

6. Click **Start Test**.

The speed test begins to measure the download and upload speeds between the two endpoints.

Troubleshooting Speed Test Issues

The speed test uses iperf3 with the TCP protocol. The speed test result depends on the latency and packet loss between the client and server.

The built-in speed test servers are not based on geographic proximity, so end users are highly recommended to input and use an iPerf3 server located near them.

The following table provides troubleshooting information for speed testing:

Table 6: Troubleshooting Scenarios

Error Information	Possible Root Cause
Failed to resolve iperf server address	DNS server is not configured at edge device or is unable to resolve the iperf server from the configured DNS server at edge device.
Speed test servers not reachable	The speed test server ping failed. The edge device cannot reach the server IP.
iPerf client: unable to connect stream: Resource temporarily unavailable	Unable to connect to the speed test server. Access may be blocked by access-control list (ACL) permissions.
iPerf client: unable to connect to server	The iPerf3 server is not providing the test service at the user-specified port or default port 5201.
Device Error: Speed test in progress	The selected source or destination device is performing a speed test and cannot start a new one.
Device error: Failed to read server configuration	The data stream configuration is missing. Workaround: Running a CLI command at the edge device and clearing the Cisco Catalyst SD-WAN control connections can fix the issue.
Speed test session has timed out	The speed test has not successfully completed in 180 seconds. This might be because the edge device has lost the control connection to Cisco SD-WAN Manager during the speed testing.

Run a Traceroute

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Trace Route**.
5. In the **Destination IP** field, enter the IP address of the corresponding device in the network.

For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

6. From the **VPN** drop-down list, choose a VPN to use to reach the device.
7. From the **Source/Interface for VPN** drop-down list, choose the interface to use to send the traceroute probe packets.
8. Click **Advanced Options**.
9. In the **Size** field, enter the size of the traceroute probe packets, in bytes.
10. Click **Start** to trigger a traceroute to the requested destination.

The lower part of the right pane displays the following information:

- Raw output of the path the traceroute probe packets take to reach the destination.
- Graphical depiction of the path the traceroute probe packets take to reach the destination.

From Cisco vManage Release 20.10.1, the **Trace Route** option can be accessed using one of these methods:

- Choose **Monitor** > **Devices**, click **…** adjacent to the device name, and choose **Trace Route**.
- In the **Site Topology** page, click a device or tunnel name, and then click **Trace Route** in the right navigation pane.

Discover Underlay Paths

Minimum release: Cisco vManage Release 20.10.1

Diagnostic Monitoring Log Capture

Table 7: Feature History

Feature Name	Release Information	Description
Diagnostic Monitoring Log Capture	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature enables you to collect and record diagnostic data, such as logs and traces, to help diagnose and troubleshoot issues in Cisco SD-WAN Manager, Cellular Gateways and Cisco IOS XE Catalyst SD-WAN devices.

Configure Diagnostic Monitoring Log Capture

Before you begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 To choose a device, click the device name in the **Hostname** column.

Step 3 Click **Troubleshooting** in the left pane.

Step 4 In the **Logs** area, click **Diagnostic Monitoring Log Capture**.

The **Diagnostic Monitoring Log Capture** page opens.

Step 5 From the **Interface for VPN** drop-down list, choose a cellular interface.

Step 6 Expand the **Advance Settings** drop-down list.

Step 7 In the **Modem radio reset**, turn modem radio off and back on for log collection and check the **Enable rotation** field to enable continuous log collection.

Logs consist of multiple files. By default, when file size limit is reached for any given file, log collection continue into the next file until log size limit is reached. If rotation is enabled, log collection continues after log size limit is reached by overwriting the oldest file. Log collection stops when you stop the log collection or when the auto stop timer is reached.

Step 8 In the **Timer**, enable **auto stop timer** to automatically stop log collection after specified time is reached or optionally you can set a **Stop time**.

The range for stop time is 1 to120 minutes.

Step 9 In the **Filter upload**, upload the filter file.

The supported filter file formats are `.sqf`, `.cfg`, and `.bin`.

Step 10 Click **Start** to start the log capture.

You can check the log capture status and download the file after the file is ready.

BFD Tunnel Troubleshooting

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the **Tunnel Troubleshooting** pane is available on the **Monitor** > **Devices** > **Tunnel** page in Cisco SD-WAN Manager:

You can initiate BFD troubleshooting through the Cisco SD-WAN Manager. It provides a user-friendly workflow for identifying and resolving issues. The integration of detailed forensic data and automated debugging steps helps streamline the troubleshooting process, making it more accessible and efficient for network administrators. A functioning BFD session involves various elements like, TLOC, BFD-session, SDWAN-session, IPsec-session, and NAT under the hood functioning and programmed correctly across the layers. When you enable BFD logging for all the existing BFD sessions, the relevant logs for a BFD helps in troubleshooting.

Cisco SD-WAN Manager provides a method to logically group the BFD down sessions so that you can make logical analysis and launch BFD troubleshoot.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that is displayed.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Tunnel Troubleshooting**. The **Tunnel Troubleshooting** window opens.
5. Choose the device from the **Select Device** drop-down box. Or you can search for a device from the **Search** field.
6. Choose the local circuit from the **Select local circuit** drop-down box.
7. Choose the remote device from the **Select remote device** drop-down box
8. Choose the remote circuit from the **Select remote circuit** drop-down box.
9. Choose the encapsulation details from the **Encapsulation** drop-down box.
10. Click **Go**

    You can check the **Progress** and **Conclusions** pane for details on BFD sessions.

Progress Examples

- Collecting troubleshoot data from a local device.
- Checking BFD session, Tunnel, SDWAN session, resource allocation and anomalies from device.
- Collecting troubleshoot data from a remote device.
- Processing troubleshoot data collected from local and remote device.
- Verifying BFD session setup, state machine, echo packets, tunnel setup, sdwan session setup, underlay setup, symnat for BFD session

Conclusion Examples

- Machine reasoning has completed
- Local Device : Local TLOC is created
- Local Device : Remote TLOC is created
- Local Device : IPSec session is created
- Local Device : BFD session is created
- Local Device : SDWAN session is created
- Local Device : BFD discriminator is allocated
- Local Device : IPSec flow ID is allocated
- Local Device : Adjacency is resolved
- Local Device : BFD state is Up

- Remote Device : Local TLOC is created
- Collecting troubleshoot data from a local device.

On-Demand Troubleshooting

Table 8: Feature History

Feature Name	Release Information	Description
On-Demand Troubleshooting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature lets you view detailed information about the flow of traffic from a device. You can use this information to assist with troubleshooting.
Enhancement to On-Demand Troubleshooting	Cisco vManage Release 20.11.1	You can view the detailed troubleshooting progress of the flow of traffic from a device.

Information About On-Demand Troubleshooting

On-demand troubleshooting lets you view detailed information about the flow of traffic from a device.

By default, Cisco SD-WAN Manager captures aggregated information about flows. You can obtain detailed information for specific devices and for specific historical time periods by adding an on-demand troubleshooting entry. When you add an entry, Cisco SD-WAN Manager compiles detailed information according to parameters that you configure.

To conserve system resources, Cisco SD-WAN Manager compiles detailed information only when you request it by adding an entry. In addition, Cisco SD-WAN Manager stores the information for a limited time (3 hours by default), then removes it. You can request the same information again, if needed.

Note On a Cisco SD-WAN Manager cluster setup, only a connected node can remove an on-demand troubleshooting task or mark it as complete.

Restrictions for On-Demand Troubleshooting

Ensure that no Cisco or third-party APIs that instruct on-demand troubleshooting to stop are called when you are using on-demand troubleshooting. These APIs prevent on-demand troubleshooting from compiling information.

Page Elements

The **On Demand Troubleshooting** window provides options for configuring and adding an on-demand troubleshooting entry. The **On Demand Troubleshooting** window displays information about existing on-demand troubleshooting entries and provides the following information and options.

Item (Field)	Description
ID	System-assigned identifier of the entry.
Device ID	System IP of the device to which the entry applies.
Data Type	Type of data for which the entry provides detailed information.
Creation Time	Date and time that you added the entry.
Expiration Time	Date and time that the entry expires. At this expiration time, the entry is removed from the table automatically, and the corresponding detailed information is no longer available. By default, an entry is removed 3 hours after its creation time.
Data Backfill Start Time	Start date and time of the data backfill period.
Data Backfill End Time	End date and time of the data backfill period.
Status	Status of the entry: • **IN_PROGRESS**: Detailed troubleshooting information is in the process of being compiled. • **QUEUED**: Detailed troubleshooting information is queued for compilation. • **COMPLETED**: Detailed troubleshooting information has been compiled.

Configure On-Demand Troubleshooting

You can configure on-demand troubleshooting for a device from the **Tools** > **On Demand Troubleshooting** window in Cisco SD-WAN Manager. This window provides options for adding an on-demand troubleshooting entry, and for managing existing entries.

Cisco vManage Release 20.6.1 and earlier: You can configure on-demand troubleshooting for a device from the **Monitor** > **On Demand Troubleshooting** window in Cisco SD-WAN Manager.

You can also start on-demand troubleshooting from various locations in the **Monitor** > **Devices** window for a device. See View On-Demand Troubleshooting Information for a Device, on page 22.

Cisco vManage Release 20.6.1 and earlier: You can start on-demand troubleshooting from various locations in the **Monitor** > **Network** window for a device.

On-demand troubleshooting is qualified for troubleshooting entries for up to 10 devices concurrently.

Add an On-Demand Troubleshooting Entry

Adding an entry in the **On Demand Troubleshooting** window instructs Cisco SD-WAN Manager to compile detailed troubleshooting information for the device that you specify, using the parameters that you configure.

To add an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. From the **Select Device** drop-down list, choose the Cisco IOS XE Catalyst SD-WAN device or the Cisco vEdge device for which you want to enable on-demand troubleshooting.

3. From the **Select Data Type** drop-down list, choose **SAIE** or **ConnectionEvents**.

4. Choose an option for the data backfill period:

   - **Last 1 hour**: Provides detailed stream information for the period beginning 1 hour before you add the troubleshooting entry and ending at the time that you add the entry.
   - **Last 3 hours**: Provides detailed stream information for the period beginning 3 hours before you add the troubleshooting entry and ending at the time that you add the entry.
   - **Custom Date and Time Range**: Use the **Start date and time** and the **End date and time** fields to designate the backfill period that you want. Note that the **End date and time** value cannot be later than the current date and time.

5. Click **Add**.

   The troubleshooting entry appears in the table of entries. When the value in the **Status** field for the entry shows the value **Completed**, you can view the troubleshooting information from the **Monitor** > **Devices** window, as described in View On-Demand Troubleshooting Information for a Device, on page 22.

Update an On-Demand Troubleshooting Entry

Update an on-demand troubleshooting entry to make changes to its configuration settings. For example, update an entry to adjust its backfill period.

Only entries that are in the QUEUED state can be updated.

To update an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. In the table of entries, click **…** adjacent to the entry that you want to update and choose **Update**.

3. In the **Update Troubleshoot Status** dialog box that is displayed, configure the settings as needed, and click **Add**.

Delete an On-Demand Troubleshooting Entry

Deleting an on-demand troubleshooting entry removes the entry from Cisco SD-WAN Manager. After you delete an entry, you can no longer view its detailed information.

Deleting an entry can help free resources in Cisco SD-WAN Manager.

To delete an on-demand troubleshooting entry, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **On Demand Troubleshooting**.

2. In the table of entries, click **…** adjacent to the entry that you want to delete and choose **Delete on demand queue**.
3. In the **Delete On Demand Status** window that is displayed, click **OK**.

View On-Demand Troubleshooting Information for a Device

You can view on-demand troubleshooting information for a device from the **Network** window for that device.

Before you can view this information, at least one on-demand troubleshooting entry must exist for the device. Add an entry from the **On Demand Troubleshooting** window as described in Add an On Demand Troubleshooting Entry, or add an entry from the **Network** window as described in the following procedure.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. In the **Hostname** column, click the device for which you want to view the information.
3. Perform either of these actions:
   - To view the troubleshooting information for an SAIE application:
     a. Click **SAIE Applications**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Applications** is called **DPI Applications**.

     b. In the **Applications Family** table, click an application family.
     c. In the **Applications** table, click an application.

   - To view troubleshooting information for a specific metric, in the left pane, under **ON-DEMAND TROUBLESHOOTING** click an option. Not all options apply to all device types.
     - **FEC Recovery Rate**
     - **SSL Proxy**
     - **AppQoe TCP Optimization**
     - **AppQoE DRE Optimization**
     - **Connection Events**

       From Cisco Catalyst SD-WAN Manager Release 20.16.1, if you enable unified logging for your device, you can view the firewall security connection events for inspect, pass, and drop actions. The connection event information also includes the reason for traffic drop by the firewall policy.
     - **WAN Throughput**
     - **Flows**
     - **Top Talkers**

The **Flows** and **Top Talkers** metrics are only for TCP Optimized flows.

If on-demand troubleshooting is configured for the device, detailed troubleshooting information appears. This information includes traffic statistics and metrics such as source IP address, destination IP address, number of packets, number of bytes, and more. Use the options that are available and hover your cursor over elements on the graphs to view the information that you need.

Note Starting from Cisco IOS XE Release 17.9.1a, use the **policy ip visibility features enable** command to manually enable or disable the feature fields in Flexible Netflow (FNF). Use the **show sdwan policy cflowd-upgrade-status** command to check which features were enabled before the version upgrade. You have to manually control the features after a version upgrade using the disable or enable commands.

For more information, see policy ip visibility command page.

If on-demand troubleshooting information is not configured, the **Enable On Demand Troubleshooting** option is displayed. Continue to Step 4.

4. If the **Enable On Demand Troubleshooting** option is displayed, perform these actions to start this feature for the selected device:
   a. Click **Enable On Demand Troubleshooting**.
   b. Choose one of the following options:
      - **Quick Enable**: Starts an on-demand troubleshooting entry with a backfill period of 3 hours. With this option, detailed stream information for the past 3 hours becomes available.

        After you choose this option, click **Refresh** to view the detailed troubleshooting information. It can take a few minutes for this information to become available. Alternatively, click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window that includes the entry that you just added.
      - **Go to On Demand Troubleshooting**: Displays the **On Demand Troubleshooting** window. Add an entry in this window as described in Add an On Demand Troubleshooting Entry. Repeat Steps 1 to Step 3 in this procedure to view the detailed information.

View Progress of On-Demand Troubleshooting

Minimum supported release: Cisco vManage Release 20.11.1

After you enable on-demand troubleshooting, the **On-demand Troubleshooting in Progress** message appears on the **Monitor** > **Devices** page. The message remains until the troubleshooting is complete.

Click a chart option to view the troubleshooting progress in a graphical format. Select a time period to display data or click **Custom** to display a selection of a custom time period.

You can use the **request nms olap-db** command to start, stop, or restart the Cisco SD-WAN Manager online analytical processing (OLAP) database or view the status of the database.

For more information about this command, see request nms olap-db.

View Detailed Top Source Data

After on-demand troubleshooting is configured, you can view detailed information about top application usage for a device. To do so, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** > **Top Applications**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** > **Top Applications**.

2. In the **SAIE Application** tab, click an application usage bar in the chart.

Note In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Application** is called **DPI Application**.

3. In the chart for the application that you selected, click the device usage bar.

   If on-demand troubleshooting is configured for the device, detailed top source data appears.

   If on-demand troubleshooting information is not configured, the **Go to On Demand Troubleshooting** option appears. Continue to Step 4.

4. If the **Go to On Demand Troubleshooting** option appears, perform these actions:

   a. Click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window.

   b. In the **On Demand Troubleshooting** window, add an entry, as described in Add an On Demand Troubleshooting Entry.

   c. Repeat Step 1 to Step 3 in this procedure to view the detailed information.

Troubleshoot Cisco Catalyst SD-WAN Solution Using Cisco RADKit

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1

Use Cisco RADKit to troubleshoot devices in Cisco Catalyst SD-WAN. RADKit, a Software Development Kit (SDK), is a set of ready-to-use tools and Python modules, which helps you

- securely connect to remote terminals, WebUI's or desktops,
- leverage APIs for remote or local automations, and
- share support data privately with Cisco Services without any impact on data privacy.

Before You Begin

- Ensure that you have an internet connection and have configured DNS in the transport VPN (VPN0).
- Ensure that you are running compatible operating systems. For information about supported operating systems, see Compatibility.

Installation

The RADKit installation includes a client and a service that connects to the Cisco RADKit cloud to interactively connect you to remote terminals, WebUIs, or desktops.

To install the RADKit service, go to Cisco's Support Services Technical Assistance Center (TAC) and open a support case. After you have installed the RADKit service, you can enroll to the RADKit client. For more information, see Initial Client Setup.

For more information and downloads, see RADKit.

Cisco RADKit in Cisco SD-WAN Manager

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco RADKit, version 1.8.6rc1, is directly installed in Cisco SD-WAN Manager which provides the environment and resources for RADKit to operate, including the file system, shell access, and network connectivity.

Cisco RADKit is a tool used for remote automation and troubleshooting. With it now directly installed in Cisco SD-WAN Manager, it helps you to

- eliminate the need for a separate virtual machine, simplifying deployment, and saving resources
- ensure the service remains active and functions correctly even during Cisco SD-WAN Manager reboots or upgrades, and
- quicken operations with direct access to devices , improving performance by eliminating the need for an intermediate jumphost.

Enablement and disablement of Cisco RADKit Service using API

You can enable or disable the Cisco RADKit service in Cisco SD-WAN Manager using the Cisco SD-WAN Manager API. When enabled, the service initializes, performing its setup and startup process. During enablement, the service automatically registers itself with the Cisco Catalyst SD-WAN Portal for the Cisco RADKit service to function correctly.

Cisco RADKit Restrictions

Cisco RADKit and Cisco SD-WAN Manager cluster deployment

Cisco RADKit does not support clustering. However, it can operate where Cisco SD-WAN Manager is deployed as a cluster.

Enable Cisco RADKit service in Cisco SD-WAN Manager

Enabling Cisco RADKit service in Cisco SD-WAN Manager allows you to activate its capabilities for remote automation, operation, and troubleshooting of network equipment directly from Cisco SD-WAN Manager.

This section provides the steps to enable Cisco RADKit service in Cisco SD-WAN Manager.

Before you begin

- To make API requests that modify system settings, such as enabling or disabling the RADKit service, you must have administrative privileges to access Cisco SD-WAN Manager API interface (https://<sd-wan-manager-ip>/apidocs).
- Ensure proper internet and DNS connectivity for the Cisco RADKit service to function correctly.

Procedure

Step 1 Open your web browser and navigate to the Cisco SD-WAN Manager API documentation by entering the URL: `https://<sd-wan-manager-ip>/apidocs` (replace <**`sd-wan-manager-ip`**> with the actual IP address of your Cisco SD-WAN Manager instance).

Step 2 Within the API documentation, look for the API endpoint related to container services or specifically for RADKit, for example, `/dataservice/settings/configuration/<type>` where type is radkit .

Step 3 Make a POST request to this endpoint.

You will find an option to make a `POST` request to this endpoint.

Step 4 In the request body, provide the following JSON payload:

```
{"mode": "enabled"}
```

Step 5 Click **Execute**.

Once the API call is successfully executed, the RADKit service is enabled, and it will begin its initialization and setup process.

What to do next

Confirm that the RADKit container is running and healthy. You can do this by using the CLI command `request nms container-manager diagnostics`.

To disable the service, post an API request to the RADKit service endpoint in Cisco SD-WAN Manager with a JSON payload of `{"mode": "disabled"}`.

Use the Cisco RADKit Service APIs

This task explains how to correctly format URLs for making API calls to the Cisco RADKit service. To successfully access RADKit functionalities, you must include `/radkit` as a mandatory prefix before the specific API endpoint in your URL. This ensures your request is properly routed within the Cisco SD-WAN Manager environment.

To access RADKit Service API endpoints, follow these steps:

Before you begin

Ensure you have access to your Cisco SD-WAN Manager instance's IP address and port.

Procedure

Construct the API URL by including the /radkit prefix before the actual endpoint.

Example:

To access the login API, the format for the URL is:

```
https://<sd-wan-manager-ip>:<port>/radkit/your/api/endpoint
```

Example:

```
https://10.240.185.84:8443/radkit/api/v1/auth/login
```

You have successfully constructed the correct URL format for accessing a Cisco RADKit Service API endpoint.

What to do next

Proceed to make your API calls to the Cisco RADKit Service using the constructed URL.

Verify Cisco RADKit service in Cisco SD-WAN Manager

By verifiying Cisco RADKit service in Cisco SD-WAN Manager, you can confirm the Cisco RADKit Service's operational status (enabled or disabled).

This section provides the steps to verify whether the Cisco RADKit service in Cisco SD-WAN Manager is enabled or disabled.

Before you begin

- Ensure you have CLI access to Cisco SD-WAN Manager.

Procedure

From the CLI interface of Cisco SD-WAN Manager, execute the following command:

request nms container-manager diagnostics

```
NMS container manager
Checking container-manager status

Listing all images
------------------------
REPOSITORY                  TAG         IMAGE ID       CREATED        SIZE
sdwan/reporting             latest      10d3363a0c7c   15 hours ago   941MB
sdwan/messaging-server      0.20.0      30547ceba4b9   15 hours ago   150MB
sdwan/radkit                1.8.6rc1    5ebe514b17d4   15 hours ago   782MB
sdwan/cluster-orchestrator  1.0.1       5aa1fd0e8e18   15 hours ago   669MB
sdwan/configuration-db      4.4.38      d6b9eb6fd60e   15 hours ago   548MB
sdwan/olap-db               24.3.6.48   219369311a35   15 hours ago   409MB
sdwan/cloudagent-v2         1.0.0       a56c3552ab49   15 hours ago   703MB
sdwan/upgrade-coordinator   2.0.0       d95f20da260b   15 hours ago   141MB
sdwan/application-server    24.0.1      7d505d68bf3f   15 hours ago   1.15GB
```

```
sdwan/coordination-server    3.8.4       91b45542b9e2   15 hours ago   346MB
sdwan/vault                  1.0.1       b2323a89ada8   2 weeks ago    511MB
sdavc                        4.7.0       d1512d663ac7   7 weeks ago    749MB
sdavc-gw                     4.7.0       4ed15cea64ee   7 weeks ago    463MB

Listing all containers
------------------------
CONTAINER ID   IMAGE                              COMMAND                  CREATED         STATUS
                     PORTS

                                                     NAMES
ed8024e0dbb5   sdwan/messaging-server:0.20.0      "/bin/bash /entrypoi…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:4222->4222/tcp, 127.0.0.1:6222->6222/tcp, 127.0.0.1:8222->8222/tcp

                                                      messaging-server
9013b37451d9   sdwan/olap-db:24.3.6.48            "/usr/bin/tini -- /e…"   6 minutes ago   Up 6
minutes (healthy)        127.0.0.1:8123->8123/tcp, 127.0.0.1:9363->9363/tcp

                                                        olap-db
95fea11679e7   sdwan/cloudagent-v2:1.0.0          "./entrypoint.sh"        6 minutes ago   Up 6
minutes (healthy)        127.0.0.1:9051-9052->9051-9052/tcp

                                                        cloudagent-v2
2e534bbea1af   sdwan/reporting:latest             "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes                  80/tcp, 127.0.0.1:9080->9080/tcp

                                                        reporting
b25381e8e543   sdwan/coordination-server:3.8.4    "/docker-entrypoint.…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:2181->2181/tcp, 127.0.0.1:2888->2888/tcp, 127.0.0.1:3888->3888/tcp,
 127.0.0.1:4888->4888/tcp
                                                     coordination-server
0b696e5f38d5   sdwan/vault:1.0.1                  "docker-entrypoint.s…"   6 minutes ago   Up 6
minutes (healthy)        8200/tcp, 127.0.0.1:8201-8202->8201-8202/tcp

                                                        vault
3c7254a24f5a   sdavc:4.7.0                        "/usr/local/bin/sdav…"   6 minutes ago   Up About
 a minute (healthy)   127.0.0.1:10503->8080/tcp, 127.0.0.1:10504->8443/tcp

                                                     sdavc
944e74177a8f   sdavc-gw:4.7.0                     "/bin/bash -c 'exec …"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:8444->8444/tcp, 127.0.0.1:10501->8080/tcp, 127.0.0.1:10502->8443/tcp,
 127.0.0.1:10000->50000/udp
                                                    sdavc-gw
0c9c29dbf0a8   sdwan/configuration-db:4.4.38      "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes (healthy)       127.0.0.1:2004->2004/tcp, 127.0.0.1:5000->5000/tcp, 127.0.0.1:6000->6000/tcp,
 127.0.0.1:6362->6362/tcp, 127.0.0.1:6372->6372/tcp, 127.0.0.1:7000->7000/tcp,
127.0.0.1:7473-7474->7473-7474/tcp, 127.0.0.1:7687-7688->7687-7688/tcp   configuration-db
c7fe7153a21a   sdwan/application-server:24.0.1    "/usr/bin/tini -g --…"   6 minutes ago   Up 6
minutes (healthy)

                                                        base-application-server
6c8f3ec5103f   sdwan/cluster-orchestrator:1.0.1   "/entrypoint.sh"         7 minutes ago   Up 7
minutes (healthy)        127.0.0.1:9090->9090/tcp, 127.0.0.1:9099->9099/tcp

                                                        cluster-orchestrator

Docker info
------------------------
Client:
 Context:    default
 Debug Mode: false

Server:
 Containers: 11
```

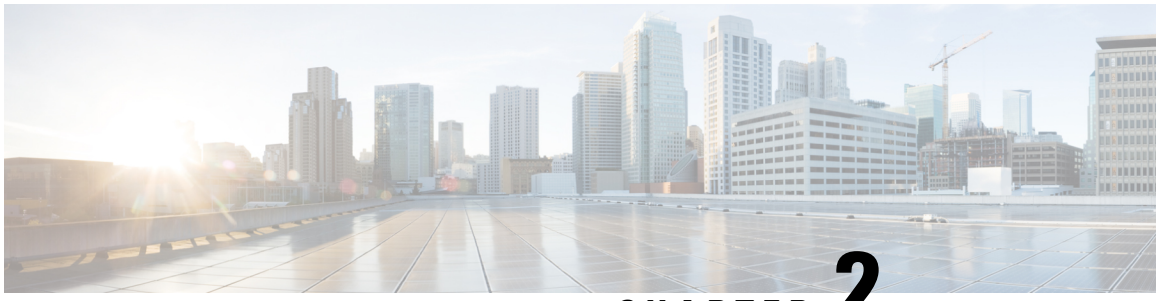
```
 Running: 11
 Paused: 0
 Stopped: 0
Images: 13
Server Version: 23.0.6
Storage Driver: overlay2
 Backing Filesystem: extfs
 Supports d_type: true
 Using metacopy: false
 Native Overlay Diff: true
 userxattr: false
Logging Driver: local
Cgroup Driver: cgroupfs
Cgroup Version: 1
Plugins:
 Volume: local
 Network: bridge host ipvlan macvlan null overlay
 Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
Swarm: inactive
Runtimes: io.containerd.runc.v2 runc
Default Runtime: runc
Init Binary: docker-init
containerd version: b1624c3628954e769dd50783b63823040b2db38c.m
runc version: v1.1.14-0-g2c9f5602-dirty
init version: b9f42a0-dirty
Security Options:
 seccomp
  Profile: builtin
Kernel Version: 6.6.21-yocto-standard
Operating System: viptela 20.18.1 (scarthgap)
OSType: linux
Architecture: x86_64
CPUs: 8
Total Memory: 23.48GiB
Name: vm
ID: 7f6e3203-ad3a-40af-aacd-21e43cbe1c9c
Docker Root Dir: /var/lib/nms/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false

WARNING: No cpu cfs quota support
WARNING: No cpu cfs period support
WARNING: No blkio throttle.read_bps_device support
WARNING: No blkio throttle.write_bps_device support
WARNING: No blkio throttle.read_iops_device support
WARNING: No blkio throttle.write_iops_device support
```

What to do next

Analyse the output within the **Listing all containers** section; the `radkit` container will be listed there Cisco RADKit service if is enabled.

For detailed information on Cisco RADKit user operations, see the documentation: https://radkit.cisco.com/docs/control_api/control_api.html#user-operations.



CHAPTER 2

Troubleshoot Cisco Catalyst SD-WAN Solution

- Support Articles, on page 31
- Submit feedback for a support document, on page 33
- Disclaimer and caution, on page 34

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

Document	Description
Activate Debugs in vManage	This video provides the steps to activate debugs in Cisco Catalyst SD-WAN Manager
Manual Certificate Renewal on SD-WAN Controller	This video provides the steps to get controllers certificates renewal.
Troubleshoot software image expansion failure due to lack of bootflash space	Describes how to verify that a device successfully expanded a software image file when changing from Autonomous mode to Controller mode. It indicates how to troubleshoot if the expansion was not successful.
Error message during software upgrade or setting default software version	This troubleshooting document describes scenarios in which error messages can occur during device software upgrade or when setting the default software version.

Cisco TAC articles

Document	Description
Cisco Catalyst SD-WAN Control Traffic Overhead User Guide	Describes how to calculate control traffic overhead on an SD-WAN overlay deployment.

Document	Description
Collect an Admin-Tech in SDWAN Environment and Upload to TAC Case	Describes how to initiate an `admin-tech` in a Cisco Catalyst SD-WAN environment.
Configure Basic Parameters to Form Control Connections on cEdge	Describes the basic configuration and correct commit order to onboard a cEdge to a Software-Defined Wide Area Network (SD-WAN) overlay.
Configure HSECK9 License on cEdge SD-WAN XE	Describes how to install and troubleshoot HSECK9 licenses on SD-WAN XE cEdges.
Configure SD-AVC on Cisco Catalyst SD-WAN	Describes how to configure Software Defined-Application Visibility and Control (SD-AVC) on a Software-Defined Wide Area Network (SD-WAN).
Deploy a CSR1000v/C8000v on Google Cloud Platform	Describes the procedure to deploy and configure a Cisco Cloud Services Router 1000v (CSR1000v) and Catalyst 8000v (C800v) Edge Router on Google Cloud Platform (GCP).
How To Generate Self-Signed Web Certificate For Cisco Catalyst SD-WAN Manager	Describes how to generate and install a self-signed web certificate when the existing one is expired on an on-prem Cisco SD-WAN Manager. Cisco does not sign web certificates for such deployments, customers have to sign it by own Certificate Authority (CA) or some third-party CA.
HSEC License FAQs for Cisco Catalyst SD-WAN	Describes a few queries about the HSEC license for the autonomous and SD-WAN modes.
Modifying "Statistics Configuration > Collection Interval" in a vManage Cluster	Describes the process of modifying the **Statistics Configuration** > **Collection Interval** in a vManage cluster.
Quick Start Guide - Data Collection for Various Cisco Catalyst SD-WAN Issues	Describes several SD-WAN issues along relevant data that must be collected in advance before you open a TAC case to improve the speed of troubleshooting and/or problem resolution. This document is broken up into two main technical sections: Cisco SD-WAN Manager and Edge routers. Relevant outputs and command syntax are provided dependent upon the device in question.
Replace a cEdge RMA Router	Describes how to replace a failed cEdge unit with another one. This consists of a copy of the configuration from the failed router to the replacement router, the removal of this cEdge, and the addition of the new router into the network. This process is similar to vEdge replacement however, the copy option is missed in Cisco SD-WAN Manager for cEdges.
Transfer Files between a cEdge and Cisco Catalyst SD-WAN Manager	Describes how to transfer files between a remote cEdge and a local Cisco SD-WAN Manager through CLI.

Document	Description
Transfer Files between a vEdge and Cisco Catalyst SD-WAN Manager	Describes how to transfer files between a remote vEdge and a local Cisco SD-WAN Manager through CLI.
Understand the Web Certificate For Cisco Catalyst SD-WAN Manager	Describes the difference between the Web Certificate and the Controller Certificates on the Cisco Catalyst SD-WAN solution. This document also explains in detail the Web Certificate and clarifies the use between these two types of certificates.
Upgrade Cisco Catalyst SD-WAN cEdge Router with the Use of CLI or Cisco Catalyst SD-WAN Manager	Describes the process to upgrade or downgrade an SD-WAN cEdge (Cisco Edge) router in Controller mode from the Command Line (CLI) and from Cisco SD-WAN Manager.
Verify APIs Used by vManage to Gather Statistics	Describes how to get a specific API call used by Cisco Catalyst SD-WAN Manager to gather statistics from the overlay.
Activate Debugs in vManage	This video provides the steps to activate debugs in Cisco Catalyst SD-WAN Manager
Manual Certificate Renewal on SD-WAN Controller	This video provides the steps to get controllers certificates renewal.
Troubleshoot software image expansion failure due to lack of bootflash space	Describes how to verify that a device successfully expanded a software image file when changing from Autonomous mode to Controller mode. It indicates how to troubleshoot if the expansion was not successful.

Submit feedback for a support document

Procedure

Step 1 Provide feedback using the **Feedback** button located at the right panel of the corresponding article.

The document owner will be notified and will either update the article or flag it for removal.

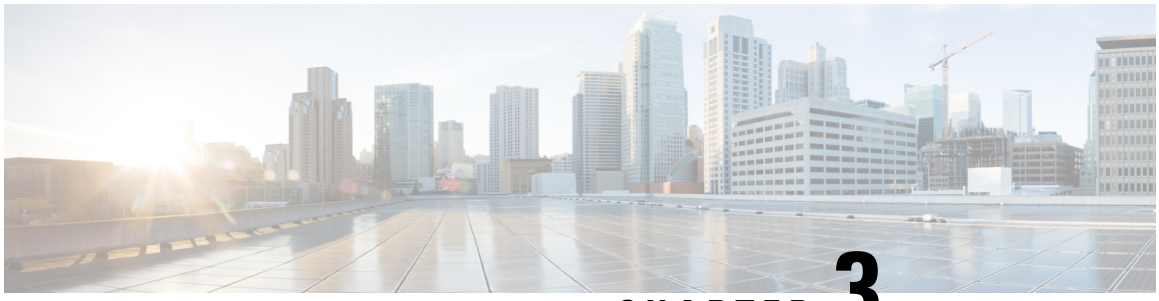
Step 2 Include information regarding the section, area, or issue you had with the document and what could be improved.

Provide as much detail as possible to help the document owner understand and address your feedback.

After submitting feedback, the document owner will review your input and may update the article or flag it for removal based on your suggestions.

Disclaimer and caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



CHAPTER 3

Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS

Table 9: Feature History

Feature Name	Release Information	Description
Unified Debug Condition To Match IPv4 and IPv6 Over MPLS	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature introduces a debug condition to identify and resolve issues related to matching IPv4 and IPv6 traffic over an MPLS network.

- Information About the Unified Debug Condition, on page 35
- Restrictions of the Unified Debug Condition, on page 36
- Use Cases for the Unified Debug Condition, on page 36
- Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI, on page 36
- Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS, on page 38

Information About the Unified Debug Condition

The Cisco IOS XE Catalyst SD-WAN devices support the ability to add a debug condition for IPv4 and IPv6 traffic over MPLS packets. You can specify a filter condition to select the overlay IP address and optionally, the underlay MPLS label with a stack depth. Use the unified debug condition to troubleshoot MPLS networks by identifying specific packets that match certain filtering criteria and troubleshoot any issues related to the MPLS traffic to ensure that your network runs smoothly. The matching of IPv4 and IPv6 over MPLS is a three step process:

1. Debugging
2. Specifying the filtering conditions
3. Applying the filer conditions to the devices

In Cisco IOS XE Catalyst SD-WAN devices, the MPLS label is used to represent an IP VRF and is distributed by OMP protocol.

Restrictions of the Unified Debug Condition

- The debug condition for IPv4 and IPv6 over an MPLS network is supported only using the device CLI.
- Cisco SD-WAN Manager doesn't display the filtered debugging results as part of the packet trace debugging output.
- You can't enable the debug condition to match IPv4 traffic over MPLS and IPv6 traffic over MPLS at the same time.
- You can match only one MPLS label with either IPv4 or IPv6 traffic.
- The number of configurable Feature Invocation Array (FIA) entries per array is 31.

Use Cases for the Unified Debug Condition

The following are the use cases for matching IPv4 and IPv6 traffic over an MPLS network using a debug condition:

- Debugging conditions can help troubleshoot connectivity or performance issues in the network. By matching specific IPv4 and IPv6 traffic over the MPLS network, administrators can isolate the traffic that is causing the issue and analyze the behavior in more detail.
- Debugging conditions can also be useful for implementing QoS policies on the network. By matching specific IPv4 and IPv6 traffic over the MPLS network, administrators can apply different QoS policies to different types of traffic based on their characteristics, such as bandwidth requirements, latency sensitivity, or priority.

Debug to Match IPv4 and IPv6 Traffic Over MPLS Using the CLI

Use the **debug platform condition mpls match-inner** command to match IPv4 and IPv6 traffic over MPLS using various filtering conditions such as *match-inner ipv4*, *match-inner ipv6*, and *allow-no-label*. Specify the MPLS label information, inner IPv4 and IPv6 address based on the debugging requirement.

1. Debug the MPLS network.

   ```
   debug platform condition mpls
   ```

2. Specify the debugging conditions as per your requirement.
   - Use the following condition to debug IPv4 traffic over an MPLS network without specifying the MPLS label:

     ```
     match-inner ipv4
     ```

   - Use the following condition to debug IPv6 traffic over an MPLS network without specifying the MPLS label:

     ```
     match-inner ipv6
     ```

- Use **allow-no-label** condition to match IPv4 or IPv6 packets irrespective of the MPLS labels being encapsulated or not. Use the allow-no-label condition when you want the decapsulated router traffic from the MPLS network to be transmitted as IPv4 or IPv6 packets:

  match-inner ipv4 *{ipv4-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

  or

  match-inner ipv6 *{ipv6-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

- Specify the MPLS label and depth to filter IPv4 packets flowing through a particular MPLS interface:

  [interface *interface-name interface-number*] **mpls** *depth-of-mpls-label* **match-inner ipv4** *{ipv4-source-prefix | any | host | payload-offset | protocol}{ipv4-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

- Specify the MPLS label and depth to filter IPv6 packets flowing through a particular MPLS interface:

  [interface *interface-name interface-number*] **mpls** *depth-of-mpls-label* **match-inner ipv6** *{ipv6-source-prefix | any | host | payload-offset | protocol}{ipv6-destination-prefix | any | host}* **{application | both | ingress | egress}[bidirection] [allow-no-label]**

3. Exit the privileged EXEC mode:

   exit

Examples

The following example shows how to use the debug condition **debug platform condition mpls** command to enable matching of IPv4 or IPv6 traffic over MPLS networks :

```
Device# debug platform condition mpls match-inner ipv4
Device# debug platform condition mpls match-inner ipv4 any any
Device# debug platform condition mpls match-inner ipv4 any any both
Device# debug platform condition mpls match-inner ipv4 any any both allow-no-label
```

For more information see, debug platform condition mpls command page.

The following example shows how to use the debug condition **debug platform condition interface mpls** command to enable matching of IPv4 or IPv4 traffic over MPLS networks for a specific interface:

```
Device# debug platform condition interface
Device# debug platform condition interface Loopback 3 mpls
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888 any both
Device# debug platform condition interface Loopback 3 mpls match-inner ipv6 host
2001:db8:3333:4444:5555:6666:7777:8888 any both allow-no-label
```

Verify the Unified Debug Condition to Match IPv4 and IPv6 Traffic Over MPLS

Verify the Debug State

The following is a sample output from the **show platform conditions** command:

```
Device# show platform conditions

Conditional Debug Global State: Start

Conditions
     Direction
-------------------------------------------------------------------------------------------|---------
All Interfaces                          & MPLS [ALL LABEL] & IPV4 Filter [ALL PROTO] [host
 10.20.24.17] [host 10.20.25.16] both bi



Feature Condition       Type                      Value
----------------------|-----------------------|-------------------------------------------------------



Feature      Type           Submode
                                Level
---------|---------|-------------------------------------------------------------------------|-------
```

In this output, **Conditional Debug Global State: Start** indicates that the debugging is enabled. You can verify the debug filter configuration as well.

Packet Trace Statistics

The following is a sample output from the **show platform packet-trace statistics** command:

```
Device# show platform packet-trace statistics
Packets Summary
  Matched  2
  Traced   2
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     0
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0             0             0
TCP              0             0             0
UDP              0             0             0
IP               0             0             0
IPV6             0             0             0
ARP              0             0             0
```

```
          PKT_DIR_OUT
              Dropped       Consumed       Forwarded
INFRA               0              0               0
TCP                 0              0               0
UDP                 0              0               0
IP                  0              0               0
IPV6                0              0               0
ARP                 0              0               0
```

In this output, **Matched** and **Traced** indicates the number of matched and traced packets.

Decode the IPv4 and IPv6 Matching over MPLS

The following is a sample output from the **show platform packet-trace** *packet 0* **decode** command:

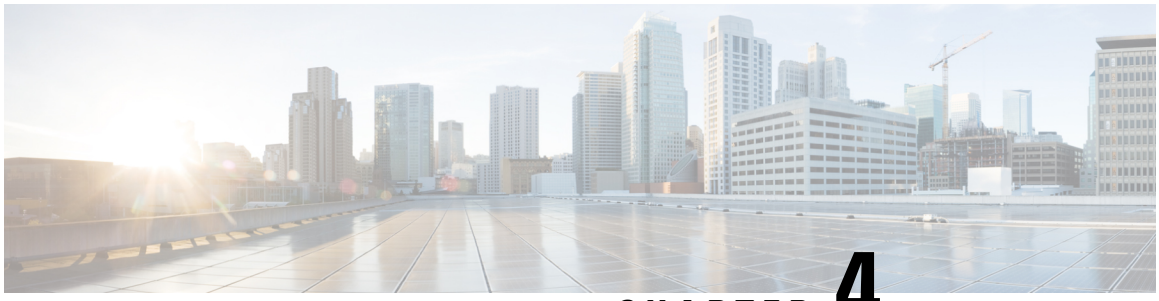
```
Device# show platform packet-trace packet 0 decode
Packet: 0 CBUG ID: 39872
Summary
Input : GigabitEthernet5
Output : GigabitEthernet1
State : FWD
Timestamp
Start : 10090556741529 ns (12/02/2022 05:54:03.730220 UTC)
Stop : 10090556747391 ns (12/02/2022 05:54:03.730226 UTC)
Path Trace
Feature: MPLS(Output)
Input : GigabitEthernet5
Output : Tunnel1
Label Stack Entry[1]: 0x003eb17f
StackEnd:YES, TTL:127, EXP:0, Label:1003, is SDWAN:YES
SDWAN Proto: IPV4, SDWAN dst_vpn: 1
Feature: MPLS_OUTPUT_L2_REWRITE
Entry : Output - 0x81323e6c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 239 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x81499d88
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 33 ns
Feature: MPLS_OUTPUT_FRAG
Entry : Output - 0x814cdb3c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 152 ns
Feature: SDWAN_LOSS_PROTECT_TX
Entry : Output - 0x814d962c
Input : GigabitEthernet5
Output : Tunnel1
Lapsed time : 15 ns
Feature: MPLS_SDWAN_TUNNEL_OUTPUT_FINAL
Entry : Output - 0x814d60cc
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 157 ns
Feature: SDWAN_TUNNEL_PRE_CHK_LKUP
Entry : Output - 0x814d911c
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 19 ns
Feature: SDWAN_TUNNEL_PRE_QOS_OUTPUT
Entry : Output - 0x814d956c
Input : GigabitEthernet1
```

```
Output : Tunnel1
Lapsed time : 70 ns
Feature: SDWAN_TUNNEL_OUTPUT_UNIFY_FNF_FINAL
Entry : Output - 0x814aaa68
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 95 ns
Feature: IPV4_OUTPUT_IPSEC_SDWAN_FEATURE
Entry : Output - 0x814c7480
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 101 ns
Feature: IPV4_OUTPUT_IPSEC_CLASSIFY
Entry : Output - 0x814c7438
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 151 ns
Feature: IPV4_IPSEC_FEATURE_RETURN
Entry : Output - 0x814c7478
Input : GigabitEthernet1
Output : Tunnel1
Lapsed time : 35 ns
Feature: IPV4_TUNNEL_PRE_GOTO_OUTPUT
Entry : Output - 0x814d60c4
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 461 ns
Feature: CBUG_OUTPUT_FIA
Entry : Output - 0x81499d68
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 35 ns
Feature: IPV4_VFR_REFRAG
Entry : Output - 0x814c894c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 33 ns
Feature: DEBUG_COND_APPLICATION_OUT_CLR_TXT
Entry : Output - 0x81499d74
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 11 ns
Feature: IPV4_OUTPUT_L2_REWRITE
Entry : Output - 0x81323e50
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 53 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x81499d88
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 34 ns
Feature: DEBUG_COND_APPLICATION_OUT
Entry : Output - 0x81499d78
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 11 ns
Feature: IPV4_OUTPUT_FRAG
Entry : Output - 0x814c78e8
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 44 ns
Feature: IPV4_OUTPUT_DROP_POLICY
Entry : Output - 0x814d16b8
```

```
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 247 ns
Feature: IPV4_OUTPUT_SDWAN_FNF_FINAL
Entry : Output - 0x814aaa4c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 74 ns
Feature: DEBUG_COND_OUTPUT_PKT
Entry : Output - 0x81499d8c
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 24 ns
Feature: MARMOT_SPA_D_TRANSMIT_PKT
Entry : Output - 0x814df374
Input : GigabitEthernet1
Output : GigabitEthernet1
Lapsed time : 780 ns
Packet Copy In
003eb17f 4500002a 0eb70000 7f11ed0a 10000001 30000001 a2c42710 00160000
801296c3 9baf96f9 9b56c437 0aca
Unable to decode layer 2 trying to skip to layer 3
MPLS
Label Stack Entry[1]
TTL : 127
Label : 1003
EXP : 0
StackEnd : YES
SDWAN : YES
SDWAN Label : 1003
SDWAN Proto : IPV4
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 42
Identifier : 0x0eb7
IP Flags : 0x0
Frag Offset : 0
TTL : 127
Protocol : 17 (UDP)
Header Checksum : 0xed0a
Source Address : 10.0.0.1
Destination Address : 10.0.0.1
UDP
Source Port : 41668
Destination Port : 10000
Length : 22
Checksum : 0x0000
Decode halted - unsupported udp port number
Packet Copy Out
52540095 dbed5254 007ffb83 08004500 0046ab1a 4000ff2f 9d4d0a01 0f0f0a01
10100000 8847003e b17f4500 002a0eb7 00007f11 ed0a1000 00013000 0001a2c4
27100016 00008012 96c39baf 96f99b56 c4370aca
ARPA
Destination MAC : 5254.0095.dbed
Source MAC : 5254.007f.fb83
Type : 0x0800 (IPV4)
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 70
Identifier : 0xab1a
```

```
IP Flags : 0x2 (Don't fragment)
Frag Offset : 0
TTL : 255
Protocol : 47 (GRE)
Header Checksum : 0x9d4d
Source Address : 10.0.0.1
Destination Address : 10.0.0.1
GRE ver 0
Optional Fields : None
Strict Source Route : NO
Recursion Control : 0
Flags : 0x00
Protocol : 0x8847 (MPLS)
MPLS
Label Stack Entry[1]
TTL : 127
Label : 1003
EXP : 0
StackEnd : YES
SDWAN : YES
SDWAN Label : 1003
SDWAN Proto : IPV4
IPv4
Version : 4
Header Length : 5
ToS : 0x00
Total Length : 42
Identifier : 0x0eb7
IP Flags : 0x0
Frag Offset : 0
TTL : 127
Protocol : 17 (UDP)
Header Checksum : 0xed0a
Source Address : 10.255.255.255
Destination Address : 10.255.255.254
UDP
Source Port : 41668
Destination Port : 10000
Length : 22
Checksum : 0x0000
Decode halted - unsupported udp port number
```

In this example, **Source Address** and **Destination Address** indicate that the debugging condition is successful. The **MPLS** section displays the SD-WAN labels specified.



CHAPTER 4

Collecting System Information in an Admin-Tech File

- Feature history: Admin-tech file, on page 43
- Collecting system information using an admin-tech file, on page 45
- Generate admin-tech files, on page 46
- View admin-tech files, on page 48
- Upload an admin-tech file to a TAC case, on page 48

Feature history: Admin-tech file

Table 10: Feature history

Feature Name	Release Information	Description
Admin-Tech Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enhances the admin-tech file to include commands like **show tech-support memory**, **show policy-firewall stats platform**, **show sdwan confd-log netconf-trace** and so on in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.
Generate System Status Information for a Cisco SD-WAN Manager Cluster Using Admin Tech	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature adds support for generating an admin-tech file for a Cisco SD-WAN Manager cluster. The admin-tech file is a collection of system status information intended for use by Cisco Catalyst SD-WAN Technical Support for troubleshooting. Before this feature was introduced, Cisco Catalyst SD-WAN was only able to generate an admin-tech file for a single device.

Feature Name	Release Information	Description
View Generated Admin-Tech Files at Any Time	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides support for viewing the generated admin-tech files whenever the admin-tech files are available on a device. You can view the list of generated admin-tech files and then decide which files to copy from your device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.
Additional Diagnostics Information Added to Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests from Cisco SD-WAN Manager. This streamlines the steps required for working with TAC to troubleshoot a problem.
Generate an Admin-Tech File with the Feature Filter	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds new options for information to include in the admin-tech file. For Cisco IOS XE Catalyst SD-WAN devices, you can include information about IPsec and security policy. For Cisco Catalyst SD-WAN Control Components, you can include information about the forwarding information base and routing information base.
Include Custom CLI Command Output in an Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can include the output of specific **show** commands in an admin-tech file. This is helpful for troubleshooting.
Cellular Modem Auto-Collect Crash Data	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	You can use the **lte modem crash-action auto-collect** command to configure a router to collect essential information about cellular modem operation, ensuring that the admin-tech file contains necessary details for troubleshooting in the event of an LTE modem crash.

Collecting system information using an admin-tech file

An admin-tech file is a collection of system status information used for troubleshooting a given issue. Send your Cisco SD-WAN Manager admin-tech files to Cisco Catalyst SD-WAN Technical Support to resolve your issue.

You can generate an admin-tech file for a single device or for all the nodes in a SD-WAN Manager cluster.

Note Starting from Cisco vManage Release 20.7.1, the admin-tech file includes additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.

Note The admin-tech generation fails if any malformed characters are present in the disk.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, the generation of admin tech in Cisco SD-WAN Manager fails when disk space usage exceeds the designated limits. When the total utilized space surpasses the limit, you may attempt to delete the existing admin tech data from Cisco SD-WAN Manager.

If this action is ineffective, or if there are no admin tech files available for deletion, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total utilized space at /opt/data/ remains below 80% and can attempt to delete admin tech across tenants in a multi-tenant setup.

Benefits collecting system information using an admin-tech file

- Provides a consolidated file with system status information to submit to Cisco Catalyst SD-WAN Technical Support for diagnostics and troubleshooting.
- Provides support for directly uploading admin-tech files to Cisco Catalyst SD-WAN Technical Support

Prerequisites for collecting system information using an admin-tech file

All of the nodes in the Cisco SD-WAN Manager cluster must be in a healthy state to generate an admin-tech file for all of the nodes in the cluster.

Restrictions for collecting system information in an admin-tech file

- All in-progress admin-tech requests are purged every three hours.
- You can have only one outstanding admin-tech request for an SD-WAN Manager cluster at a time. A second admin-tech request fails if there is an existing admin-tech request.

- Creating an admin-tech file for an SD-WAN Manager cluster is successful only if an admin-tech request is not running for individual devices.

Generate admin-tech files

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. Do one of the following:
   - To generate an admin-tech file for all the nodes in a SD-WAN Manager cluster, click **Generate Admin Tech for Manager**.
   - To generate an admin-tech file for a single device, click ... adjacent to the device and choose **Generate Admin Tech for Manager**.
3. In the **Generate admin-tech File** pane, choose the content to include in the admin-tech tar file, as follows:

Field	Description
Logs	Include log files. **Note** The log files are stored in the `/harddisk/tracelogs` directory on the local device.
Core	Include core files. **Note** The core files are stored in the `/harddisk/core` directory on the local device.

Field	Description
Tech Features	**Note** From Cisco Catalyst SD-WAN Manager Release 20.15.1, this field is no longer available. This option is available in SD-WAN Manager Releases 20.13.x and 20.14.x. Choose additional information to include in the admin-tech file. The options depend on whether you are generating an admin-tech file for a single Cisco IOS XE SD-WAN device or for all devices and SD-WAN Control Components. For Cisco IOS XE Catalyst SD-WAN devices: • **IPsec**: Include IPsec information. • **Security Policy**: Include security policy information. The technical information for the features is stored in a separate tech files in the folder /var/tech/ directory. By default, the admin file collects the technical information for IPsec and security features. The feature specific technical files are named as /var/tech/ipsec and /var/tech/security. For Cisco SD-WAN Control Components: • **All**: Include forward information base and route information base details. **Include fib detail**: Include forwarding information base details. **Include rib detail**: Include routing information base details.
Use Custom Commands	(Optional) Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 Enter **show** commands, separated by commas, to include **show** command output in the admin-tech file. The command output is available in the `/var/tech/custom` file path in the admin-tech zip file. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, some OMP and TTM commands are not supported. If you enter an unsupported command, the admin-tech file displays an error.

4. Click **Generate**.

   SD-WAN Manager creates the admin-tech file.

   The file name has the format *date-time*-admin-tech.tar.gz.

By default, the admin-tech file collects the technical information for IPsec and security features. The feature-specific technical files are named as `/var/tech/ipsec` and `/var/tech/security`.

View admin-tech files

You can perform any of the following operations after the admin-tech file is generated:

- View the list of the generated admin-tech files.
- Copy the selected admin-tech files from your device to Cisco SD-WAN Manager.
- Download the selected admin-tech files to your local device.
- Delete the selected admin-tech files from Cisco SD-WAN Manager, the device, or both.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **. . .** and choose **View Admin Tech List**.

   A tar file appears that contains the admin-tech contents of the device that you selected earlier. This file has a name similar to *ip-address-hostname*-20210602-032523-admin-tech.tar.gz, where the numeric fields are the date and the time.

   You can view the list of the generated admin-tech files and decide which files that you want to copy to SD-WAN Manager.
3. Click the **Copy** icon to copy the admin-tech file from the device to SD-WAN Manager.

   A hint appears letting you know that the file is being copied from the device to SD-WAN Manager.
4. After the file is copied from the device to SD-WAN Manager, you can click the **Download** icon to download the file to your local device.

   You can view the admin-tech file size after the file is copied to SD-WAN Manager.
5. After the admin-tech file is successfully copied to SD-WAN Manager, you can click the **Delete** icon and choose which files to delete from SD-WAN Manager, the device, or both.

Upload an admin-tech file to a TAC case

From Cisco vManage Release 20.7.1, Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, and Cisco SD-WAN Release 20.7.1, you can upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case.

Before you begin

Ensure that you have generated admin-tech files from Cisco SD-WAN Manager.

Upload an admin-tech file to a TAC case

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. After you generate **Admin-Tech** files, click **Show Admin Tech List**.

The **List of Admin-techs** window is displayed.

3. From the list of Admin-tech files, select the admin-tech file and click **Upload**.
4. In the **SR Number** and **Token** fields, enter the details.
5. Choose the **VPN** from the VPN options. The options are VPN 0 and VPN 512.
6. Click **Upload**.

   The selected admin-tech file is uploaded to the relevant service request.