Performing Path Traces

- About Path Trace, page 1
- Performing a Path Trace, page 13
- Collecting QoS and Interface Statistics in a Path Trace, page 15

About Path Trace

With Path Trace, the controller reviews and collects network topology and routing data from discovered devices. Then it uses this data to calculate a path between two hosts or Layer 3 interfaces. Optionally, you can choose to collect interface and QoS statistics for a path. You can use the information gathered through Path Trace to monitor and debug traffic paths that are distributed among the various devices throughout your network.

You perform these tasks by running a path trace between two nodes in your network. The two nodes can be a combination of wired or wireless hosts and/or Layer 3 interfaces. In addition, you can specify the protocol for the controller to use to establish the path trace connection, either TCP or UDP.

At every node in the path, the controller reports information about the device and path. For example, if a Layer 2 protocol is used to discover a node, the controller reports that the path is a switched path and labels it as **Switched**. If the controller detects load balancing decisions being made on a discovered device, it reports the path as an ECMP path and labels it as **ECMP**. Path trace can identify the following information about the devices and paths:

- HSRP
- SVI
- Layer 2
- Layer 2 Port Channel
- Layer 3 Routing Protocol
- ECMP/TR
- Netflow
- ECMP over SVI
- Subinterface

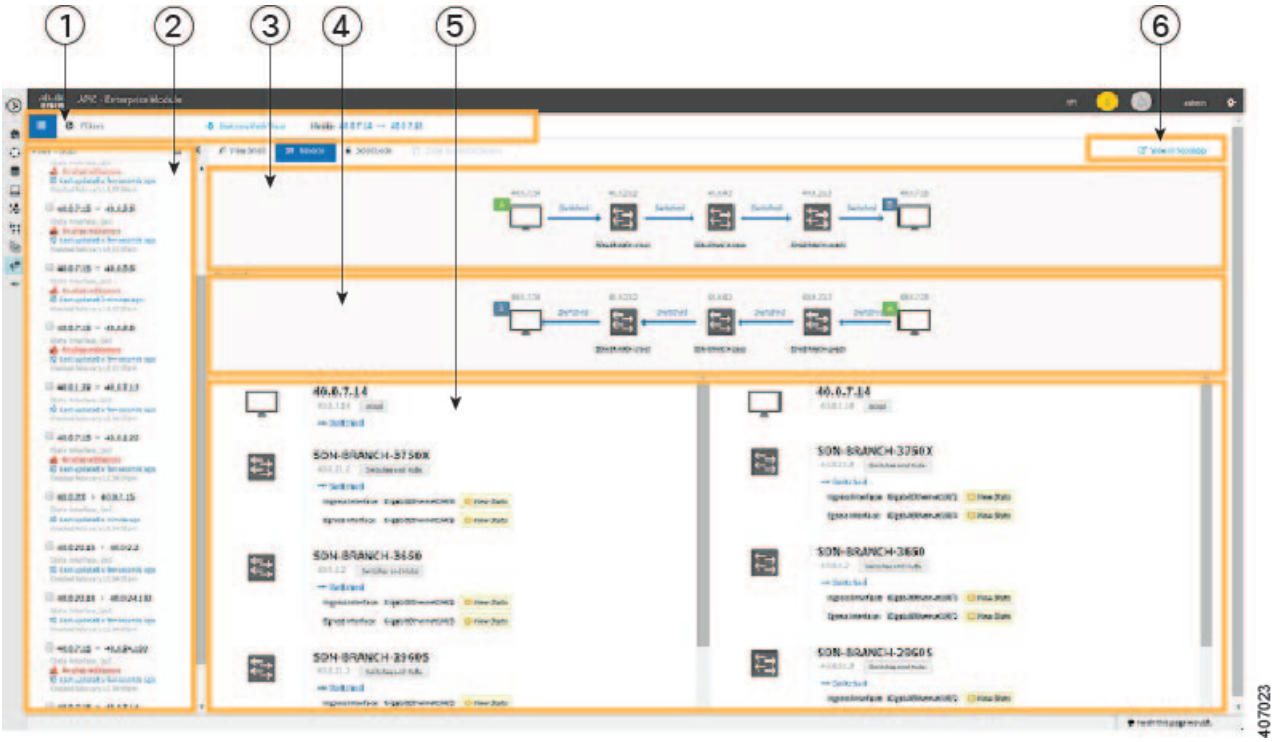
- EIGRP
- Level 3 Recursive Loop

For nodes that are unknown devices within a path trace (usually non-Cisco devices), the controller calculates the path between the unknown devices starting from the last known Cisco device (from the **Host Source IP**) to the next, neighboring Cisco device (sometimes the **Destination Source IP**). The collected IP address data about the unknown device is then sent from this neighboring Cisco device to the controller to calculate the trace path. The unknown device is displayed in the controller's GUI as a question mark (?).

Note In certain circumstances, a path trace may flow between one of two (or more) devices. To determine which device actually received the flow for the path trace, the controller reads the NetFlow configurations and records on the devices (if they exist). By reading this data from the devices, the controller can determine the likelihood of the actual path.

To access the **Path Trace** window, from the Navigation pane, click **Path Trace**.

Figure 1: Path Trace Window



Callout Number	Name	Description
1	**Toolbar**	Provides the following functions: • **Path Traces List** icon—Toggles the display of the list of completed path traces. You can delete path traces that you no longer need by placing your cursor over the path trace and clicking the **Trash Can** icon. • **Filters**—Allows you to search for devices by source or destination IP address. • **Start new Path Trace**—Displays a dialog box for you to specify the parameters of the path trace and then start the trace. You must enter the source and destination IP address for the path trace. Optionally, you can specify whether to refresh the path trace every 30 seconds and whether to collect QoS and interface statistics. Additional options allow you to specify the source and destination ports and the protocol (TCP or UDP). • **Hosts**—Displays the IP addresses of the source and destination devices for the current path trace.
2	**In-progress, Active, and Completed Path Traces**	In-progress path traces are those that have not completed yet. Active path traces are completed and being updated once every 30 seconds. Completed path traces are calculated once and are not updated.
3	**Trace Results Graphical Display**	Displays the results of the path trace. For information, see Understanding Path Trace Results, on page 8.
4	**Reversed Results Graphical Display**	Shows the path trace in reverse order, from the destination host to the source host. For information, see Understanding Path Trace Results, on page 8.
5	**Trace Results Device Details**	Provides detailed information about the devices along the path. For information, see Understanding Path Trace Results, on page 8.
6	**View in Topology** button	Displays the trace results in the **Topology** window.

Path Trace Support

Cisco APIC-EM can perform path trace calculations for both campus and WAN networks based on physical connectivity and the protocols used by devices within the path. Specifically, the Cisco APIC-EM supports path traces through the following networking environments:

- Campus/data center to campus/data center

- Campus/data center to branch
- Branch to campus/data center
- Branch to branch

Note If the controller can not complete a path trace for the selected hosts or interfaces, it displays the results of a partial trace.

Path Trace Protocols and Network Connections

The following table describes the supported device protocols and network connections (physical, wireless, and virtual) for a Cisco APIC-EM path trace.

Note For detailed information about protocol, wireless, and AP support by platform and scenario, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Table 1: Path Trace Supported Device Protocols and Network Connections

Supported Device Protocols and Network Connections	Description
Border Gateway Protocol (BGP)	When BGP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Equal Cost Multi Path (ECMP)	When an ECMP routing strategy is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made. **Note** The controller's GUI will display when ECMP is used between devices in a path trace segment.

Supported Device Protocols and Network Connections	Description
Hot Standby Router Protocol (HSRP)	When HSRP is used in a network, the controller automatically looks up the HSRP active router for a given segment and calculates the path appropriately for a path trace. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Intermediate System-to-Intermediate System (IS-IS) Protocol	When IS-IS is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Layer 3 Forwarding Interface	The controller can perform path traces between two Layer 3 forwarding interfaces or between a Layer 3 forwarding interface and a host.
MPLS-VPN (WAN)	The controller provides path trace support for a branch-to-branch connected and provider-managed MPLS-VPN service. Supported devices for this type of path trace include: • Cisco ASR 1000 Series Aggregation Services Router • Cisco ASR 9000 Series Aggregation Services Router • Cisco Integrated Services Routers (ISR) G2 All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers. **Note** The above supported devices will be tagged as **Border Routers** for their **Device Role** in the **Device Inventory**. You must keep the above supported devices tagged as **Border Routers** when performing a path trace. The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.

Supported Device Protocols and Network Connections	Description
Open Shortest Path First Protocol (OSPF)	When OSPF is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Physical connectivity (Ethernet, Serial and Packet over SONET (PoS))	The path trace for a given application flow can be displayed over Ethernet, Serial over SONET, and Packet over SONET. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Spanning Tree Protocol (STP)	The controller provides Layer 2 support for Spanning Tree Protocol (STP). The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Static Routing	When static routing is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Virtual connectivity—Layer 2 Port Channel	When virtual connectivity (Layer 2 port channel) is used within a network, the path trace for a given application flow is displayed. The path trace over virtual interfaces (port channels) is displayed, so that the user can visualize an end-to-end path for an application.
Virtual connectivity—VLAN/SVI	When virtual connectivity (VLAN/SVI) is used within a network, the path trace for a given application flow is displayed. The path trace is displayed, so that the user can visualize an end-to-end path for an application. The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.

Supported Device Protocols and Network Connections	Description
Wireless	The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility. When wireless network elements are used, the path trace for a given application flow is displayed. The user knows the exact path a particular application is taking. **Note** The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace. The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Equal Cost Multipath/Trace Route (ECMP/TR)	When ECMP/TR is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained on demand by polling the device. When performing a path trace on ECMP, Cisco Express Forwarding (CEF) lookup is performed on the device on demand for requested tuples. When a path trace detects a number of unknown or unmanaged devices in the path, the path trace is executed on demand from the last known or managed Cisco device and the path calculation is restarted from the first known or managed Cisco device in the trace route result. The unknown or unmanaged hops discovered using path trace are added to the path as unknown devices along with their IP addresses.
Netflow	When Netflow is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. When we have multiple border routers in the destination island, the Netflow cache from the devices are used to find the actual ingress border router. The Netflow record is matched from these devices on demand for a given tuple. It is essential to configure Netflow on the border routers. If Netflow is not configured, trace route is used to find the ingress interfaces, which might not be accurate.

Supported Device Protocols and Network Connections	Description
Sub interfaces	When sub interfaces are used within a network, the path trace for a given application flow is displayed. The path trace between the two sub interfaces is displayed, so that the user can visualize an end-to-end path for an application.
Enhanced Interior Gateway Routing Protocol (EIGRP)	When EIGRP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Layer 3 Recursive Lookup	When Layer 3 Recursive Lookup is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. Up to three recursive lookups are supported. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.

Understanding Path Trace Results

After you run a path trace, the results are displayed in the **Trace Results Graphical Display** pane.

Path Traces Pane

The Path Traces pane lists the path traces in one of three categories:

- **IN PROGRESS—** Path is currently being calculated. No results to show yet.
- **ACTIVE—**A path has been calculated and will be refreshed every 30 seconds. Statistics may also be collected periodically.
- **COMPLETED—**The path has been calculated one time and is not being refreshed. However, statistics may still be collected periodically.

Trace Results Graphical Display

At the top of the **Trace Results Graphical Display** pane, the toolbar provides buttons for adjusting the path trace display.

Table 2: Trace Results Toolbar

Name [1]	Description
View Small	Minimizes the trace results to view the details better.
Show Reverse	Displays the trace results from the host destination IP to the host source IP. The reverse path trace graphic is displayed directly below the original path trace. The reverse path trace details are displayed to the right of the original path trace details.
Scroll Lock	Locks the scrolling of the path trace and reverse path trace details windows. (Available when **Show Reverse** is enabled.)
Show Duplicate Devices	Displays or hides duplicate devices within a path trace.
View in Topology	Opens the **Topology** window and highlights the path trace results in your network topology. For more information about using the Topology window, see About Topology.

1 Depending on the trace results, some of these items on the toolbar might be unavailable.

The controller graphically displays the path direction and the devices and networks that the path traverses. The following information is also provided:

- Hosts and devices (including their IP addresses) on the path trace between the source (host A) and destination (host B).
- **Link Source—**Whether the path source between devices is either **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.

Note Clicking an individual device in the path trace highlights the device in the **Trace Results Device Details** area.

Trace Results Device Details

You can review the detailed information displayed for each device in the path trace.

Table 3: Trace Results Device Details

Name	Description
IP	IP address of the device.

Name	Description
Type	Wired or wireless device (access point, switch, or router).
Link Source	Information about the link between two devices (source and destination). Link information is based on the configuration of the source device. • **BGP—**Link is based on the BGP routes configured on the source device. • **ECMP—**Link is based on a Cisco Express Forwarding (CEF) load balancing decision. • **EIGRP—** Link is based on EIGRP routes configured on the source device. • **Connected—**The source host (host A) is directly connected to the destination host (host B). In the case of a reverse path, the destination host (host B) is directly connected to the source host (host A). • **InterVlan Routing—**There is an SVI configuration on the source device. A VLAN is configured on the source device from which the path is switched to the destination device. • **ISIS—**Link is based upon the IS-IS routes configured on the source device. • **NetFlow—**Link is based on NetFlow records collected on the source device. • **OSPF—**Link is based on the OSPF routes configured on the source device. • **Static—**Link is based on a static route configured on the source device. • **Switched—**Link is based on Layer 2 VLAN forwarding. • **Trace Route—**Link is based on trace route. • **Wired—**The source device is wired to the destination device. • **Wireless—**The source device is a wireless host connected to the destination device (access point).
Tunnels	CAPWAP data (wireless) or mobility tunneling **Note** Path trace provides a graphical view of the CAPWAP tunnel around the devices involved. You are able to adjust the view by zooming in or out.

Name	Description
Ingress interface	Ingress interface of the device for the path trace (physical or virtual). For example, a physical ingress interface is **GigabitEthernet1/0/1** and a virtual ingress interface is **GigabitEthernet1/3 [Vlan1]**. If statistics were gathered for this path trace, clicking the **View Stats** button displays the interface or QoS statistics. For information, see Understanding the Interface Statistics Retrieved During a Path Trace, on page 11 or Understanding the QoS Statistics Retrieved During a Path Trace, on page 13.
Egress interface	Egress interface of the device for the path trace (physical or virtual). For example, a physical interface is **GigabitEthernet1/0/2** and a virtual ingress interface is **GigabitEthernet1/4 [Vlan2]**. If statistics were gathered for this path trace, clicking the **View Stats** button displays the interface or QoS statistics. For information, see Understanding the Interface Statistics Retrieved During a Path Trace, on page 11 or Understanding the QoS Statistics Retrieved During a Path Trace, on page 13.
Accuracy note	If there is uncertainty about the path trace on a segment between devices, path trace displays a note that indicates the accuracy of the computed path as a percentage. For example, 10 percent would indicate lower accuracy than 90 percent. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.

Understanding the Interface Statistics Retrieved During a Path Trace

When you perform a path trace, you can collect interface statistics that show how the interfaces are performing. In this way, you can monitor the effect of the QoS policies on the network and make any changes, if necessary. The following table lists the interface statistics that are retrieved.

Table 4: Interface Statistics by Policy

Parameter	Description
Admin Status	Administrative status of the interface: • **Up—**Interface has been enabled through the CLI. • **Down—**Interface has been disabled through the CLI.
Input Packets	Number of packets being received on the interface.

Parameter	Description
Input Queue Drops	Number of packets dropped from the input queue due to the queue reaching its maximum threshold.
Input Queue Max Depth	Maximum number of packets that the input queue can hold before it must start dropping packets.
Input Queue Count	Number of packets in the input queue.
Input Queue Flushes	Number of packets dropped due to Selective Packet Discard (SPD). SPD is a mechanism that quickly drops low priority packets when the CPU is overloaded in order to save some processing capacity for high priority packets.
Input Rate (bps)	Number of bits per second at which packets are entering the interface.
Operational Status	Operational status of the interface: • **Up—**Interface is transmitting or receiving traffic as desired. To be in this state, an interface must be administratively up, the interface link layer state must be up, and the interface initialization must be completed. • **Down—**Interface cannot transmit or receive (data) traffic.
Output Drop	Number of packets dropped from the output queue due to the queue reaching its maximum threshold.
Output Packets	Number of packets leaving the interface.
Output Queue Count	Number of packets in the output queue.
Output Queue Depth	Maximum number of packets that the output queue can hold before it must start dropping packets.
Output Rate (bps)	Number of bits per second at which packets are leaving the interface.
Refreshed At	Date and time that the current statistics were gathered.

Understanding the QoS Statistics Retrieved During a Path Trace

When you perform a path trace, you can collect QoS statistics that show how the QoS policies are performing. The only interface statistics included in the QoS statistics are those for the border router egress interface. Collecting QoS statistics helps you to monitor the effect of the QoS policies on your network devices and make any changes, if necessary. The following table lists the QoS Statistics that are retrieved.

Table 5: QoS Statistics by Policy

Parameter	Description
Policy Name	Drop-down list of policy names that QoS statistics have been collected about.
Class Map Name	Name of the class map.
Num of Bytes	Average number of bytes forwarded by the queue.
Offered Rate	Traffic rate offered for that particular traffic.
Queue Bandwidth (bps)	Rate (bps) at which the queue can process packets.
Queue Total Drops	Number of packets dropped from the queue due to the queue reaching its maximum threshold.
Drop Rate	Number of bits per second at which packets are being dropped from the queue.
Num of Packets	Number of packets that the queue can hold.
Queue Depth	Maximum number of packets that the queue can hold before it must start dropping packets.
Queue No Buffer Drops	Number of times that packets were dropped due to not enough buffer allocated.
Refreshed At	Date and time that the current statistics were gathered.

Performing a Path Trace

You can perform a path trace between two nodes in your network. The two nodes may be two hosts and/or Layer 3 interfaces.

Note The path trace application may display accuracy notes. Accuracy notes are red boxes that appears on a node or path segment indicating the accuracy of the computed path as a percentage. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Ensure that the controller has SSH or Telnet access to the devices.

Procedure

Step 1 In the Navigation pane, click **Path Trace**.

Step 2 From the path trace toolbar, click **Start new Path Trace**.

Step 3 In the **Source** field, enter the IP address of the host or the Layer 3 forwarding interface where you want the trace to start.
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.

Step 4 In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end.
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.

Step 5 (Optional) To configure source and destination ports or protocols, click **More Options**.

Step 6 (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to end.

Step 7 (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.

Step 8 (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.

Step 9 (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.

Step 10 (Optional) To configure the path trace to collect additonal statistics, check the **Stats** check box and any of the following check boxes, as desired:

- **QoS Stats—**Collects and displays information about quality of service.
- **Interface Stats—**Collects and displays information about the interfaces on the devices along the path.

Step 11 Click **Start Trace**.
Review the path trace output. For more information, see Understanding Path Trace Results, on page 8.

Step 12 To view the path trace in the **Topology** window. Click **View in Topology**.
The **Topology** window opens with the path trace highlighted in your network. For more information about the **Topology** window, see About Topology.

Note If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

Collecting QoS and Interface Statistics in a Path Trace

You can perform a path trace between two nodes in your network and collect interface and/or QoS statistics about the devices in the path.

Note The path trace application may display accuracy notes. Accuracy notes are red boxes that appears on a node or path segment indicating the accuracy of the computed path as a percentage. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.

Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 In the Navigation pane, click **Path Trace**.

Step 2 From the path trace toolbar, click **Start new Path Trace**.

Step 3 In the **Source** field, enter the IP address of the host or the Layer 3 forwarding interface where you want the trace to start.
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.

Step 4 In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end.
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.

Step 5 (Optional) To configure source and destination ports or protocols, click **More Options**.

Step 6 (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to end.

Step 7 (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.

Step 8 (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.

Step 9 (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.

Step 10 Check the **Stats** check box.

Step 11 Check one or both of the following check boxes:

- **QoS Stats**
- **Interface Stats**

Step 12 Click **Start Trace**.
The results are displayed in the **Trace Results Device Details** pane. For information, see Understanding the Interface Statistics Retrieved During a Path Trace, on page 11 and Understanding the QoS Statistics Retrieved During a Path Trace, on page 13.

Step 13 (Optional) To view the path trace in the **Topology** window. Click **View in Topology**.
The **Topology** window opens with the path trace highlighted in your network.

Note If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

For more information about the **Topology** window, see About Topology.

What to Do Next

Review the path trace output. For information, see Understanding the Interface Statistics Retrieved During a Path Trace, on page 11 and Understanding the QoS Statistics Retrieved During a Path Trace, on page 13.