Cisco Path Trace Application on APIC-EM User Guide, Release 1.5.0.x

First Published: 2015-11-02

Last Modified: 2017-06-23

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

CONTENTS

Preface

Audience

This publication is intended for experienced network administrators who will configure and maintain the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM). This guide is part of a documentation set that is designed to help you install, troubleshoot, and upgrade your Cisco APIC-EM. For a complete list of the Cisco APIC-EM documentation set, see Related Documentation, on page vii.

Note In this guide, the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to as the controller.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.

Convention	Description
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.

Convention	Description
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS XE software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Related Documentation

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

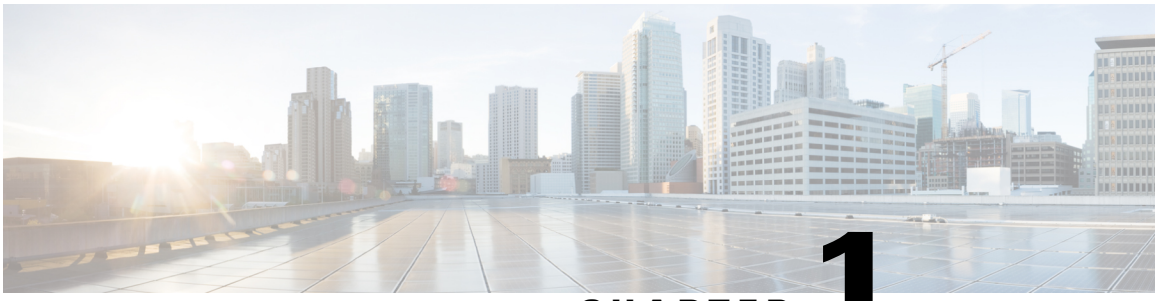
- Cisco APIC-EM Documentation:
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco Network Visibility Application for the Cisco APIC-EM
  - *Cisco Network Visibility Application for APIC-EM Release Notes*
  - *Cisco Network Visibility Application for APIC-EM Supported Platforms*
  - *Cisco Network Visibility Application for APIC-EM User Guide*

- Cisco Path Trace Application for Cisco APIC-EM
  - *Cisco Path Trace Application for APIC-EM Release Notes*
  - *Cisco Path Trace Application for APIC-EM Supported Platforms*
  - *Cisco Path Trace Application for APIC-EM User Guide*
- Cisco EasyQoS Application for Cisco APIC-EM
  - *Cisco EasyQoS Application for APIC-EM Release Notes*
  - *Cisco EasyQoS Application for APIC-EM Supported Platforms*
  - *Cisco EasyQoS Application for APIC-EM User Guide*
- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*
  - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Open Plug-n-Play Agent Configuration Guide*
  - *Mobile Application User Guide for Cisco Network Plug and Play*
- Cisco Active Advisor Documentation for the Cisco APIC-EM:
  - *Cisco Active Advisor for APIC-EM Release Notes*
- Cisco SD-Bonjour Documentation for the Cisco APIC-EM:
  - *Cisco SD-Bonjour Application for APIC-EM Release Notes*
- Cisco Integrity Verification Documentation for the Cisco APIC-EM:
  - *Cisco Integrity Verification Application (Beta) for APIC-EM Release Notes*
  - *Cisco Integrity Verification Application (Beta) for APIC-EM User Guide*

Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the developer.cisco.com/site/apic-em Web site.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.



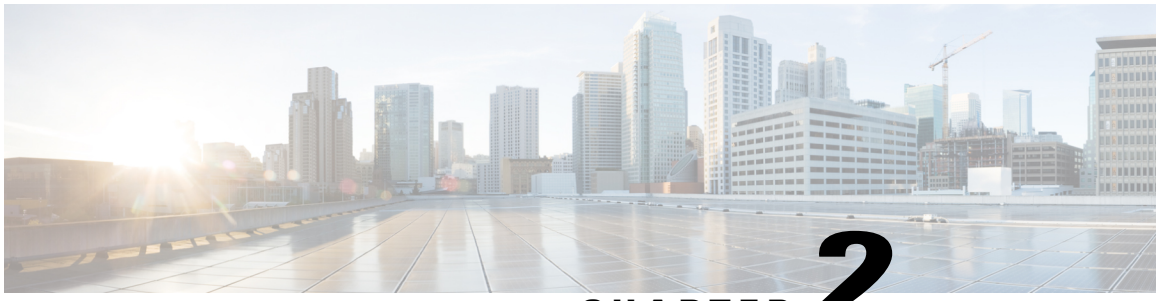
CHAPTER 1

New and Changed Information

New and Changed Information

There are no new Path Trace features in this release.

New and Changed Information



CHAPTER 2

Overview

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (SDN) Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP application is one of the components in the Cisco Network PnP solution. The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.
Cisco Active Advisor	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status
Cisco SD-Bonjour	The Cisco SD-Bonjour application provides controller functions in the network. It enables discovery and distribution of policy-based Cisco SD-Bonjour services, independent of network boundaries.
Cisco Integrity Verification	The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release.

Feature	Description
Cisco Remote Troubleshooter	The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel. As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Logging into the Cisco APIC-EM

You access the Cisco APIC-EM GUI by entering its network IP address in your browser. The IP address was configured for the Cisco APIC-EM network adapter during the initial setup using the configuration wizard. This IP address connects to the external network.

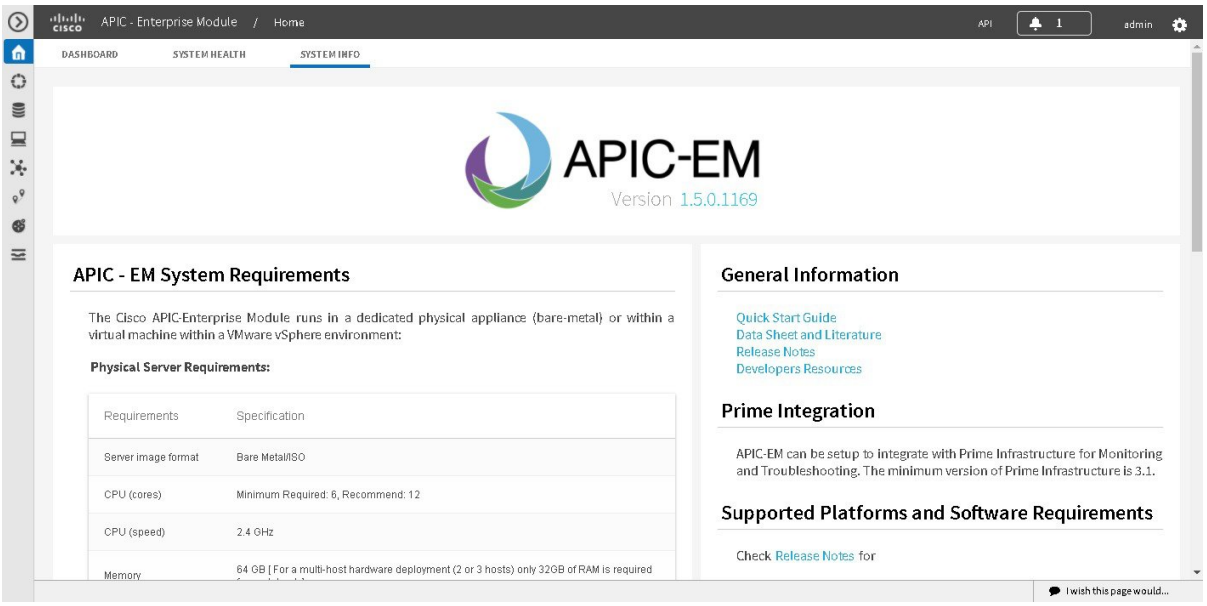
Step 1 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:
https://*IP address*

Step 2 On the launch page, enter your username and password that you configured during the deployment procedure. The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following three tabs:

- **DASHBOARD**

- SYSTEM HEALTH
- SYSTEM INFO

Figure 1: SYSTEM INFO Tab



What to Do Next

Click on each tab and review the data provided in the GUI.

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, QoS, device, and Performance Monitor 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.

Note Path traces from the a router's loopback interface or a wireless controler's management interface are not supported.

Note For devices connected to a voice or video endpoint (for example, Cisco IP phones), you need to enable IP Device Tracking (IPDT) for these devices to discover voice/data VLAN information about the endpoints. For information, see IP Device Tracking Configuration, on page 14.

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**. For a complete list of the protocols and technologies that path trace can identify, see Supported Protocols and Technologies, on page 8.

For 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.

Path Trace also supports unknown destinations, where the device is not managed by the Cisco APIC-EM but is reachable.

After the Cisco APIC-EM performs an initial scan, additional on-going network scans are performed at regular intervals every few minutes. Information captured during the on-going scans are displayed in the **Devices** table. Click **Device Inventory** in the navigation pane to view the **Devices** table. Each time the Cisco APIC-EM performs a scan, it also reads and records access control list, quality of service, and SPAN policy configuration information from the network.

Supported Network Environments

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.

Supported Protocols and Technologies

The following table describes the device protocols, network connections (physical, wireless, and virtual), and features that Path Trace supports.

Note For detailed information about protocol, wireless connection, and feature support by platform and scenario, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Table 2: Path Trace Supported Device Protocols and Network Connections

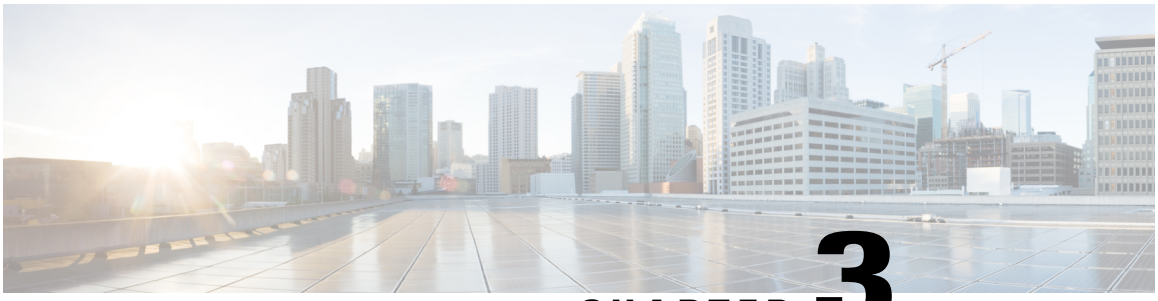
Supported Device Protocols and Network Connections	Description
Access Control List (ACL)	Access Control List (ACL) Trace analyzes how a flow is affected by ACLs programmed on the path. After the path is calculated between the source and the destination, the ACL Trace analyzes both ingress and egress interfaces of all devices on the path. Analysis is independent among the ACLs throughout the path. For example, if an ACL has entries that would deny the traffic on an interface along the path, the results of the analysis are reported as if the traffic had reached the destination without being denied by the ACL. However, analysis of entries within an individual ACL is cumulative. That is, if a higher priority ACE is a match, lower-priority ACEs are ignored.
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.
Dynamic Multipoint VPN (DMVPN)	Path Trace shows DMVPN dynamic tunnels between two spokes by identifying the link information source. For more information, see Understanding DMVPN Path Trace Results, on page 30.
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.

Supported Device Protocols and Network Connections	Description
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.
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.
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.

Supported Device Protocols and Network Connections	Description
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.
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.
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.
Next Hop Resolution Protocol (NHRP)	Path Trace shows DMVPN dynamic tunnels between two spokes by identifying the LinkInformationSource as NHRP.

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.
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.
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
Virtual Routing and Forwarding (VRF)	Path trace supports VRF Lite and VRF route leaking. For information, see Understanding VRF Path Trace Results, on page 31.
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.



CHAPTER 3

Device Configuration Prerequisites

Required Platform Configurations for Path Trace

For certain Path Trace features to work properly, you need to make some changes to the platforms mentioned in the following table.

Table 3: Required Platform Configurations for Path Trace

Platform	Required Configuration
• Cisco ASR 1000 • Cisco ASR 9000 • Cisco ISR-G2 • Cisco ISR-4451 -X	Configure NetFlow on these routers. For information, see Cisco NetFlow Configuration, on page 14.
Devices connected to a voice or video endpoint (for example, Cisco IP phones).	Enable IPDT for these devices to discover voice/data VLAN information about the endpoints. For information, see IP Device Tracking Configuration, on page 14.

Platform	Required Configuration
Devices on which you want Performance Monitor information.	You do not need to make any changes to the devices to run a path trace to gather performance monitor information. Cisco Path Trace does this automatically when you initiate this type of a path trace. For information about the configuration changes that Cisco Path Trace makes, see Performance Monitor Configuration, on page 14.

Cisco NetFlow Configuration

Cisco NetFlow needs to be enabled on the following devices to support the Cisco APIC-EM path trace functionality:

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ISR-G2 Routers
- Cisco ISR-4451 -X

The controller pulls cached NetFlow records from the device for path trace. To enable NetFlow on your devices, refer to your specific device documentation. For general information about Cisco NetFlow technology, see the Cisco IOS Flexible NetFlow Technology Q&A document.

IP Device Tracking Configuration

The Cisco APIC-EM discovery function uses several protocols and methods to retrieve network information, such as hosts IP addresses, MAC addresses, and network attachment points. To use IP Device Tracking (IPDT) for discovery, you must manually enable IPDT on the devices and interfaces for this protocol to be used to collect host information. To enable IPDT on your devices, refer to your specific device documentation. For general information about IPDT, see IP Device Tracking (IPDT) Overview.

Performance Monitor Configuration

When you run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM automatically configures all of the devices in the requested path with the necessary flow monitor commands. The Cisco APIC-EM removes the configuration from the device if there is no corresponding path trace request present or after 24 hours of the path trace request, whichever is first.

The following configuration is sent to each device in the requested path:

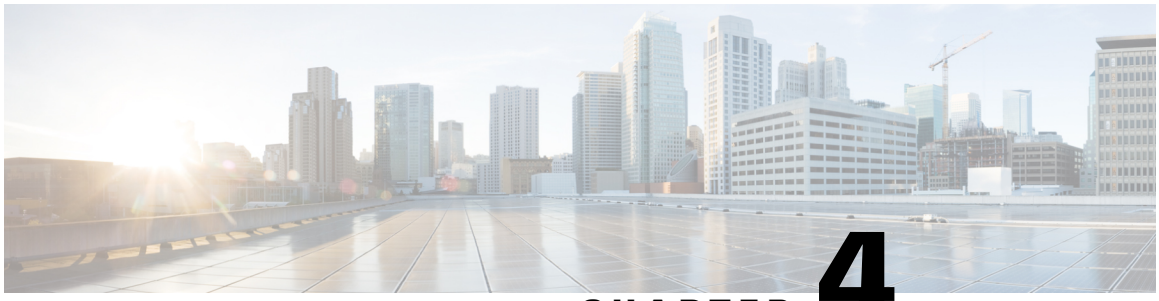
```
flow record type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_RECORD
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
```

```
    match transport destination-port
    match transport rtp ssrc
    collect ipv4 dscp
    collect ipv4 ttl
    collect transport rtp jitter mean
    collect transport rtp jitter minimum
    collect transport rtp jitter maximum
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect counter bytes rate
    collect counter packets drop (not applicable to routers)
flow monitor type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_MONITOR
    description APIC_EM flow-analysis request monitor
    record APIC_EM-FLOW_ANALYSIS_PERFMON_RECORD

ip access-list extended APIC_EM-FLOW_ANALYSIS_ACL
    class-map APIC_EM-FLOW_ANALYSIS_PERFMON_CLASSMAP
    match access-group name APIC_EM-FLOW_ANALYSIS_ACL
policy-map type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_POLICYMAP
    class APIC_EM-FLOW_ANALYSIS_PERFMON_CLASSMAP
    flow monitor APIC_EM-FLOW_ANALYSIS_PERFMON_MONITOR
interface GigabitEthernet x/y
    service-policy type performance-monitor input APIC_EM-FLOW_ANALYSIS_PERFMON_POLICYMAP

ip access-list extended APIC_EM-FLOW_ANALYSIS_ACL
    permit ip host aa.bb.cc.dd host ww.xx.yy.zz
[1]
```

[1] aa.bb.cc.dd is source ip and ww.xx.yy.zz is destination ip.



CHAPTER 4

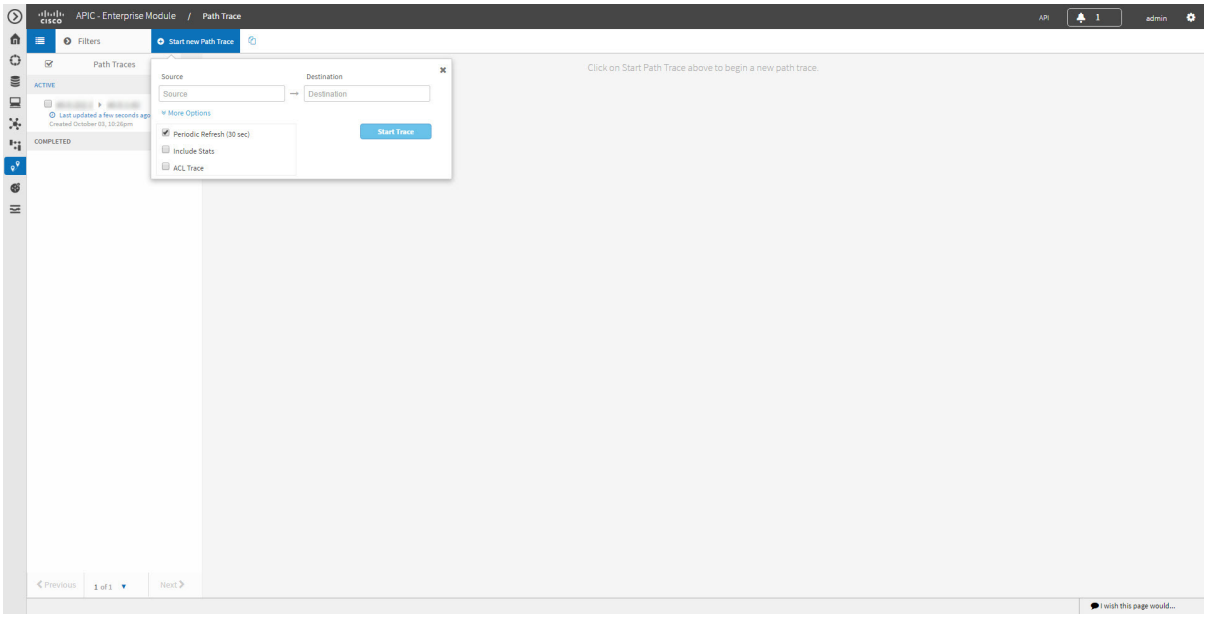
Performing Path Traces

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.

Figure 2: Path Trace Window



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.

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. You can also enter an IP address of an unmanaged device (called an unknown destination).
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 **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—**Collects and displays information about quality of service.
- **Interface—**Collects and displays information about the interfaces on the devices along the path.
- **Device—**Collects and displays information, such as a device's CPU and memory usage.
- **Perf Mon—**Collects and displays performance monitoring information about the devices along the path.

Note When you choose the **Perf Mon** option, APIC-EM enables performance monitoring configuration for all of the flows on the devices in the path. To proceed, you need to confirm this configuration.

Step 11 (Optional) Select the **ACL Trace** check box to run an ACL-based path trace.

Step 12 Click **Start Trace**.
Review the path trace output. For more information, see Understanding Path Trace Results, on page 24.

Step 13 Unless you performed a path trace to an unknown destination, you can view the path trace in the **Topology** window. To do so, click **View in Topology**.
The **Topology** window opens in a new window with the path trace highlighted in your network. For more information about the **Topology** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

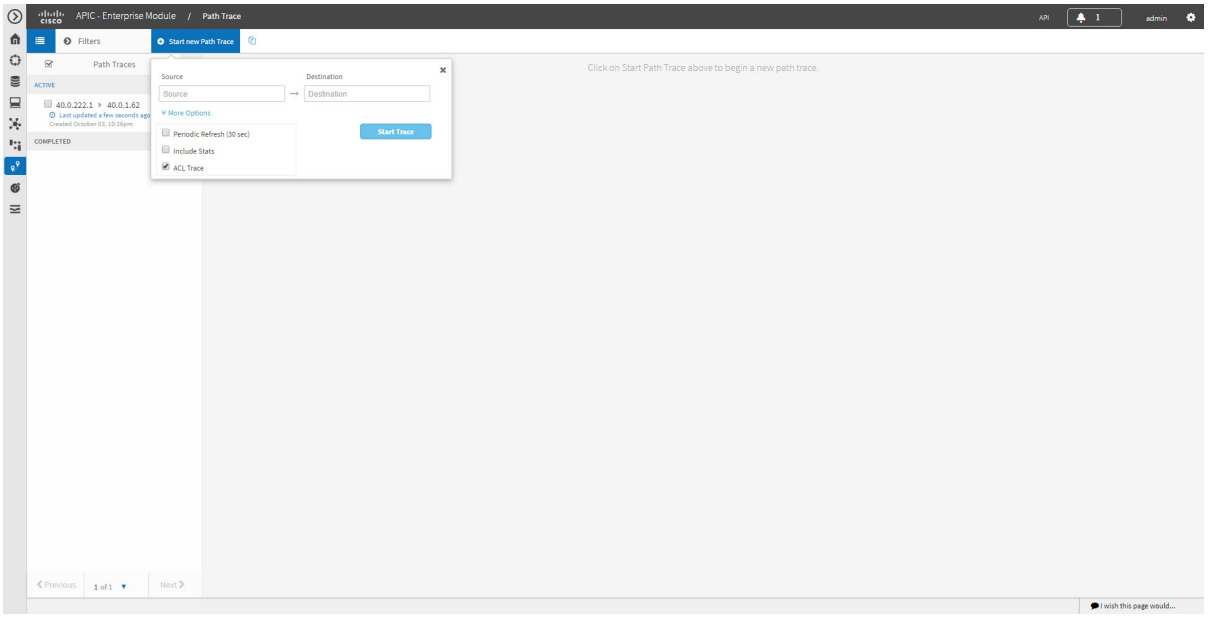
Note If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

Performing an ACL-Based 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.

Figure 3: Path Trace Window Showing ACL Trace Selected



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.

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. You can also enter an IP address of an unmanaged device (called an unknown destination).
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 **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—**Collects and displays information about quality of service.
- **Interface—**Collects and displays information about the interfaces on the devices along the path.
- **Device—**Collects and displays information, such as a device's CPU and memory usage.
- **Perf Mon—**Collects and displays performance monitoring information about the devices along the path.

Note When you choose the **Perf Mon** option, APIC-EM enables performance monitoring configuration for all of the flows on the devices in the path. To proceed, you need to confirm this configuration.

Step 11 Select the **ACL Trace** check box to run an ACL-based path trace.

Step 12 Click **Start Trace**.
Review the path trace output. For more information, see Understanding ACL Path Trace Results, on page 29.

Step 13 Unless you performed a path trace to an unknown destination, you can view the path trace in the **Topology** window. To do so, click **View in Topology**.
The **Topology** window opens with the path trace highlighted in your network. For more information about the **Topology** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

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.

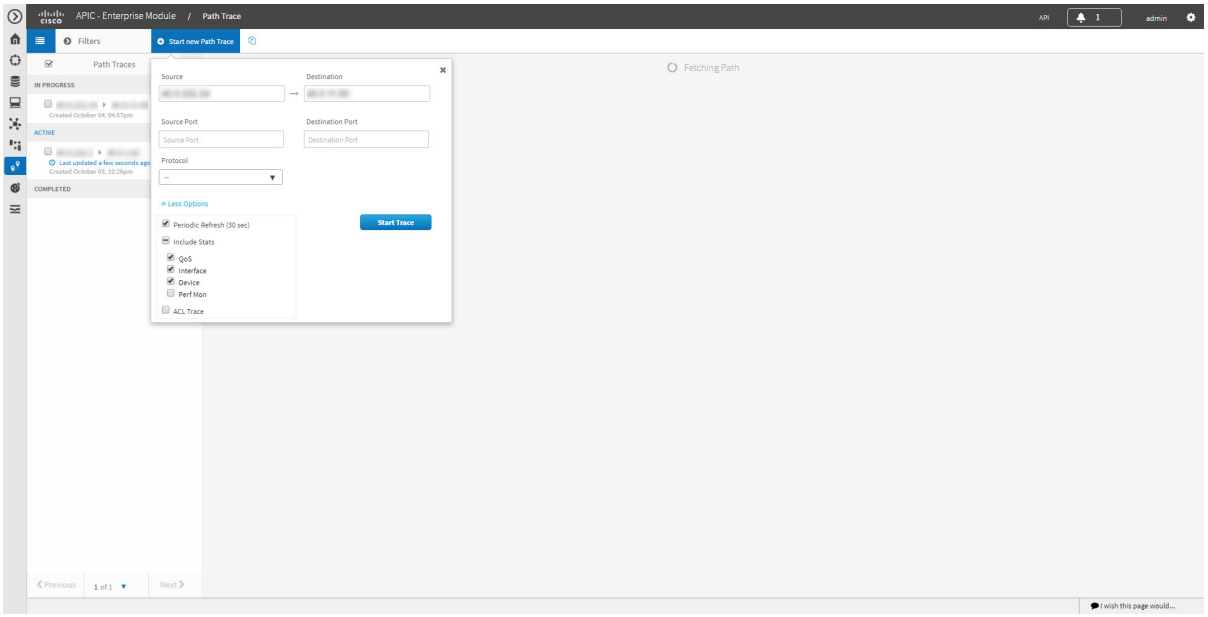
Collecting Statistics During a Path Trace

You can perform a path trace between two nodes in your network and collect the following types of statistics about the path:

- Quality of Service (QoS)
- Interface
- Device
- Performance Monitor (If you choose to run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM configures all of the devices in the requested path with the necessary flow monitor configuration. For information about this configuration, see Performance Monitor Configuration, on page 14.)

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.

Figure 4: Path Trace Window Showing Statistics Selected



Before You Begin

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

SUMMARY STEPS

1. In the **Navigation** pane, click **Path Trace**.
2. From the path trace toolbar, click **Start new Path Trace**.
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.
4. In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end.
5. (Optional) To configure source and destination ports or protocols, click **More Options**.
6. (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to start.
7. (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.
8. (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
9. (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.
10. Check the **Stats** check box.
11. Check any of the following check boxes corresponding to the type of statistics that will be collected:
12. Click **Start Trace**.
13. (Optional) To view the path trace in the **Topology** window. Click **View in Topology**.

DETAILED STEPS

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.

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.

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 start.

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 any of the following check boxes corresponding to the type of statistics that will be collected:

- **QoS Stats**
- **Interface Stats**
- **Device Stats**
- **Perf Mon Stats**

Note If you choose to run a path trace to collect **Perf Mon** statistics, you need to grant the Cisco APIC-EM permission to configure all of the devices in the requested path with the necessary flow monitor configuration. When the confirmation dialog box appears, click **OK** to allow this configuration or **Cancel** to discontinue this action. For information about this configuration, see Performance Monitor Configuration, on page 14.

Step 12 Click **Start Trace**.
The results are displayed in the **Trace Results Device Details** pane. For information, see the following topics:

- QoS Statistics, on page 34
- Interface Statistics, on page 33
- Device Statistics, on page 32
- Performance Monitor Statistics, on page 36

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.

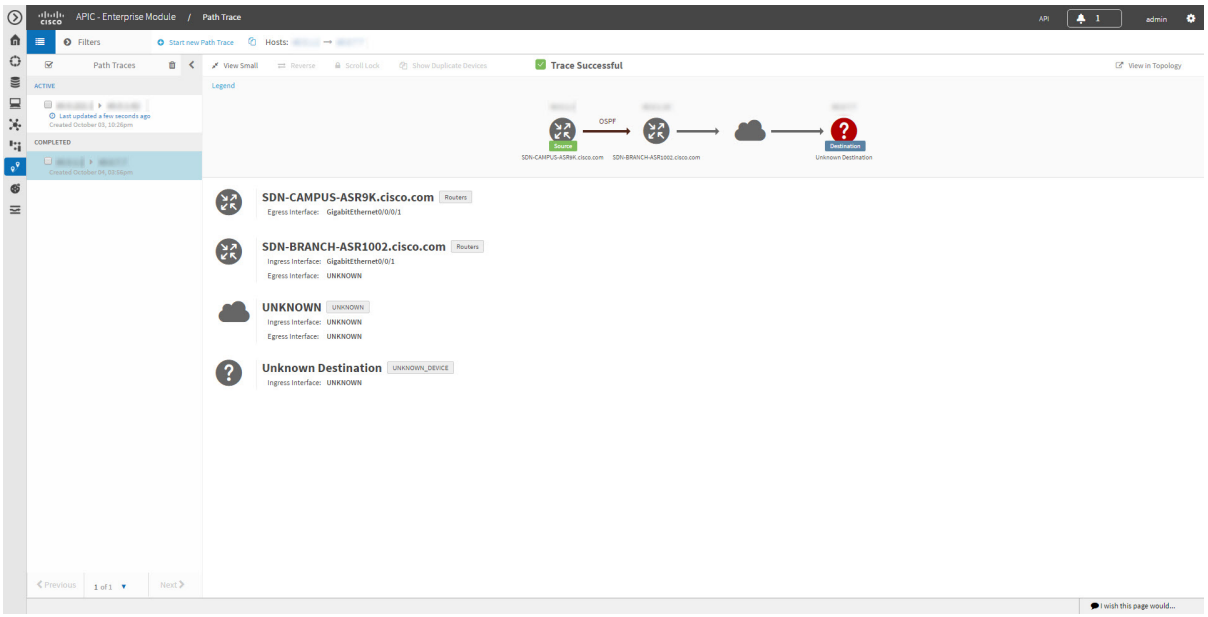
Note If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

For more information about the **Topology** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Understanding Path Trace Results

After you run a path trace, the results are displayed in the **Path Trace** window.

Figure 5: Path Trace Window Showing Results



Path Trace Toolbar

The **Path Trace Toolbar** provides the following options and information:

- **Filters—**Allows you to search for path traces by source or destination IP address, source or destination ports, protocol, creation date, or statistics gathered (QoS, Device, Interface, Perf Mon, and ACL trace)
- **Start new Path Trace—**Displays a dialog box where you can define the parameters for your path trace.
- **Copy** icon**—**Allows you to create a new path trace using the parameters that are defined in the selected (source) path trace. You can keep any of the values from the source path trace and change, add, or deselect any parameters for the new path trace.

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 Toolbar

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

Table 4: Trace Results Toolbar

Name [2]	Description
View Small	Minimizes the trace results to view the details better.
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. **Note** If you performed a path trace to an unknown destination, you cannot display the reverse path trace.
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.

Name [2]	Description
ACL Trace checkbox [3]	Displays an icon at each device or interface that indicates whether any ACLs are blocking traffic on the path.
Stats	If statistics were collected for the trace, you can select one or more of the interface, QoS, device, and performance monitor check boxes to display the corresponding information in the graphical display.
View in Topology	Opens the **Topology** window and highlights the path trace results in your network topology. If you performed a path trace to an unknown destination, this option is not available. For more information about using the Topology window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

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

3 Available only if you performed an ACL Path Trace.

Trace Results Graphical Display

The controller graphically displays the path direction and the hosts and devices (including their IP addresses) along the path between the source (host A) and destination (host B). Clicking an individual device in the path trace highlights the device in the **Trace Results Device Details** area. The display also shows the protocol of the path source between devices along the path: **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.

If you performed an ACL trace, the devices show whether the traffic matching your criteria would be permitted or denied based on the ACLs configured on the interfaces. For more information, see Performing an ACL-Based Path Trace, on page 19.

Trace Results Device Details

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

Table 5: Trace Results Device Details

Name	Description
IP	IP address of the device.
Type	Wired or wireless device (access point, switch, or router).

Name	Description
Link Source	Information about the link between two devices (source and destination). Link information is based on the configuration of the source device. • **Boarder Gateway Protocol (BGP)—**Link is based on the BGP routes configured on the source device. • **Equal Cost Multipath (ECMP) routing—**Link is based on a Cisco Express Forwarding (CEF) load balancing decision. • **Enhanced Interior Gateway Routing Protocol (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 switched virtual interface (SVI) configuration on the source device. A VLAN is configured on the source device from which the path is switched to the destination device. • **Intermediate System-to-Intermediate System Protocol (IS-IS)—**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. • **Next Hop Resolution Protocol (NHRP)—**Path Trace shows DMVPN dynamic tunnels between two spokes by identifying the LinkInformationSource as NHRP. • **Open Shortest Path First (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).

Name	Description
Tunnels	Path trace provides a graphical view of these types of tunnels: • Control and Provisioning of Wireless Access Points protocol (CAPWAP) data (wireless) or mobility tunneling. • Dynamic Multipoint VPN (DMVPN) tunnel—Path Trace shows the DMVPN tunnel route from spoke to spoke, spoke to hub, and from hub to spoke and indicates the underlay protocols that are in use. However, it does not show the underlay devices. For information, see Understanding DMVPN Path Trace Results, on page 30.
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 Interface Statistics, on page 33 or QoS Statistics, on page 34.
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 Interface Statistics, on page 33 or QoS Statistics, on page 34.
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.
VRF	If Path Trace detects a VRF on a router, it displays the VRF in the graphical display and provides the interface name and VRF name. For more information, see Understanding VRF Path Trace Results, on page 31.

Trace Results Statistics

If you specified that device statistics be included in the path trace, statistical information about the device is gathered and displayed. You can select or deselect one or more of the options from the **Stats** drop-down list so that you can isolate different information.

For information about the statistics, see the following sections:

- Device Statistics, on page 32
- Interface Statistics, on page 33
- QoS Statistics, on page 34
- Performance Monitor Statistics, on page 36

Understanding ACL Path Trace Results

An ACL path trace shows whether the traffic matching your criteria would be permitted or denied based on the ACLs configured on the path.

The following rules effect the ACL path trace results:

- Only matching ACEs are reported.
- If you leave out the protocol, source port, or destination port when defining a path trace, the results include ACE matches for all possible values for these fields.
- If no matching ACEs exists in the ACL, the flow is reported to be implicitly denied.

Figure 6: Path Trace Window Showing ACL Trace Selected

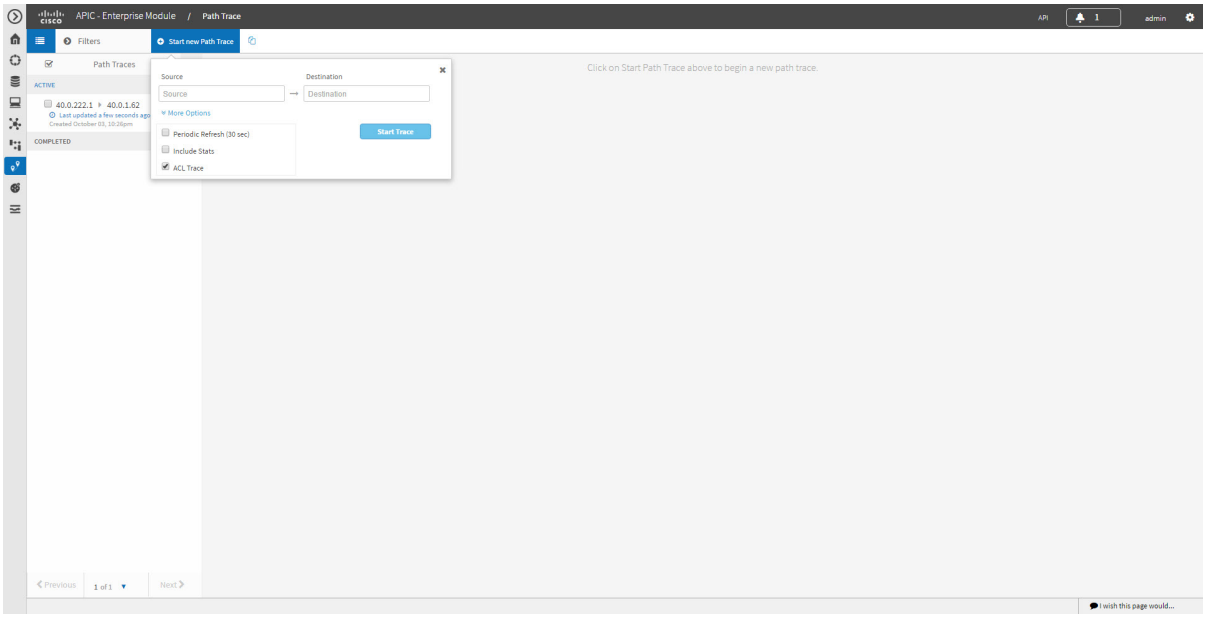


Table 6: ACL Path Trace Icons

Icon	Description
	There are ACLs that permit the traffic applied on the interface.

Icon	Description
	Traffic may or may not be blocked. For example, if your traffic matches a deny access control entry (ACE), traffic is denied. However, if your traffic matches any other ACEs, it is permitted. You can get this type of results if you leave out the protocol, source port, or destination port when defining a path trace.
	There is an ACL on the device or interface that is blocking the traffic on the path.
	There are no ACLs applied on the interface.

Understanding DMVPN Path Trace Results

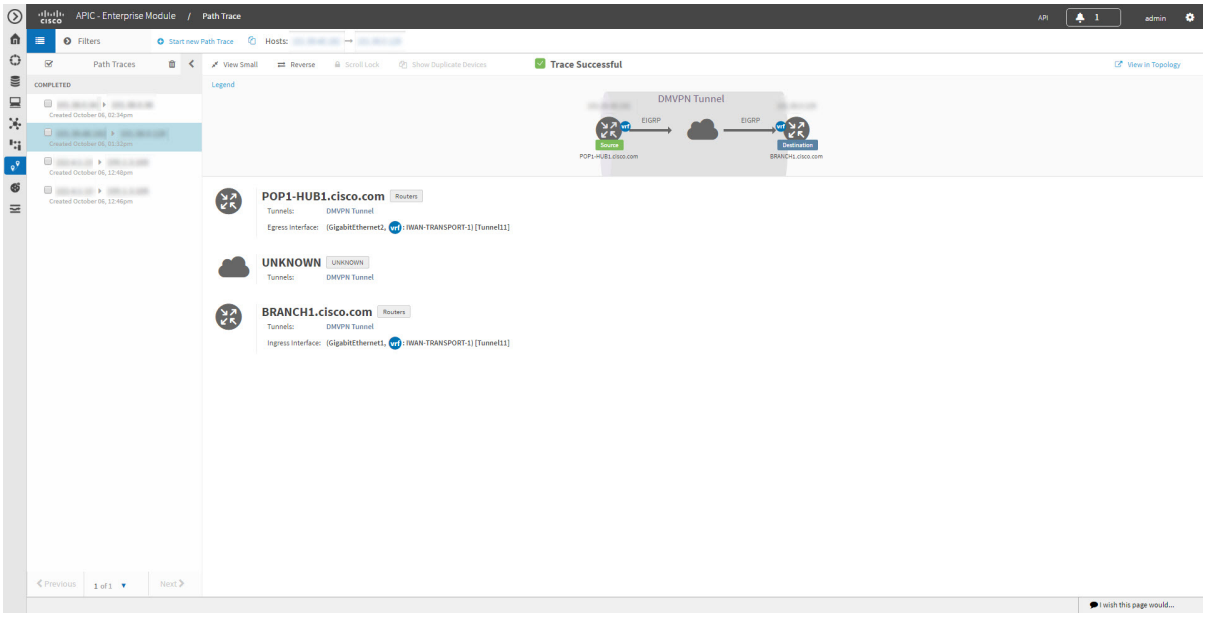
When you perform a path trace on a spoke-to-spoke connection, Path Trace determines (in real time) whether there is a dynamic NHRP entry due to traffic occurring between the two spokes. If there is, Path Trace shows the LinkInformationSource as NHRP.

If the there is no traffic between the two spokes, Path Trace uses the inventory data collected during device discovery to determine the next hop server (NHS), which is the hub for the two spokes. Path trace identifies and highlights the routing protocol advertised by hub, for example EIGRP or OSPF. In addition, path trace shows any intermediate hops, including service providers (shown as a cloud icon).

Path Trace identifies all tunnel source interface types and highlights them as egress or ingress interfaces and indicates the tunnel transport types, such as Front Door VRF (FVRF) and Inside VRF (IVRF).

PathTrace shows the mGRE tunnel interface as a virtual interface and the underlay interface as physical interface on a DMVPN endpoint.

Figure 7: Path Trace Window Showing DMVPN Tunnel



Understanding VRF Path Trace Results

Path trace supports VRF Lite and VRF route leaking. If Path Trace detects a VRF on a router, it displays the VRF in the graphical display and provides the interface name and VRF name. VRFs are shown as a colored circle, making it easy to see where they are along the path. VRFs with the same name have the same color.

Understanding the Statistics Retrieved During a Path Trace

Device Statistics

If you specified that device statistics be included in the path trace, Path Trace gathers and displays statistical information about the device. Not all device types support all of the parameters (5 minutes, 5 seconds, and 1 minute). If a device does not support a particular parameter, Path Trace displays **N/A** (not supported).

Figure 8: Path Trace Window Showing Device Statistics

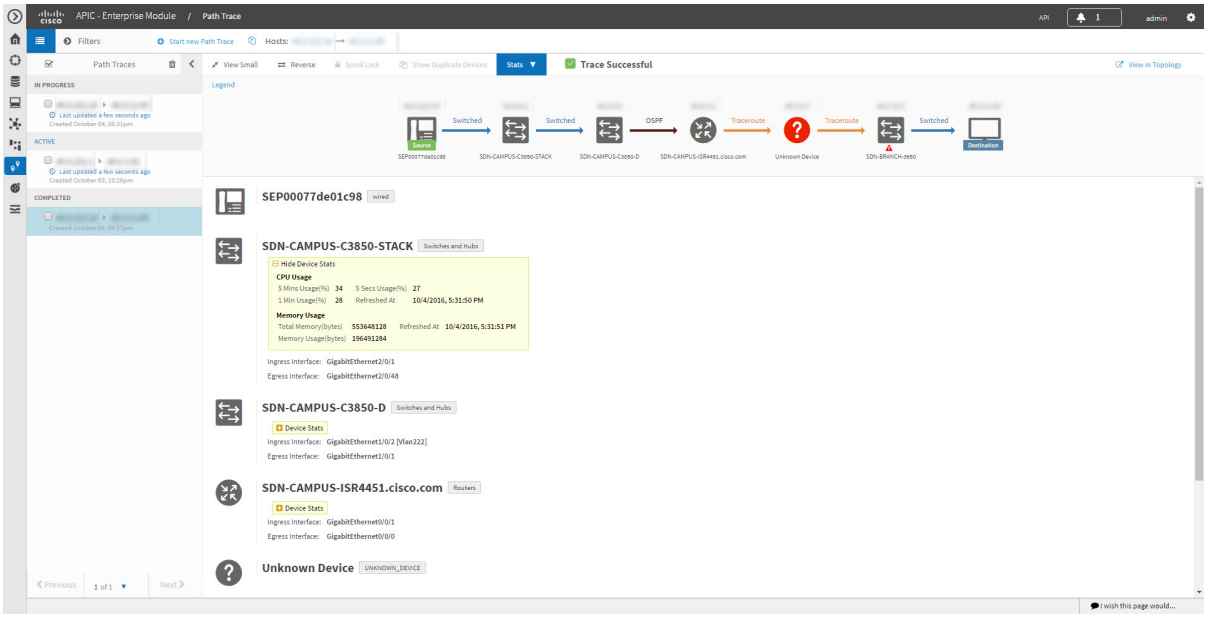


Table 7: Path Trace Device Statistics

Parameter	Description
CPU Usage	
5 Mins Usage(%)	Percentage of the device's CPU usage for the last 5 minutes.
5 Secs Usage(%)	Percentage of the device's CPU usage for the last 5 seconds.
1 Min Usage(%)	Percentage of the device's CPU usage for the last minute.
Refreshed At	Date and time when the information was gathered.
Memory Usage	
Refreshed At	Date and time when the information was gathered.

Parameter	Description
Memory Usage(bytes)	The sum of the physical memory usage and I/O memory usage (in bytes) that the device is using.
Total Memory (bytes)	Total memory (in bytes) of the device.

Interface Statistics

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.

Figure 9: Path Trace Window Showing Interface Statistics

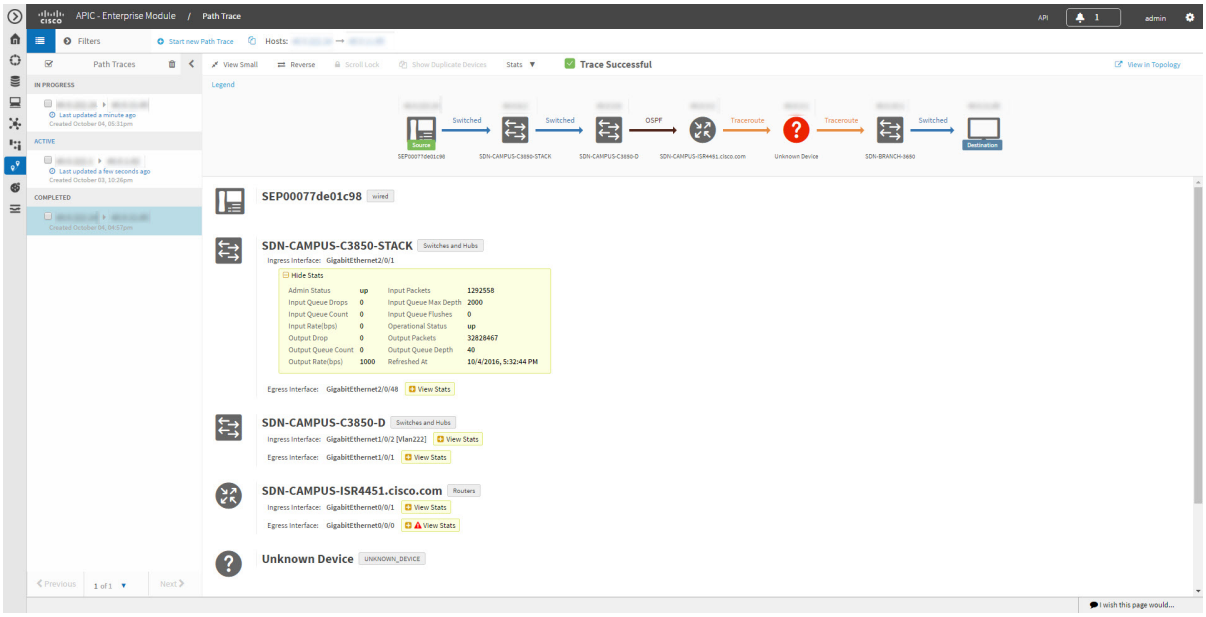


Table 8: Interface Statistics by Policy

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.

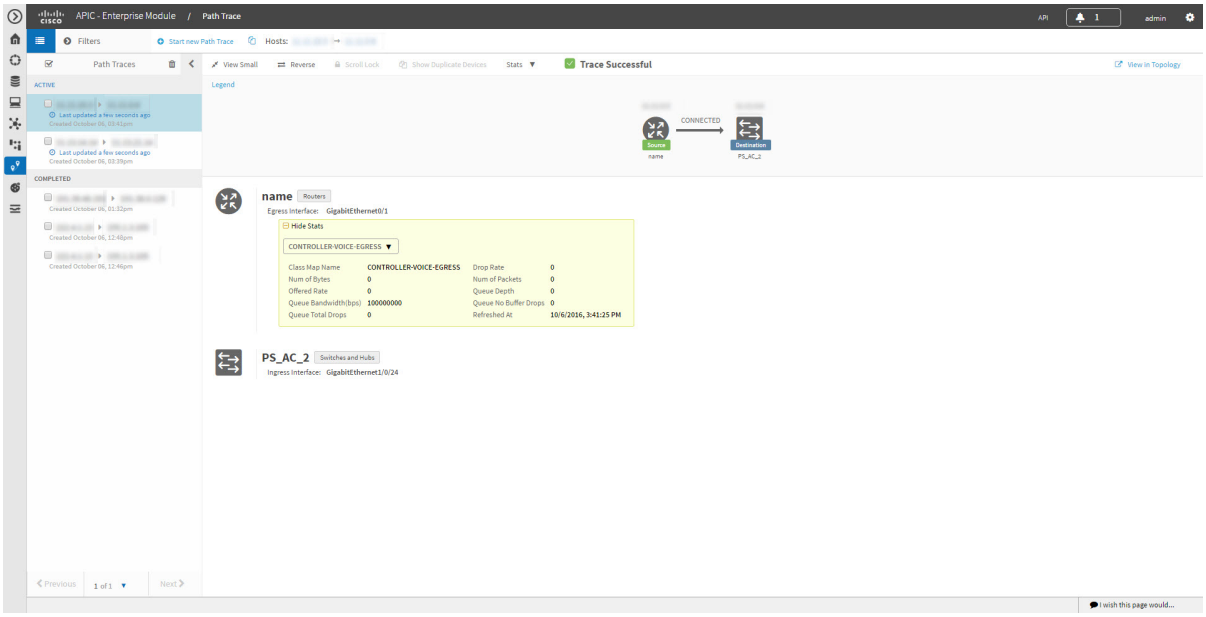
Parameter	Description
Input Queue Drops	Number of packets dropped from input queue since the interface counters were last cleared. It is not associated with any interval.
Input Queue Max Depth	Maximum number of packets that the input queue can hold before it must start dropping packets.
Input Queue Count	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 statisticswere gathered.

QoS Statistics

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.

Figure 10: Path Trace Window Showing QoS Statistics



The following table lists the QoS Statistics that are retrieved.

Table 9: QoS Statistics by Policy

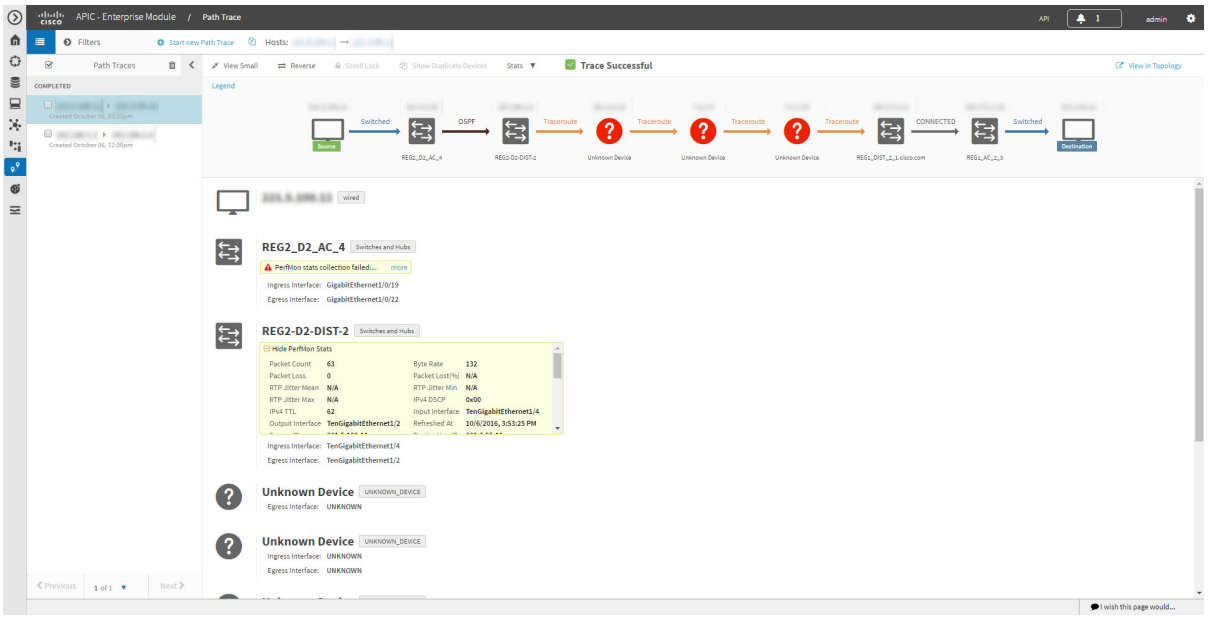
Parameter	Description
Policy Name	Drop-down list of policy names that QoS statistics have been collected about.
Class Map Name	Name of the class map.
Num of Bytes	Average number of bytes forwarded by the queue.
Offered Rate	Traffic rate offered for that particular traffic.
Queue Bandwidth (bps)	Rate (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.

Parameter	Description
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.

Performance Monitor Statistics

When you run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM automatically configures all of the devices in the requested path with the necessary flow monitor configuration, and then removes the configuration when it is no longer needed (no pending performance monitor path trace for the path or 24 hours, whichever is first). For information about this configuration, see Performance Monitor Configuration, on page 14.

Figure 11: Path Trace Window Showing Performance Monitor Statistics



The following table lists the performance monitor statistics that are retrieved.

Table 10: Performance Monitor Statistics

Parameter	Description
Packet Count	Total number of IP packets sent.

Parameter	Description
Byte Rate	Average number of packets or bytes (as configured) that were processed by the monitoring system per second during the monitoring interval.
Packet Loss	Total number of IP packets lost by any intermediate system in the monitored flow.
Packet Loss (%)	Percentage of IP packets lost by any intermediate system in the monitored flow.
RTP Jitter Mean	Mean deviation (in microseconds) of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
RTP Jitter Min	Minimum value of the Real-time Transport Protocol (RTP) jitter in microseconds.
RTP Jitter Max	Maximum value of the Real-time Transport Protocol (RTP) jitter in microseconds.
IPv4 DSCP (Hexadecimal)	Hexadecimal value of the IPv4 differentiated services code point (DSCP) type of service (ToS).
IPv4 TTL	Value of the IPv4 time-to-live (TTL).
Input Interface	Name of the input interface that was used as match criteria.
Output Interface	Name of the output interface that was used as match criteria.
Refreshed At	Date and time that the performance monitor statistics were gathered.
Source IP	IP address of the source interface for all of the packets sent by a flow exporter.
Destination IP	IP address of the destination interface for all of the packets sent by a flow exporter.

INDEX