



## Managing Applications

---

- [Cisco Network Plug and Play, page 1](#)
- [Cisco Intelligent WAN \(IWAN\), page 2](#)
- [Topology, page 3](#)
- [Performing Path Traces, page 19](#)

### Cisco Network Plug and Play

The Cisco Network Plug and Play application provides a simple and secure solution for day-zero deployment of Cisco routers, switches, and wireless access points. The Cisco Network Plug and Play application allows users to preprovision devices by specifying the required image, configuration, and other details. When the device installer installs and powers up a Cisco network device, the device automatically discovers the Cisco APIC-EM controller using DHCP or DNS. After the discovery process is complete, the Cisco Network Plug and Play application provisions the device with the preconfigured information. If a device is not preconfigured, after it discovers and connects to the Cisco APIC-EM, it is listed as an unplanned device in the Cisco Network Plug and Play application. You can use the Cisco Network Plug and Play application to claim the unplanned device and configure it with a new configuration and Cisco IOS image. Cisco APIC-EM supports an embedded Plug and Play (PnP) protocol server that simplifies network device provisioning by securely and automatically delivering an image and configuration file to Cisco devices that support PnP. The PnP server communicates with a Cisco PnP agent installed on the PnP-supported Cisco devices.

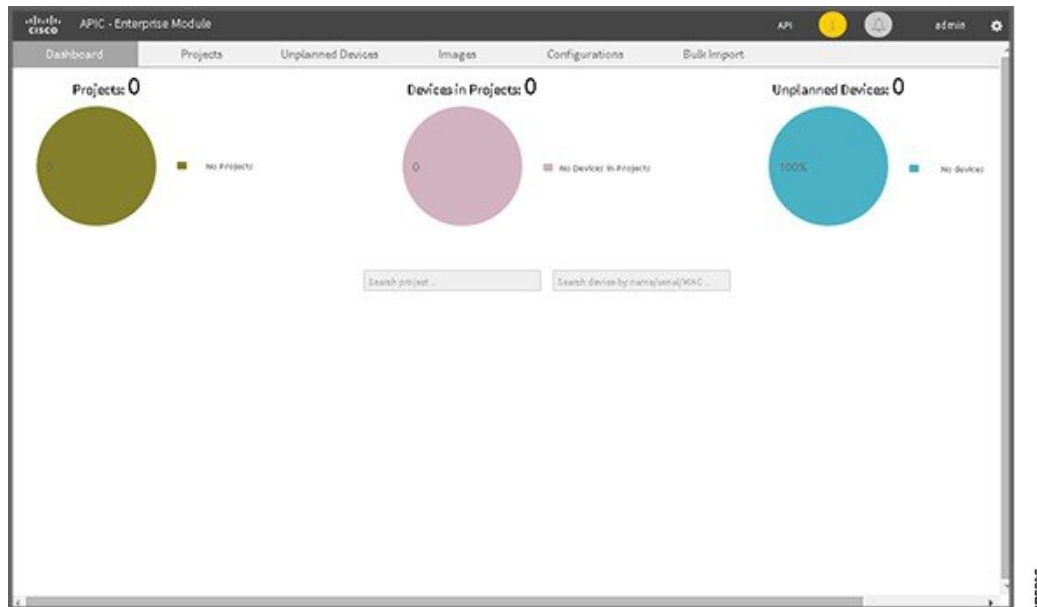
From the Network Plug and Play dashboard page, you can check the status of your site deployment. You can also start defining new sites using the **Projects** link, or view unclaimed devices using the **Unplanned Devices** link.

See the Cisco Network Plug and Play documentation for information about Cisco Network Plug and Play configuration procedures.

**Note**

You may need to import a proxy gateway certificate if the PnP application is enabled on the controller and a proxy gateway exists in the DMZ between the PnP-enabled devices and the controller. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

**Figure 1: Cisco Network Plug and Play Dashboard**



## Cisco Intelligent WAN (IWAN)

The Cisco Intelligent WAN (IWAN) helps IT deliver an uncompromised user experience over any connection while lowering operational costs. IWAN also simplifies IT operations through a software-based controller model, automating management tasks to ensure faster, more successful deployments.

The Cisco IWAN Application leverages the APIC-EM to abstract the network devices into one system to eliminate network complexity, and provide centralized provisioning of the infrastructure to speed up application and service roll outs.

The Cisco IWAN Application with APIC-EM extends Software Defined Networking to the branch with an application-centric approach based on business policy and application rules. This provides IT centralized management with distributed enforcement across the network.

From the IWAN dashboard page, you can configure your network-wide settings, provision sites, and configure application policies.

See the Cisco IWAN documentation for information about Cisco IWAN network configuration procedures.

**Note**

You may need to import a proxy gateway certificate if the IWAN application is enabled on the controller and a proxy gateway exists in the DMZ between network devices and the controller. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

**Figure 2: IWAN Dashboard**



## Topology

The **Topology** window displays a graphical view of your network. Using the discovery settings that you have configured, the Cisco APIC-EM discovers and maps devices to a physical topology with detailed device-level data.

To access the **Topology** window, click **Topology** in the Navigation pane. The **Topology** window appears.

In addition, auto-visualization of Layer 2 and 3 topologies on top of the physical topology provides a granular view for design planning and simplified troubleshooting.

For a Layer 2 topology, the controller discovers configured VLANs within your network to display in the **Topology** window. For a Layer 3 topology, the controller discovers all forms of a Layer 3 topology (OSPF, IS-IS, etc.), depending on what is currently configured and in use within your network to display in the **Topology** window.

**Note**

Individual device configurations are retrieved and stored in a network information base (NIB).

Clicking on a device icon provides information about that device.

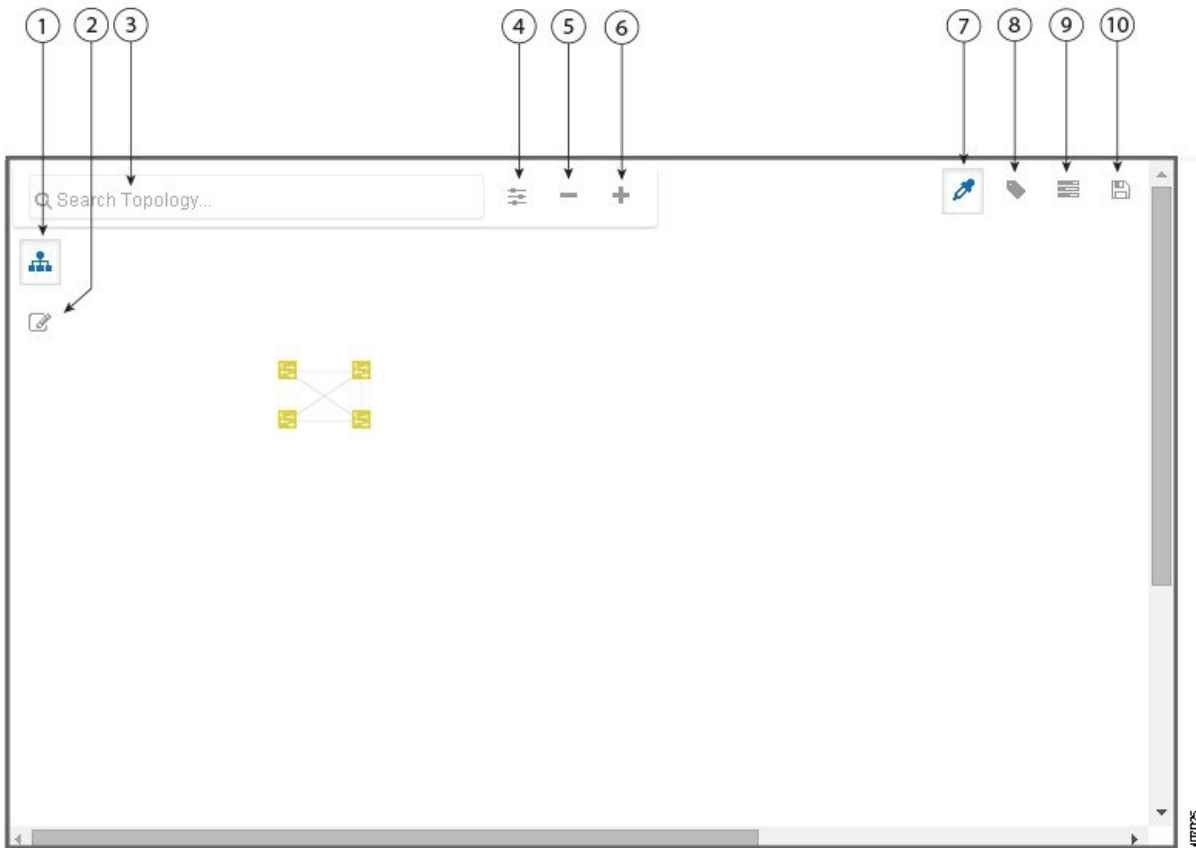
**Note**

For additional detailed information about the paths between hosts and through the network devices, use the **Path Trace** feature. Click **Path Trace** in the Navigation pane to access this application.

## Topology Toolbar

The Topology toolbar is located at the top of the **Topology** window.

**Figure 3: Topology Window**










Callout Number	Icon Name	Description
1	<b>Multiselect</b>	<p>Allows you to select multiple devices by dragging the mouse over the desired devices or shift-clicking on devices. You can also select multiple groups of devices by clicking shift and dragging the mouse over a group of devices. After selecting the group of devices, you can aggregate or tag them. If you aggregate devices of different product families, the Cisco APIC-EM shows them as generic devices (without a device type) and the number of devices. Multiselect is off by default.</p>
2	<b>Toggle Aggregation</b>	<p>Enables or disables device aggregation. Aggregating devices means grouping devices together. You can group devices in any way that makes sense to you.</p> <p>You can save the layout for future reference by clicking the <b>Save</b> icon.</p> <p>This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default.</p>
3	<b>Search Topology</b>	<p>Searches for a device by device name, device type, or IP address. As you enter information into this field, the Cisco APIC-EM displays matches. Select the device from the results that appear. The selected device appears in the <b>Topology</b> window.</p>

Callout Number	Icon Name	Description
4	<b>Filters</b>	<p>Displays options to change the default view of the topology:</p> <ul style="list-style-type: none"> <li>• <b>Enterprise (Default)</b>— Displays your network topology, separating your devices on connection branches. For example, if a group of devices are connected to Router A, and another group of devices are connected to Router B, the topology would show this division and would separate the devices.</li> <li>• <b>Connections</b>—Displays the devices according to their number of connections. Starting from the left, the devices with no connections are displayed, then devices with one connection, then devices with two connections, and so on.</li> <li>• <b>Type and Role</b>—Displays the devices according to their role in the network: access router, distribution switch, core switch and hub, and boarder router.</li> </ul>
5	<b>Zoom out</b>	<p><b>Note</b> Adjusts the <b>Topology</b> window's view. Click the - (minus) icon to minimize the view of the network devices.</p>
6	<b>Zoom in</b>	<p>Adjusts the <b>Topology</b> window's view. Click the + (plus) icon on the menu bar to maximize the view of the network devices.</p>
7	<b>Toggle Color Code</b>	<p>Toggles between displaying the device icons in different colors or in a single color. Color coding is enabled by default.</p>
8	<b>Tags</b>	<p>Displays the available tags. Clicking on an individual tag highlights the device or devices in the <b>Topology</b> window that have this tag.</p> <p>You can also apply tags to devices by selecting the device, clicking <b>Device Tagging</b> in the <b>Device Information</b> dialog box, and then creating and applying the tags.</p>


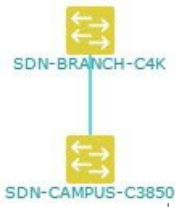
Callout Number	Icon Name	Description
9	Layers	<p>Displays the Layer 2 and Layer 3 options:</p> <ul style="list-style-type: none"> <li>• <b>Layer 2</b>—Displays a topology of devices based on the selected VLAN or Layer 2 protocol. Select either a VLAN from the drop-down menu or one of the Layer 2 protocols.</li> </ul> <p><b>Note</b> You can also access a management network view by choosing a management selection from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>Layer 3</b>—Displays a topology of devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available: <ul style="list-style-type: none"> <li>◦ <b>Intermediate System-to-Intermediate System (IS-IS)</b></li> <li>◦ <b>Open Shortest Path First (OSPF)</b></li> <li>◦ <b>Enhanced Interior Gateway Routing Protocol (EIGRP)</b></li> <li>◦ <b>Static-Route</b></li> </ul> </li> </ul> <p><b>Note</b> The default Layer 3 topology that displays contains all Layer 3 protocols.</p>
10	Save and Load Options	<p>Displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Save Current Layout</b>—Saves the current layout, device aggregations, and labels.</li> <li>• <b>Load Saved Layout</b>—Loads the previously saved layout, device aggregations, and labels) options.</li> </ul>
11	Map view (Not shown)	<p>Displays the <b>Topology</b> map view. Click this icon to view the network topology in a graphical representation of your network's physical location.</p> <p><b>Note</b> This icon is displayed only if you have added location markers for your devices from the <b>Device Inventory</b> window.</p>

## Topology Icons

The following icons appear in the **Topology** window:

Icon	Network Element	Description
 cloud	Cloud	Representation of the external network.
 hostname	Host	Displays the hostname or IP address of the host.
 DEVICE-NAME	Router	Displays the device name.
 DEVICE-NAME	Switch	Displays the device name.
 DEVICE-NAME	Access Point	Displays the device name.
 DEVICE-NAME	Wireless LAN Controller	Displays the device name.
 3 accesspoint	Aggregated Devices	Displays the number of aggregated devices and the device type. <b>Note</b> If different devices types are aggregated, only the number of aggregated devices is displayed.



Icon	Network Element	Description
	<p><b>Location Marker</b></p>	<p>Displays the device name. The device icon is displayed with a location marker as a background.</p> <p>If you add location markers to your devices (from the <b>Device Inventory</b> window) and then click <b>Topology</b> in the navigation pane or click the <b>Map</b> button on the Topology toolbar, the Topology map view appears. The map view shows where you have placed your location markers (for example, San Jose and London). Click a location marker on the map to display the topology for that location (for example, San Jose).</p> <p>Devices that use a different location marker (for example, London) are shown with a location marker as a background.</p>
	<p><b>Links</b></p>	<p>Lines between devices.</p> <p>Click on a link to display information about the connected devices.</p> <p><b>Note</b> Some of the links may be hidden due to device aggregations.</p>

**Related Topics**

- [Applying Tags to Devices](#)
- [Viewing Device Data](#)
- [Searching for Devices and Hosts, on page 16](#)
- [Configuring the Topology Structure, on page 13](#)
- [Changing the Aggregated Devices Label, on page 12](#)
- [Removing Tags from Devices](#)
- [Viewing Devices with Tags](#)
- [Adding a Location Marker](#)
- [Aggregating Devices in the Topology Window, on page 11](#)
- [Configuring the Topology Structure, on page 13](#)
- [Topology](#)

## Displaying Device Data

You can display data for a specific device in the **Topology** window. Displaying device data is helpful when troubleshooting network connectivity issues between devices.



**Note**

The device data that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

The following device data is available:

- Location (Location information is displayed if the selected device icon has a location marker background. Click the **Location** link to display the topology for devices that share that location marker.)
- Type
- Device role (For information about changing the device role, see [Changing the Device Role](#).)
- IP address
- MAC address
- OS (operating system)
- Software version
- Ports
  - Gigabit Ethernet ports
  - 10-Gigabit Ethernet ports
  - Management ports
- VLAN (if exists)
- Number of connections
- List of connected devices (Each connected device shows its device type (icon) and the number of connections. Clicking on a connected device displays the details for that device.)
- Tags

---

**Step 1** From the **Navigation** pane, click **Topology**.  
The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** To display data for a specific device, click that device in the **Topology** window.

**Step 3** To display a list of aggregated devices, do the following:

- a) In the **Topology** window, click an **aggregated devices** icon.
  - b) In the **Device Details** pane, click the **Details** link for each device to view the device data.
  - c) Click the **Aggregated Results** link to return to the list of aggregated devices.
- 

### What to Do Next

Select and review data from other devices within your network, or perform other tasks including the following:

- Aggregate or disaggregate selected groups
- Search for device using device names and IP addresses
- Apply tags to devices within your network
- Change the device role

## Device Aggregation

You use the Cisco APIC-EM device aggregation feature to adjust how devices are displayed in the **Topology** window. This feature enhances network navigation and manageability.

### Aggregating Devices in the Topology Window

You can aggregate and disaggregate devices into and out of groups in the **Topology** window.

#### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

- 
- Step 1** Click **Topology** in the navigation pane.  
The **Topology** window appears.
- Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.
- Step 2** Click the **Toggle Aggregation** icon to enable device aggregation.
- Note** Device aggregation is enabled by default.
- Step 3** Drag and drop a device icon onto another device icon.  
The device icon changes to an aggregated devices icon. For more information about the aggregated devices icon, see [Topology Icons](#), on page 8.
- Note** You can also select multiple devices by clicking the **Multiselect** icon, dragging the mouse over the desired devices, and clicking the **Aggregate Selected** link.
- 

#### Related Topics

- [Topology](#)
- [Topology Icons](#), on page 8
- [Topology Toolbar](#)

### Disaggregating Devices in the Topology Window

#### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

- 
- Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.
- Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.
- Step 2** Click on an **aggregated devices** icon.  
A list of the aggregated devices appears.
- Step 3** From the list, click the **Disaggregate** link for each device that you want to remove from the aggregated devices.  
The device is removed from the list and from the aggregated devices icon. The aggregated device label and the aggregated devices icon are updated to reflect the number of devices.
- 

## Changing the Aggregated Devices Label

The default label for aggregated devices is the number of devices and the device type (*# devicetype Devices*). However, you can change the default label to one that is meaningful in the context of your network topology.

### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

- 
- Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.
- Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.
- Step 2** Click an **aggregated devices** icon.  
A list of the aggregated devices appears. At the top of the list is the aggregated devices label.
- Step 3** Click the aggregated devices label to open an edit field where you can change the label.
- Step 4** Change the label, then click outside of the edit field to save your changes.
- 

### Related Topics

[Topology](#)

[Topology Icons, on page 8](#)

[Topology Toolbar](#)

## Configuring the Topology Structure

You can choose from three default topology layouts. You can also use advanced settings to modify these layouts, such as the overall size of the topology graph, the spacing that separates individual elements, and more.

### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

**Step 1** From the **Navigation** pane, click **Topology**.  
The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** From the **Topology** toolbar, click the **Filters** icon.

**Step 3** Select a filter from the drop down list. Available options are **Branch**, **Connections**, or **Device & Role**.

**Step 4** Click the **Advanced View** button to configure how each filter is displayed. Click the **Basic View** button to return to the basic view.

Filter	Basic View	Advanced View
Enterprise	Arranges the device icons into a structured connection hierarchical view, from top to bottom.	<p><b>Device type</b>—Use the slider to adjust the amount of space between device icons based on their device types.</p> <p><b>cloud-centralizeX</b>— When checked (default), the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.</p> <p><b>Device role</b>—Use the slider to adjust the amount of space between device icons based on their device roles.</p> <p><b>Branch</b>— Use the slider to adjust the amount of space between branches.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>aggregate-WIRED</b>—When checked (default), wired hosts are aggregated. When unchecked, wired hosts are disaggregated.</p> <p><b>aggregate-WIRELESS</b>—When checked (default), wireless hosts are aggregated. When unchecked, wireless hosts are disaggregated.</p> <p><b>Note</b> Select x or y from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>

Filter	Basic View	Advanced View
<b>Connections</b>	<p>Arranges the device icons from left to right based on the number of connections, from least to most.</p> <p><b>Note</b> Aggregated devices are disaggregated in this view.</p>	<p><b>Connections</b>—Use the slider to adjust the amount of space between connections.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>centralizeY</b>—When checked, the device icons are centered along the Y axis. When unchecked, the device icons are aligned to the Y axis.</p> <p><b>Note</b> Select <b>x</b> or <b>y</b> from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>
<b>Type and Role</b>	<p>Arranges the device icons from top to bottom based on device type (cloud, router, WLC, switch, access point, wired, wireless) and role (border router, core, distribution, host, and access)</p> <p><b>Note</b> Aggregated devices are disaggregated in this view.</p>	<p><b>Device type</b>—Use the slider to adjust the amount of space between device icons based on their device types.</p> <p><b>Device role</b>—Use the slider to adjust the amount of space between device icons based on their device roles.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>centralizeX</b>—When checked, the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.</p> <p><b>Note</b> Select <b>x</b> or <b>y</b> from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>

### What to Do Next

Save the current layout or load a previously saved layout. For information, see [Saving a Topology Layout, on page 14](#) and [Opening a Saved Topology Layout, on page 15](#).

### Related Topics

- [Topology](#)
- [Topology Icons, on page 8](#)
- [Topology Toolbar](#)
- [Topology](#)
- [Topology Icons, on page 8](#)
- [Topology Toolbar](#)

## Saving a Topology Layout

You can save a topology layout so that you can open and view it later.

### Before You Begin

You must have administrator role permissions.

You must have scanned your network using discovery to populate device and host inventory into the database.

- 
- Step 1** From the **Navigation** pane, click **Topology**.  
The **Topology** window appears.
- Step 2** From the **Topology** toolbar, click the **Save** icon.
- Step 3** In the **Topology Title** field, enter a name for the topology and click **Save as New**.
- Step 4** Click **OK** to confirm the save.  
The topology is saved and the name appears at the top of the dialog box.
- 

## Opening a Saved Topology Layout

You can open a topology layout that you have previously saved.

### Before You Begin

You must have administrator role permissions.

You must have scanned your network using discovery to populate device and host inventory into the database.

You must have saved a topology layout.

- 
- Step 1** From the **Navigation** pane, click **Topology**.  
The **Topology** window appears.
- Step 2** From the **Topology** toolbar, click the **Save** icon.  
A dialog box appears listing the saved topology layouts.
- Step 3** For the topology layout that you want to open, click the **Folder** icon..
- Step 4** Click **OK** to confirm.  
The topology layout opens in the **Topology** window.
- 

## Changing the Device Role in the Topology Window

During the scan process, a device role is automatically assigned to each discovered device. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

A device can have one of the following roles within the Cisco APIC-EM:

- Unknown—Device role is unknown.
- Access—Device is located within and performs tasks required for the access layer or first tier/edge.
- Border Router—Device performs the tasks required for a border router.
- Distribution—Device is located within and performs tasks required for the distribution layer.
- Core—Device is located within and performs tasks required for the core.

You can change the device role when you select a device and display the device data.

**Note**

You can also change the device role from the **Device Inventory** window.

**Before You Begin**

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

- 
- Step 1** From the **Navigation** pane, click **Topology**.  
The **Topology** window appears.
- Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.
- Step 2** Click a specific device in the **Topology** window to select it.
- Step 3** Choose a role from the **Role** drop-down list: **Access**, **Core**, **Distribution**, or **Border Router**.
- Step 4** (Optional) Select additional devices and change device roles.
- Step 5** Click the **Filters** icon on the **Topology** toolbar.
- Step 6** (Optional) Select a filter from the drop down list. Available options are **Branch**, **Connections**, or **Device and Role**.
- Step 7** Click the refresh button to the right of the filter type to update all of the device roles.  
The **Topology** structure refreshes showing the changed device roles.
- 

## Searching for Devices and Hosts

You use the Cisco APIC-EM search function to locate specific hosts or devices within your network. This function allows you to search the network using any string value. To locate a specific host or device quickly, use any of the following values in the search field:

- Device or host name
- Aggregation label
- IP address
- Device role
- Device type





**Note** The search function supports fragmented results. For example, if you enter **12** in the search field, you will get results for devices with IP addresses or device names that contain 1 and 2 (.12, .120, .102, 10.20, 1-switch2, etc).

### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine the string value to be used within your network for your search.

**Step 1** Click **Topology** in the navigation pane.  
The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.

**Step 2** From the Topology toolbar, enter a keyword in the **Search Topology** field.  
As you begin typing, the controller displays a list of possible matches to your entry.

**Note** You can click the **x** in the search field to clear the search keyword field and the results.

**Step 3** Click on a device from the search results to highlight that device and its links in the **Topology** window. Click on the device again to display detailed data for that device.

**Step 4** Proceed with any provisioning or troubleshooting tasks on the located hosts or devices.

### What to Do Next

Search using other string values for other hosts or devices within your network, or perform other tasks including the following:

- Viewing the data for specific devices
- Applying tags to devices within your network

### Related Topics

[Topology](#)

[Topology Icons](#), on page 8

[Topology Toolbar](#)

## Applying Tags to Devices

You use the Cisco APIC-EM tag feature to associate devices within your network with a single attribute. A tag also enables the grouping of devices based upon an attribute. For example, you can create a tag and use it to group devices based upon a platform ID, Cisco IOS releases, or location.

To apply tags to devices within your network in the **Topology** window, perform the following steps.



---

**Note** Applying a tag to a host is not supported.

---

### Before You Begin

You should have performed the following tasks:

- Scanned your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.
- Determined the tags that you will use to apply to devices within your network.

- 
- Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.
- Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see [Topology Icons, on page 8](#).  
**Note** To deselect devices in your selection, click outside of the selected device.  
The **Device Information** dialog box appears.
- Step 3** Click **Device Tagging**.  
The **Device Tagging** dialog box appears.
- Step 4** From the **Available Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by following these steps:  
a) Enter the name of the tag in the **Tag Title** field.  
b) Click **+New Tag**.
- Step 5** When you are done tagging, click **x** to close the dialog box.
- Step 6** You can verify the tagging by clicking on one of the devices that you tagged.  
The **Device Information** dialog box shows the **Tags** field with the total number and the names of the tags applied to the device.
- 

## Displaying Devices with Tags

To display tagged devices from the **Topology** window, perform the following steps.

### Before You Begin

You should have performed the following tasks:

- Discovered the devices on your network to populate the device and host inventory database.

- Created tags and applied them either through the **Device Inventory** or **Topology** window.

---

**Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the Topology for that location.

**Step 2** From the Topology toolbar, click the **Tags**.  
A tag selection box appears.

**Step 3** To identify the devices associated with a tag, click the tag. To return the devices to their normal display, click the tag again.

Tags are color-coded, so when you click a tag, a circle of the same color is drawn around its associated devices.

**Note** You can click more than one tag at a time. The tag that you chose to display first is the innermost circle around the device, followed by the next tag as the next circle, and so on.

**Step 4** To close the tag selection box, click the **Tags** icon in the **Topology** toolbar.

---

## Performing Path Traces

### About Path Trace

Path trace involves the controller reviewing and collecting protocol and other types of data from discovered devices in your network, and then using this data to calculate a path between two hosts or Layer 3 interfaces. You can use the path trace application 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 (?).



---

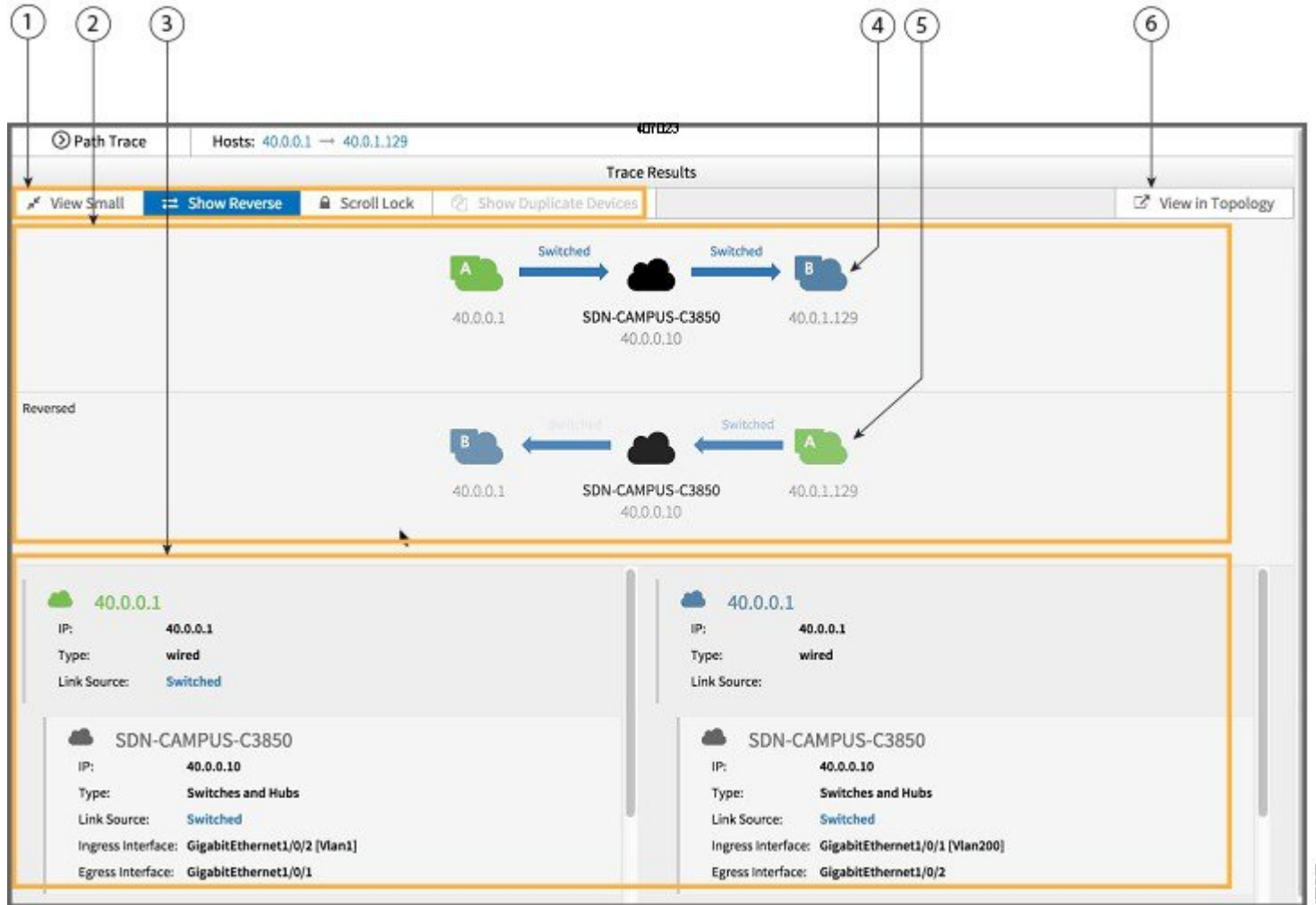
**Note**

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 perform a path trace, from the Navigation pane, click **Path Trace**. The **Path Trace** window opens.

**Figure 4: Path Trace Window**



Callout Number	Name	Description
1	Toolbar	Contains tools that act on the path trace shown in the <b>Trace Results Graphical Display</b> .
2	<b>Trace Results Graphical Display</b>	Shows a graphical representation of the path trace.
3	<b>Trace Results Details</b>	Provides detailed information about the devices along the path.
4	<b>Original Trace Results</b>	Shows the path trace from the source host to the destination host.

Callout Number	Name	Description
5	<b>Reverse Results</b>	Shows the path trace in reverse order, from the destination host to the source host.
6	<b>View in Topology</b> button	Displays the trace results in the Topology window.  <b>Note</b> The trace results are not preserved when you exit the <b>Path Trace</b> window. If you click <b>View in Topology</b> to view the trace results in the <b>Topology</b> window and then return to the <b>Path Trace</b> window, the trace results that you were previously viewing are no longer shown.

### Related Topics

[Performing a Path Trace, on page 27](#)

## 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**

<b>Supported Device Protocols and Network Connections</b>	<b>Description</b>
Border Gateway Protocol (BGP)	<p>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.</p> <p>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.</p>
Equal Cost Multi Path (ECMP)	<p>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.</p> <p>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.</p> <p><b>Note</b> The controller's GUI will display when ECMP is used between devices in a path trace segment.</p>
Hot Standby Router Protocol (HSRP)	<p>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.</p> <p>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.</p>
Intermediate System-to-Intermediate System (IS-IS) Protocol	<p>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.</p> <p>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.</p>
Layer 3 Forwarding Interface	<p>The controller can perform path traces between two Layer 3 forwarding interfaces or between a Layer 3 forwarding interface and a host.</p>

Supported Device Protocols and Network Connections	Description
MPLS-VPN (WAN)	<p>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:</p> <ul style="list-style-type: none"> <li>• Cisco ASR 1000 Series Aggregation Services Router</li> <li>• Cisco ASR 9000 Series Aggregation Services Router</li> <li>• Cisco Integrated Services Routers (ISR) G2</li> </ul> <p>All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers.</p> <p><b>Note</b> The above supported devices will be tagged as <b>Border Routers</b> for their <b>Device Role</b> in the <b>Device Inventory</b>. You must keep the above supported devices tagged as <b>Border Routers</b> when performing a path trace.</p> <p>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.</p>
Open Shortest Path First Protocol (OSPF)	<p>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.</p> <p>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.</p>
Physical connectivity (Ethernet, Serial and Packet over SONET (PoS))	<p>The path trace for a given application flow can be displayed over Ethernet, Serial over SONET, and Packet over SONET.</p> <p>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.</p>
Spanning Tree Protocol (STP)	<p>The controller provides Layer 2 support for Spanning Tree Protocol (STP).</p> <p>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.</p>



Supported Device Protocols and Network Connections	Description
Static Routing	<p>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.</p> <p>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.</p>
Virtual connectivity—Layer 2 Port Channel	<p>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.</p>
Virtual connectivity—VLAN/SVI	<p>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.</p> <p>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.</p>
Wireless	<p>The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility.</p> <p>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.</p> <p><b>Note</b> The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace.</p> <p>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.</p>

<b>Supported Device Protocols and Network Connections</b>	<b>Description</b>
Equal Cost Multipath/Trace Route (ECMP/TR)	<p>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.</p> <p>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.</p>
Netflow	<p>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.</p> <p>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.</p>
Sub interfaces	<p>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.</p>
Enhanced Interior Gateway Routing Protocol (EIGRP)	<p>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.</p> <p>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.</p>

Supported Device Protocols and Network Connections	Description
Layer 3 Recursive Lookup	<p>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.</p> <p>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.</p>

## 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 an accuracy notice—a red box with a percentage number in. An accuracy notice that appears on a node or path segment indicates the accuracy level of the path based on the information used to determine the path. Click the accuracy notice to display suggestions for you to take to improve that path trace's accuracy. You can use these suggestions to adjust the device configurations on the path and then perform a second trace for a more accurate result.

### Before You Begin

Scan your network using the discovery function to populate device and host inventory for the database.

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

### Step 1

In the Navigation pane, click **Path Trace**.  
The **Path Trace** window appears.

### Step 2

In the **Source IP** field, enter the IP address of the first host or the Layer 3 forwarding interface.  
To determine the current list of hosts recognized by the controller, display the **Host Inventory** table.  
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 3

In the **Destination IP** field, enter the IP address of the second host or the Layer 3 forwarding interface.  
To determine the current list of hosts recognized by the controller, display the **Host Inventory** table.  
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** (Optional) In the **Source Port** field, enter the port number of the first host.
- Step 5** (Optional) In the **Destination Port** field, enter the port number of the second host.
- Step 6** (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
- Step 7** Click **Trace**.  
Review the path trace output. For more information, see [Understanding Path Trace Results, on page 28](#).
- Step 8** 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 [Topology, on page 3](#).
- 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.

### Related Topics

[About Path Trace, on page 19](#)

## Understanding Path Trace Results

After you run a path trace, the controller displays the results in the **Path Results** pane.

### Toolbar

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

<b>View Small</b>	Minimizes the trace path graphic to better view the trace path details.
<b>Show Reverse</b>	Displays the trace path graphic 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.
<b>Scroll Lock</b>	Locks the scrolling of the path trace and reverse path trace details windows. (Available when <b>Show Reverse</b> is enabled.)
<b>Show Duplicate Devices</b>	Displays or hides duplicate devices within a path trace.
<b>View in Topology</b>	Opens the <b>Topology</b> window and highlights the path trace results in your network topology. For more information about using the Topology window, see <a href="#">Topology, on page 3</a> .



---

**Note** Depending upon the trace results, some of the above buttons may be grayed out and not available.

---

### Trace Results Graphical Display

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 and destination.
- Link Information Source—Whether the path source between devices is either **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.



---

**Note** If the path trace is lengthy and involves many devices, clicking an individual device in the path trace adjusts the GUI view to focus on that specific device. You can then scroll the view either up or down from that specific device.

---

### Trace Results Details

Review the detailed information displayed for each device in the path trace:

<b>IP</b>	IP address of the device.
<b>Type</b>	Wired or wireless device (access point, switch, or router).

<b>Link Source</b>	<p>Assuming two devices in a path (device A and device B) and the path direction is from device A to device B, then depending upon your network configuration, the following link information source types might be displayed:</p> <ul style="list-style-type: none"> <li>• <b>BGP</b>—Link is based on the BGP routes configured on device A.</li> <li>• <b>ECMP</b>—Link is based on a Cisco Express Forwarding (CEF) load balancing decision.</li> <li>• <b>EIGRP</b>— Link is based on EIGRP routers configured on the device A.</li> <li>• <b>Connected</b>—Device B is directly connected to device A.</li> <li>• <b>InterVlan Routing</b>—There is an SVI configuration on the device A from which the path is switched to device B.</li> <li>• <b>ISIS</b>—Link is based upon the IS-IS routes configured on device A.</li> <li>• <b>NetFlow</b>—Link is based on NetFlow records collected on device A for source and destination.</li> <li>• <b>OSPF</b>—Link is based on the OSPF routes configured on device A.</li> <li>• <b>Static</b>—Link is based on a static route.</li> <li>• <b>Switched</b>—Link is based on Layer 2 VLAN forwarding.</li> <li>• <b>Trace Route</b>—Link is based on trace route.</li> <li>• <b>Wired</b>—Device A is a wired host connected to device B.</li> <li>• <b>Wireless</b>—Device A is a wireless host connected to device B (Access Point).</li> </ul>
<b>Tunnels</b>	<p>CAPWAP data (wireless) or mobility tunneling</p> <p><b>Note</b> The controller provides a graphical view of path trace CAPWAP tunnel around the devices involved. You are able to auto-adjust the view by zooming in or out.</p>
<b>Ingress interface</b>	<p>Ingress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical ingress interface is <b>GigabitEthernet1/0/1</b> and a virtual ingress interface is <b>GigabitEthernet1/3 [Vlan1]</b>.</p>
<b>Egress interface</b>	<p>Egress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical interface is <b>GigabitEthernet1/0/2</b> and a virtual ingress interface is <b>GigabitEthernet1/4 [Vlan2]</b>.</p>
<b>Accuracy note</b>	<p>If there is uncertainty about the path trace on a segment between devices, a note about the accuracy of the computed path on this segment is displayed as a percentage.</p>