Trace the Path of a Device

- About Path Trace, on page 1
- Path Trace Known Limitations, on page 1
- Perform a Path Trace, on page 3

About Path Trace

You can perform a path trace between two nodes in your network—a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts or Layer 3 interfaces or both. In addition, you can specify the protocol that the Cisco DNA Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Cisco DNA Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

Path Trace Known Limitations

Path trace has the following limitations and restrictions.

- Path trace between a fabric client and a nonfabric client is not supported.
- Path trace between two fabric clients over multi virtual routing and forwarding (VRF) virtual networks (VNs) is not supported.
- Path trace between two fabric clients over multi sites (domains) is not supported.
- Clients connected in the same fabric and same site where either edge switch is not part of the fabric is not supported.
- Path trace from a router's loopback interface is not supported.
- Overlapping IP addresses are not supported with or without fabric.
- For path trace to work on a Locator ID/Separation Protocol (LISP) fabric, make sure that the traffic is running and cache is available on the edge switches.

- Path trace in Cisco Adaptive Security Appliances (ASA) is not supported because Cisco ASA does not support CDP. It is not possible to identify the path through the Cisco ASA appliance.
- Path trace is not supported for the management interface in wireless controllers in untagged mode.
- Path trace for centralized Wireless Mobility Modes Asymmetric Mobility Tunneling is not supported.
- Path trace for Virtual Switching System (VSS), Multi-Link Aggregation Control Protocol (MLACP), or Virtual PortChannel (vPC) is not supported.
- Path trace for Equal-Cost Multi-Path Routing (ECMP) over Switched Virtual Interface (SVI) is not supported.
- Path trace is not supported on devices with NAT or firewall.
- Cisco Performance Routing (PfR) is not supported with DMVPN tunnels.
- Path trace that has VLAN ACLs (VACLs) enabled is not supported.
- For a Non Periodic Refresh (NPR) path scenario, after an upgrade, the controller does not refresh the path. Additionally, statistics collection stops. To continue statistics collection, you must initiate a new path request.
- Path trace from a host in a Hot Standby Router Protocol (HSRP) VLAN to a host in a non-HSRP VLAN that is connected to any of the HSRP routers is not supported.
- Object groups are not supported in an ACL trace.
- Port-channel Port Aggregation Protocol (PAgP) mode is not supported. Only LACP mode is supported.
- Applying a performance monitor configuration using Cisco DNA Center fails if there is a different performance monitor policy configuration on the interface. Remove the performance monitor configuration on the interface and resubmit the path trace request.
- Path trace for Performance Monitor statistics is not supported for Cisco ASR 1000 Series routers (Cisco IOS XE 16.3.1).
- Path trace for Performance Monitor statistics is not supported for the Cisco Catalyst 3850 Switch (Cisco IOS XE 16.2.x and 16.3.1).
- Path trace for Cisco Mobility Express (ME) wireless controllers is not supported.
- Path trace for wireless clients that use OTT in Cisco SD-Access fabric is not supported.
- Path trace from a Layer 2 switch is not supported.
- Cisco's Industrial Ethernet (IE) Switches are extended nodes as part of the SD-Access solution. Currently, path trace does not recognize extended nodes, so if a topology contains extended nodes, you will get an error message.
- Dual stack that has both IPv4 and IPv6 addresses for devices is not supported. If this occurs, an error message displays stating that the given address is unknown.
- Because Cisco wireless controllers do not send SNMP mobility traps, note the following:
    - For a path trace request, Cisco DNA Center does not have the right egress virtual interface highlighted on any foreign wireless controller.
    - The path trace request does not highlight any ACLs applied on the foreign wireless controller.

Note The workaround is to wait for the inventory cycle to complete.

Perform a Path Trace

The path trace feature works in a similar manner in all the devices. You can perform a path trace from the **Client 360** or **Device 360** window.

Before you begin

- Review the path trace known limitations. See Path Trace Known Limitations, on page 1.
- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, Discover Your Network Using CDP, or Discover Your Network Using LLDP.
- Make sure that CDP is enabled in the devices.

Step 1 From the **Client 360** or **Device 360** window, in the **Path Trace** category, click **Run New Path Trace**.
The **Set up Path Trace** slide-in pane appears.

Step 2 Enter the source IP address, interface, and port number; and the destination IP address, interface, and port number.

Field	Action
Source field	The IP address in the **Source** field is prepopulated; however, you can enter another source IP address by doing the following: • Enter the source IP address. • Click the **Source** field, and then choose an IP address from the available options.
Interface (optional) field	Choose an interface from the drop-down list. **Note** This field is displayed if the source IP address is a network device.
Port (optional) field	Enter the port number of the host from which you want the trace to start.
Destination field	Do one of the following: • Enter the IP address of the host or the Layer 3 forwarding interface at which you want the trace to end. • Click the **Destination** field, and then choose an IP address from the available options.
Interface (optional) field	Choose the interface from the drop-down list. **Note** This field is displayed if the IP address you choose in the Destination field is a network device.

Field	Action
Port (optional) field	Enter the port number of the host from which you want the trace to end.

Step 3 From the **Options** area do the following as appropriate:

Field	Action
Protocol drop-down list	(Optional) Choose either **tcp** or **udp**.
Live Traffic	Enable this toggle to **On** to capture the network packets traveling through select devices in real time as a .pcap file. **Max number of packets to capture** drop down list - Select the maximum number packets to be captured. **Note** **Refresh Every 30sec** toggle button gets disabled automatically when you enable **Live Traffic** toggle button and vice versa.
Refresh Every 30sec	(Optional) Set this toggle to **On** to configure the path trace topology to refresh every 30 seconds.
ACL Trace	(Optional) Set this toggle to **On** to display matched ACLs and the ACL result (Permit or Deny) for a specific traffic flow.
Include Stats options	(Optional) To configure the path trace to collect additional statistics, check the following check boxes as needed: • **Device**: Collects and displays information, such as the device CPU and memory usage. • **Interface**: Collects and displays information about the device interface. • **QoS**: Collects and displays QoS information, such as collector-voice-egress, collector-broadcast-video-egress, collector-real-time-interactive-egress, and so on.

Step 4 Click **Start**.
The path trace topology appears. The IP addresses, protocol, and the time stamp indicating when the path trace was last updated display above the topology.

Step 5 In the path trace topology, you can do the following:

a) Hover your cursor over a device to display the following information:

- CPU utilization
- Memory utilization
- Average processing delay of ACLs, tunneling, and queues
- Packet forward decision, which includes the number of packets forwarded and dropped and the drop reason

If **ACL Trace** is set to **On**, the ACL name and ACL result, such as permit or deny display.

If the following 5-tuple values (source IP address and port number, destination IP address and port number, and the protocol in use) are provided, then the ACL trace that is displayed in 100% accurate. If partial information is provided,

the ACL trace that is displayed is on best effort basis. In such a case, the ACL results might display both Permit and Deny.

Matched ACLs in a specific traffic flow are displayed with a colored icon. Green indicates **Permit**. Red indicates **Deny**. For Ingress ACLs, the icon appears on the left side of the device. For Egress ACLs, the icon appears on the right side of the device.

b) Click a device to open a slide-in pane with additional device details.
c) Hover your cursor over a Layer 2 or Layer 3 port channel interface to display information, such as used VLANs and output drops. Click **More Details** to open a slide-in pane with additional information.
d) Hover your cursor over the path to display the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.