

Network-Wide Path Insights on SD-Routing Devices

Information About Network-Wide Path Insight on SD-Routing Devices

NWPI is a diagnostic tool natively built into Cisco SD-WAN Manager that helps network administrators find the source of the network issues that users face from time to time while accessing their applications residing on-prem or in the cloud. It provides end-to-end application-tracing serviceability in a Cisco Catalyst SD-WAN network and lets the network administrators initiate application tracing and displays the trace results collected from multiple devices in a consolidated view. NWPI also provides comprehensive analyses of traffic flows in the network with information on applications accessed by users, classification of business-critical flows, monitoring and reporting of network delays, troubleshooting tips, and graphical deep insights into flow analyses.

How Network-Wide Path Insights work on SD-Routing Devices


SD-Routing uses Cisco Catalyst SD-WAN Manager to manage and optimize network paths. NWPI integrates with the SD-WAN Manager to gather detailed path information for UDP and TCP traffic. The network operator starts the process by creating an NWPI trace.

In a DMVPN or FlexVPN scenario with NHRP configured, NWPI trace works in Network-Wide mode. Here, DMVPN CMD carries NWPI metadata. As the data travels through routers, each router uses the NWPI metadata to send flow information back to the Manager. It then integrates all the received data into a unified view. In other scenarios, NWPI trace works in standalone mode. No metadata is added, and only the first router's flow information is sent to the SD-WAN Manager

Working Modes of NWPI on SD-Routing Devices

Table 1: Working modes of NWPI on SD-Routing Devices

Mode	Description	Traffic Flow Details
Standalone Mode	Shows the first hop router's information only.	<ul style="list-style-type: none"> Traffic flow from site to the internet (DIA) or WAN (MPLS VPN CE site - PE). Traffic flow from site to site via P2P GRE or GRETP tunnel. Traffic flow from site to site via P2P SVTI tunnel.

Mode	Description	Traffic Flow Details
Network Wide Mode	Provides end-to-end path across multiple sites with network-wide correlation.	<ul style="list-style-type: none"> Traffic from spoke via DMVPN tunnel (DMVPN phase 1/phase 2/phase 3). Traffic from spoke via FLEXVPN tunnel with NHRP enabled. <p> Note Network Wide Mode leverages DMVPN CMD for NWPI metadata across sites. DMVPN's network-id is shown as Local and Remote transport unique ID.</p>

Prerequisites for Network-Wide Path Insights on SD-Routing Devices

Ensure that the Data Stream option is enabled in Cisco SD-WAN Manager. In a Cisco Catalyst multitenant deployment, you must have the provider role to enable this option. To enable this option, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. For the **Data Stream** option, click **View**.
3. Click **Edit** and choose **Enable**.
4. Click **Save**.

Restrictions for Network-Wide Path Insights on SD-Routing Devices

- NWPI traces only UDP and TCP traffic
- Not all packet traces are captured per flow. The system automatically samples the most typical packets.
- You can monitor up to two traces per device and a maximum of 10 concurrent active traces per Cisco Catalyst SD-WAN Manager tenant.
- The number of active flows monitored ranges from 50 to 100 per device, with a maximum of 60,000 supported completed flows.
- Path insight does not display correctly if IPv6 is used as the underlay for the DMVPN tunnel.
- NWPI does not provide accurate information in VASI deployments.
- NWPI does not work properly when platform QoS port-channel-aggregate is enabled.
- Path insight does not show correct information if NAT64 or NAT46 occurs.
- NWPI cannot display MPLS information if the first hop is an MPLS PE router.
- NWPI Domain probe traffic cannot go over a tunnel.

- When starting a trace, you cannot specify the source interface on SD-Routing devices.
- When NWPI traces traffic over VTI tunnel on some platforms, downstream hop's LocalEdge is Unknown.

Configure Network-Wide Path Insights Tracing



Note

By default, starting an SD-Routing trace on a HUB site fails and generates an alarm. If you still want to start the trace on a HUB site, disable **Network-Wide** under **Monitoring Settings** and then start the trace again.

To start an SD-Routing trace, follow these steps.

-
- Step 1** Initiate a New Trace.
- From the Cisco SD-WAN Manager menu, choose **Tools > Network Wide Path Insight** and click **SD Routing** on the top-right.
 - Click **New Trace**.
 - (Optional) **Enable DNS Domain Discovery** if needed. Enabling this option provides information for DNS domains, especially in Direct Internet Access (DIA) deployments. For more details on the steps about DNS domain discovery, hover over the **microcopy** below **Enable DNS Domain Discovery**.
 - Enter a name for the trace in the **Trace Name** field.
 - Enter the trace duration in the **Trace Duration** field. The default value is 60 minutes.
- Step 2** Configure Basic Trace Settings.
- Select the **Site** in which you want the trace to run.
 - Choose the service VPN from the **VPN** drop-down list. This is the identifier of a VPN in which the application flow will be traced.
 - Select the appropriate **WAN Transport Interface(s)**. For an SD-Routing device to participate in the network, at least one interface must connect to a WAN transport network. For more details, hover over the **microcopy** below **WAN Transport Interface**.
 - (Optional) Specify **Source and Destination IP addresses/prefixes** if DNS domain discovery is disabled. This refers to the Source and Destination IP address of the traffic that the trace monitors.
 - (Optional) Choose the name of the **Application** or **Application groups** to monitor.
- Step 3** (Optional) Configure Advanced Filters
- Select specific devices, source ports, destination ports, protocols, and DSCP types for the trace.
- Step 4** (Optional) Configure Monitoring Settings
- Enable **QoS Insight** for throughput and drop-rate metrics. This option is enabled by default.
 - Enable **ART Visibility** for application response time metrics. This option is enabled by default.
 - Enable **App Visibility** for discovering applications using SD-Routing Application Intelligence Engine. This option is enabled by default.
 - Enable **Network-Wide** tracing to perform extensive tracing across the entire network. This option is enabled by default. Network-Wide tracing only applies on DMVPN Tunnel and NHRP/CMD based site to site FlexVPN Tunnel.
 - Enable **Sampling** and set the interval to capture flows at specified intervals.
 - Set **Local Drop Rate Threshold** and **WAN Loss Rate Threshold**.

Step 5 (Optional) Configure Grouping Fields

Enable **Client Prefix** and **Server Prefix** to additionally group information. Enabling these fields can refine the display of information to meet your preferences.

Step 6 (Optional) Configure Synthetic Traffic

- a) Enter the URL, service VPN, DNS server, DSCP, and interval for synthetic traffic. Enabling synthetic traffic generates sample user traffic that you can evaluate with other NWPI features to check whether applications are working as expected.
- b) (Optional) Add additional synthetic traffic instances if needed.

Step 7 Start and review the trace

- a) Click **Start** to initiate the trace.
- b) Review the trace information in the **Start Trace** window.
- c) **Close** the **Start Trace** window.

Network-Wide Path Insight Tracing is complete, and it is displayed in the list of traces in the **Tools > Network Wide Path Insight** window.

View and Manage Trace Information

The path trace instances appear with unique trace IDs in the Trace area. Information about each instance is also displayed, including its state and the actions that you can perform. The following table describes the fields in the **All Trace** area and the action that the network administrators can perform. Note that you can view the **Multi-Traces Insight summary** by selecting the checkbox next to **Trace Names**.

Table 2: View and Manage Trace Information

Parameter	Description
Trace Name	Trace name and the Insight Summary link, which provides you more information about the traces.
Trace ID	System-generated identifier of the trace.
Start Time	Date and time at which you started the trace.
Stop Time	Date and time at which the trace ended.
Src.Site	Source of a trace.
VPN	Identifier of the VPN in which the application flow was traced.
Application/App Group	The Applications or Application Groups that a trace monitors.
Domain	Mentions if the DNS Domain Discovery was enabled or disabled.
Trace State	View the status of a trace and error messages, if any, that have been generated.

Parameter	Description
Action	<ul style="list-style-type: none"> To view detailed information about the flows in the Insights section, click View Insight. Click Delete to remove a trace from the table. Click Stop to stop an active trace. Note that a stopped task cannot be restarted.

Display Insight Summary

An insight summary provides trace-level insight information for application traffic and flows. This information appears in a slide-in pane. In the **All Trace** section, click **Insight Summary** in the Trace Name column for the trace that you want.

Overview

The **Overview** tab displays the following information on Sampled Flow Insight and Application Statistics respectively.

Table 3: Sampled Flow Insight

VPN	This is the identifier of a VPN in which the application flow will be traced. In the VPN field, information for all the VPNs that the trace detects is selected by default.
Application	Displays information for all flows that include application traffic. Select the Application check box to enable the same. This option is enabled by default.
DNS	Displays information about each domain that the trace discovers. Select the DNS check box to display information for all the flows with DNS resolution.
Applications Graph	Displays the number of flows that the trace detects in each application in the monitored traffic. Hover your cursor over the data points in the graph to display the percentage of total flows that the corresponding application flow represents.
Critical, Warning, and Informational	To display information for events that have the corresponding severity level enable Critical , Warning or Informational as per your preference.
Events Graph	Displays the events that the trace detects in the monitored traffic and the number of application flows that each event affects. Hover your cursor over the data points in the graph to display the percentage of total application flows that the corresponding event affected.
Events	Choose the preferred Events from the drop-down list. By default, all the events that the trace detects appear in this field.

Hotspot issues [Local Drop, Server No Response, WAN Loss(>5%)]	Provides information about each application flow that was affected, including the traffic path in which the event occurred and the duration of the event.
--	---

Table 4: Application Statistics

VPN	Select the preferred VPN from the VPN drop down list.
Transport Interface	Select the preferred Interface from the Transport Interface drop down list.
Device	Select the preferred Device from the Device drop down list.
Applications (top 10) - Total Flows	Total number of application flows for the duration of the trace. The selected color is for the egress WAN interface on which flows were initialized.
Applications (top 10) - Total Bytes	Overall application bidirectional bandwidth for the duration of the trace. Upstream and downstream flow bandwidths are counted on the egress WAN on which flows were initialized.
APP Metrics/APP Metrics(Min/Ave/Max)	The Min, Ave, Max data in charts show the minimum, average, and maximum values for the duration of the trace. Choose APP Metrics or APP Metrics(Min/Ave/Max) according to your preference. Metrics are calculated at interval of one minute.
Applications (top 10) – Flow Setup Rate	New incoming flows per second, calculated at 1-minute intervals.
Applications (top 10) – Active Flow	Number of active flows, calculated at 1-minute intervals.
Applications (top 10) – Bandwidth	Number of KB per second, calculated at 1-minute intervals.
Applications (top 10) – Flow Live Time	Overall lifetime of application flows, based on the flows completed within the monitor interval and calculated at 1-minute intervals.

App Performance Insight

The **App Performance Insight** tab displays the following information.

Table 5: App Performance Insight

Field	Description
VPN	Information for all the VPNs that the trace detects are selected by default.
Group Fields	
Server Side Group By	You can arrange the information that displays into groups, according to the items that you choose in the Group Fields area.

Field	Description
Application	The five applications with the most hotspot issues appear in the Application field by default.
Hop Metrics	
Hop	Select the preferred Hop from the drop-down list.
Score graph	Provides an evaluation of application performance.
Detailed Application Metrics	
Loss graph	Provides information about packet loss.
Delay graph	Provides information about delays in the traffic flows.
Jitter graph	Provides information about the inconsistencies in latency in traffic flows.
CND/SND graph	Provides information about client network delay (CND) and server network delay (SND).
Application Path & Performance graph	Provides a snapshot of bandwidth used and loss information at a particular time. You can choose the time by clicking a dot on a timeline in a metrics graph.

Event Insight

The **Event Insight** tab displays the following information about application flows that were affected during each minute of the duration of an event. You can use this information to assist with a root-cause analysis.

Table 6: Event Insight

Field	Description
VPN	Information for all the VPNs that the trace detects are selected by default.
Group Fields	
Server Side Group By	You can arrange the information that displays into groups, according to the items that you choose in the Group Fields area.
Application	The five applications with the most hotspot issues appear in the Application field by default.
Hop Metrics	
Upstream and Downstream	Click Upstream to display information for upstream traffic in the graph and chart. Click Downstream to display information for downstream traffic in the graph and chart.
Hop	Select the preferred Hop from the drop-down list.

Field	Description
Flow Graph	Provides information about the number of flows at a particular time.
Event	Choose the preferred Events from the drop-down list. By default, all the events that the trace detects appear in this field.
Application Path and Event Flow (Flow Count)	Provides detailed information about the effect of designated events at a particular time. Hover your cursor over a data point to see more information.

QoS Insight

The **QoS Insight** tab provides comprehensive network-wide information about which application traffic entered specific QoS queues on the devices detected during a trace. It includes details on all hops for the traffic. To display information on this tab, enable the QoS Insight option when you start the trace.

The QoS Insight tab includes both graphical and chart-based information as follows.

Table 7: QoS Insight

Field	Description
Devices	The graph and chart display information for each device that appears in the Devices field.
QoS Drop Rate Graph	Shows information about the packet or byte drop rates for the selected devices over the period of the trace.
Applications	Select the preferred Application from the Application drop down list. To provide complete information about bandwidth consumers that cause dropped packets, this tab displays information for all the applications on a device.
VPNs	Select the preferred VPN from the VPN drop down list. It also displays information for default VPN and all the service VPNs, regardless of the service VPNs that you choose by using the VPN filter when you start the trace.
Interfaces	Select the preferred Interface from the Interface drop down list. All the items that the trace detects are displayed in these fields by default, except items with a packet per second (PPS) rate of less than 0.05
Queues	Select the preferred Queues from the Queue drop down list. All the items that the trace detects are displayed in these fields by default, except items with a packet per second (PPS) rate of less than 0.05.

Field	Description
Forward/Drop	Select the preferred Forward/Drop from the V drop down list. All the items that the trace detects are displayed in these fields by default, except items with a packet per second (PPS) rate of less than 0.05.
QoS - Applications Distribution	Provides detailed information about the traffic spectrum and QoS processing at a particular time. It illustrates forwarded or dropped traffic in a flow from an application to a VPN, then to a physical interface, and finally to a queue.
Display packet drop rate information	Click Packet to show packet drop rate information in the graph and PPS information in the Sankey chart
Display byte drop rate information	Click Byte to show byte drop rate information in the graph and Kbps information in the Sankey chart.

View Trace Insights

To view detailed information about a flow in a specific trace, click **View Insight** in the Actions column of the trace list. The detailed information will appear in the Insight area, displaying the following:

DNS Domains

The DNS Domains section is available only when DNS domain discovery is enabled and displays information about each domain that the trace discovers. You can expand any row in the list to display detailed information about the application.

Click **Discovered Domains** to display information for every domain that the trace discovered but that are not yet traced. Click **Monitored Domains** to display information only for domains that the trace monitored.

The following table describes the information that appears for DNS Domain:

Table 8: DNS Domains

Field	Description
Check box	Select the check box for the domains for which you want monitoring to be enabled or disabled and click Start Flow Monitor or Stop Flow Monitor.
Application Group or App Group	Name of the application group that the trace discovered in the domain.
VPN	Identifier of the VPN in which the application flow was traced.
DNS Server	Destination of DNS packets sent from clients.
DNS Redirect	DNS resolver to which a device redirects DNS traffic if a resolver is configured by a centralized policy or by Cisco Umbrella.
Resolved IP	DNS-resolved IP address for the application.

Field	Description
DNS Transport	Transport type used by the domain.
DNS Egress	Egress interface and type used by the domain.
TTL (sec)	DNS time to live, in seconds.
Request	Number of DNS packets sent.
Monitor State	Status of flow monitoring for the domain.

Applications

The Application section displays information about applications that were traced. You can expand any row in this list to display bidirectional path information with hop-by-hop metrics for each application. Column with * mark means it was showing real-time metrics and statistics during the past 1 minute.

The following table describes the information that appears for Applications:

Table 9: Applications

Field	Description
Last Updated time	Date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
App Name	Name of the application.
App Group	Application group to which the application belongs.
VPN	Identifier of the VPN in which the application flow was traced.
Total bytes (K)	Number of KBs in the upstream and downstream flows of this application.
Total Packets	Number of packets in the upstream and downstream flows of this application.
KBPS*	Number of KBs per second in the upstream and downstream flows of this application during the past minute.
PPS*	Number of packets per second in the upstream and downstream flows of this application during the past minute.
Total Flows	Number of flows that were counted for the application.
Active Flows*	Flows that had activity during the past 1 minute.
Flow Setup Rate (s)*	Average number of new flows per second during the past 1 minute.
Flow Live Time (ms)	Max/Min/Avg: Maximum, minimum, and average number of milliseconds of detectable flow activity during the duration of the trace.

Field	Description
Sampled Flows	Number of flows that were sampled in the upstream or downstream traffic of this application.
Sampled Bytes (K)	Number of KBs that were sampled in the upstream or downstream traffic of this application.

Active Flows and Completed Flows

The Active Flows section displays information about the flows that are in the Running state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics. The Completed Flows section shows information about the flows that are in the Stopped state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics.

The following table describes the information that appears for Active Flows and Completed Flows:

Table 10: Active Flows and Completed Flows

Field	Description
+	<p>Click the + icon to view the following Expanded Application Information:</p> <ul style="list-style-type: none"> • Direction: Direction of the application flow (upstream or downstream). The first packet that the flow identifies is shown as a flow in the upstream direction. • HopIndex: Hop index number for each direction of the application. • Local Edge: Name of the local edge device (source) of the application. • Remote Edge: Name of the remote edge device (destination) of the application. Note, in DIA scenerio, remote Edge will be Internet. • Local Transport: DMVPN Network-Id in network-wide mode or Egress interface in DIA scenerio. • Remote Transport: DMVPN Network-Id in network-wide mode. Remote transport is N/A in DIA scenerio. If network-Id is not configured in some tunnel configuration such as GRETP or SVTI, this value will be Network-Id: 0 • Local Drop(%), Wan Loss(%),Remote Drop (%): Packet drop, as measured in the local and remote edge routers. Packet drop is also measured in the complete WAN network. • Jitter (ms), Latency (ms): Jitter and latency metrics of the application during the past minute. These values help with evaluating the application performance in real time • ART CND (ms)/SND (ms): Application response time, in milliseconds, for client network delay (CND) and server network delay (SND) during the past minute. • Total Packets, Total Bytes: For each direction of the application flow, the total number of packets and the total byte count of packets. • Queue: Queue name configured in QoS feature. • QDepthLimit/Max/Min/Avg: Limit, maximum, minimum, and average values of the QoS queue depth for the flow.
Start-Update Time	Destination IP address of the traffic that the trace monitors.
Flow ID	System-assigned identifier of the flow.

Field	Description
Readout	<p>Click the green tick icon to display detailed information about the flow readout on a slide-in pane. If the flow identifies an application issue, you can use this information to assist with a root-cause analysis.</p> <p>The slide-in pane includes the following information:</p> <ul style="list-style-type: none"> • Overview : Includes details about flow asymmetry, NAT translation detail, flow path change, and so on. • Routing Insight : Provides information about how a forwarding path was determined for a flow. This information includes the edge router name; destination IP address; IP address lookup and matched route information; route-receiving source protocol, preference, and metrics; flow path-routing candidates; method for deciding the flow path and the flow path used. • Path Visualization : Provides underlay hop information about each overlay hop in the flow.
VPN	Identifier of the VPN in which the application flow was traced.
Source IP	Source IP address of the traffic that the trace monitors.
Src Port	Source port of the traffic that the trace monitors.
Destination IP	Destination IP address of the traffic that the trace monitors.
Destination Port or Dest Port	Destination port of the traffic that the trace monitors.
Protocol	Protocol of the traffic that the trace monitors.
DSCP Upstream/Downstream	DSCP type that the trace monitors for upstream traffic and downstream traffic.
Application	Application that the trace monitors.
Application Group or App Group	Application group that the trace monitors.
Domain	Domain that the flow belongs to. Click a domain name to display the protocol from which the domain was recognized. This field shows information only for DNS and HTTPS protocol flows. For other flow types, this field displays Unknown.
ART CND(ms) /SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).

View Advanced Trace Insights

From Cisco SD-WAN Manager navigate to **Tools > Network Wide Path Insight** and expand the **Insight-Advanced Views** section to view trace flow information.

View Domain Trend

The Domain Trend section is available when DNS discovery is enabled and displays metrics and event trends in an application flow. By hovering over the data points, you can see detailed information.

Metrics like client network delay (CND) and server network delay (SND) are measured by the application's TCP traffic. The DNS request frequency indicates how often a SaaS application is accessed. HTTP probe response time and loss rate are measured by router probes sent to the SaaS application server. These help detect a reachable direct internet access (DIA) network path and evaluate the benefits of deploying a DIA traffic policy.

You can choose metric types and specific devices from the **Chart Metrics** and **Devices** drop-down lists, respectively. By default, the section shows trend information for all metric types and devices. Additionally, you can limit the displayed trends to a specific time frame, choosing from predefined periods of 1, 10, or 30 minutes, or 1, 2, or 5 hours. For custom time ranges, you can enter a date and time or select **Real Time** to display live information.

View Flow Trend

The Flow Trend section shows trends for metrics and events in a trace flow. Hover over data points to see detailed information.

Use the **Chart Metrics** drop-down list to select specific metric types for viewing. The **Flow Direction** drop-down list allows you to choose the traffic flow direction for data display. By default, trend information is shown for latency, jitter, WAN loss and average queue depth.

To view information about a specific event, use the Navigate to Event drop-down list. You can limit the display to trends within a specified time frame or period, choosing from 1, 10, or 30 minutes, or 1, 2, or 5 hours. For custom time ranges, enter a date and time to see information as it is collected.

View Upstream and Downstream Feature Views

To view the details of the flow, expand a flow record in the flow path and metrics table by clicking on the + icon. The Upstream and Downstream Feature View provides a list of ingress and egress features applied to the flow, along with the execution results of each feature.

Troubleshooting Network-Wide Path Insight

Table 11: Problem 1: No Information Displayed in Trace Results

Issue	Action
Data stream collection might not be operating properly.	To resolve this issue, choose Administration > Settings > Data stream , click Disabled , then click Save . Click Data stream again, click Enabled , choose System for the IP address type, then click Save .

Issue	Action
DNS domain discovery might be enabled for the trace, but monitored traffic is not enabled from DNS domains.	To resolve this issue, choose Tools > Network Wide Path Insight , deselect the Enable DNS Domain Discovery check box in the Trace area, and run the trace again.