



Use Cases

- [Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy, on page 1](#)
- [Use Case 2: Troubleshoot Network Quality on a Website, on page 5](#)

Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy

Assume that you have a deployment that includes several branch sites. One of these sites, the SJC branch, with a site ID of 3, has two WAN links: an MPLS link, and a public internet link through which the Microsoft cloud can be accessed directly.

In addition, assume that a Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of an Application-Aware Routing (App-route) policy, has been created and enabled for Microsoft Office 365 applications.

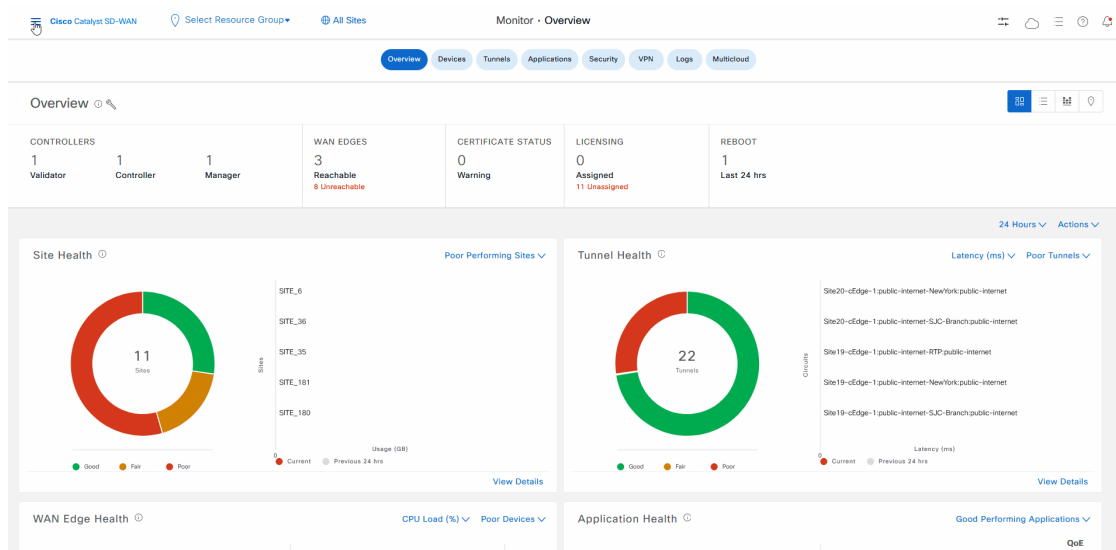
In this use case, let's see how network-wide path insight can be used to determine whether the traffic from Microsoft Office 365 applications is following the expected network path, validate that the policy is programmed correctly and operates as intended, and view the configuration of the policy.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools > Network Wide Path Insight**.
2. Click **New Trace**.
3. In the **Trace Name** field, enter a name for the trace.
In this use case, we use the name **Verify-Cor-Saas-Policy**.
4. From the **VPN** drop-down list, choose **VPN - 10**.
5. Click **Start**.

Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy

Figure 1: Start a Trace



Let the trace run for approximately 5 minutes so that it can collect data, then perform the following actions to see a Sankey diagram that shows the network paths of Microsoft Office 365 applications traffic. This application-level information lets you see whether the traffic is taking the expected network path according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Verify-Cor-SaaS-Policy** trace.
2. In the **Insight Summary** slide-in pane, choose the **App Performance Insight** tab and use the filters to see the Sankey chart that shows the network paths of Microsoft applications traffic.

The Sankey chart shows that this traffic flows directly from the SJC branch to the SaaS cloud-based host.

Figure 2: Display the Upstream Application Path & Performance Sankey Chart

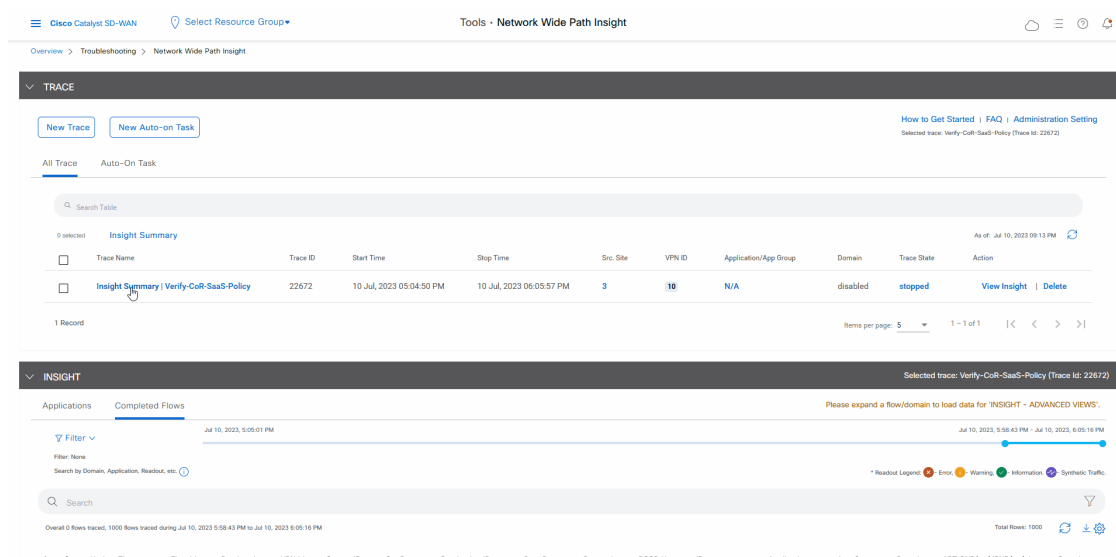
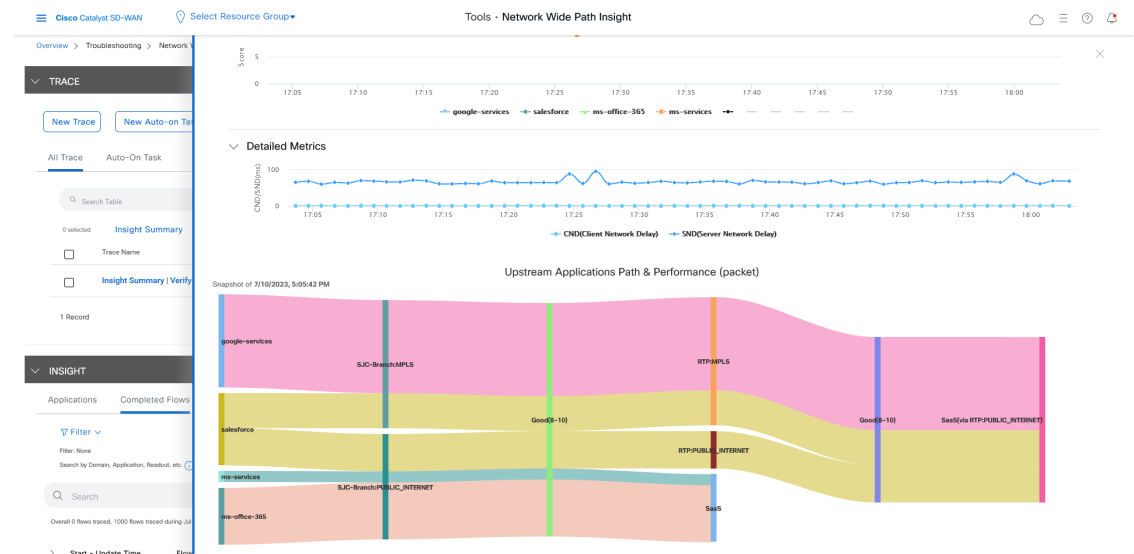


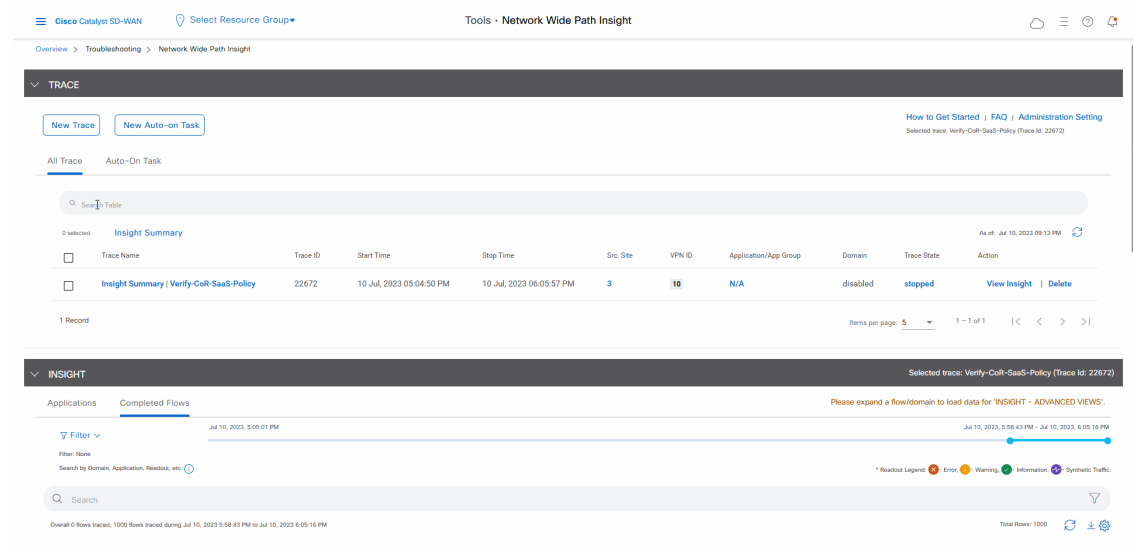
Figure 3: Upstream Application Path & Performance Sankey Chart



After reviewing application-level data, you can check whether your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy took effect for Microsoft Office 365 applications traffic. To do so, look at flow-level information for this traffic:

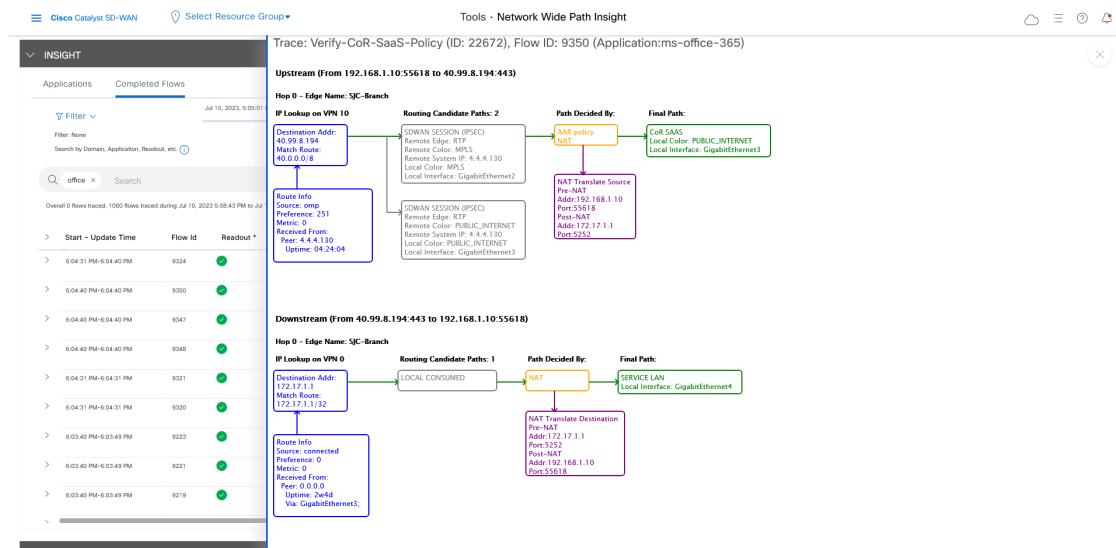
1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.
2. Search for **Office**.
3. For any Microsoft Office 365 flow, click the green check mark in the **Readout** column to display the **Flow Readout** slide-in pane.
4. Click the **Path Insight** tab in the **Flow Readout** pane.

Figure 4: View Flow-Level Information



Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy

Figure 5: Flow-Level Information



Finally, you can confirm how the App-route policy is programmed. This information lets you validate that Microsoft Office 365 applications traffic flows through the link that is intended according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of the App-route policy.


1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.
2. Expand any Microsoft Office 365 flow by clicking the right-arrow icon at the beginning of the row.
3. Scroll down to the **Insight – Advanced Views** area.
4. In the **Upstream Feature** tab:
 - a. Choose an event from the **Event List** drop-down list.
 - b. Click **Expand All Features** to see detailed ingress and egress information about the features that are executed for the flow, then click **Collapse All Features**.
 - c. In the **Ingress Feature** area, expand **SDWAN App Route Policy** to see policy information.
 - d. Click **View Policy** next to **SDWAN App Route Policy** to see the policy programming.


Figure 6: Confirm the Programming of the App-Route Policy





Tools - Network Wide Path Insight

Selected trace: Verify-CoR-SaaS-Policy (Trace ID: 22672)

Applications Completed Flows

Filter  Jul 10, 2023, 5:05:01 PM

Filter: Name
Search by Domain, Application, Readout, etc. 

Readout Legend:  Error  Warning  Information  Synthetic Traffic

Overall 0 flows traced, 1000 flows traced during Jul 10, 2023 5:58:43 PM to Jul 10, 2023 6:05:16 PM

Total Rows: 42 of 1000










>	Start - Update Time	Flow Id ...	Readout *	VPN Id	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms) *	Security
>	6:04:40 PM-6:04:40 PM	9350		10	192.168.1.10	55616	40.59.8.194	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	outlook.office	S/C-Branch: 0/110	N/A-N/A
>	6:04:40 PM-6:04:40 PM	9348		10	192.168.1.10	55602	40.59.8.194	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	outlook.office	S/C-Branch: 1/111	N/A-N/A
>	6:04:40 PM-6:04:40 PM	9347		10	192.168.1.10	42324	64.104.76.247	53	UDP(DNS)	DEFAULT * / DEFAULT *	ms-office-365(hs)	ms-cloud-group	outlook.office	N/A	N/A-N/A
>	6:04:31 PM-6:04:40 PM	9324		10	192.168.1.10	41449	13.107.6.156	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	Unknown	S/C-Branch: 0/43	N/A-N/A
>	6:04:31 PM-6:04:31 PM	9321		10	192.168.1.10	43164	13.107.6.156	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	www.office.co	S/C-Branch: 0/44	N/A-N/A
>	6:04:31 PM-6:04:31 PM	9320		10	192.168.1.10	56076	64.104.76.247	53	UDP(DNS)	DEFAULT * / DEFAULT *	ms-office-365(hs)	ms-cloud-group	www.office.co	N/A	N/A-N/A
>	6:03:40 PM-6:03:49 PM	9223		10	192.168.1.10	41910	52.98.43.130	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	outlook.office	S/C-Branch: 0/117	N/A-N/A
>	6:03:40 PM-6:03:49 PM	9221		10	192.168.1.10	41895	52.98.43.130	443	TCP	DEFAULT * / DEFAULT *	ms-office-365	ms-cloud-group	outlook.office	S/C-Branch: 0/116	N/A-N/A
>	6:03:40 PM-6:03:49 PM	9219		10	192.168.1.10	50880	64.104.76.247	53	UDP(DNS)	DEFAULT * / DEFAULT *	ms-office-365(hs)	ms-cloud-group	outlook.office	N/A	N/A-N/A

Figure 7: Detailed Information about the App-Route Policy

Cisco Catalyst SD-WAN
Select Resource Group
Tools · Network Wide Path In sight

0:04:40 PM-0:04:40 PM
0:048
10
192.168.1.1
192.168.1.1
192.168.1.1
192.168.1.1
ms-cloud-group
outlook-office - SJC-Branch 1/1/11
N/A-N/A

0:04:40 PM-0:04:40 PM
0:047
10
192.168.1.1
192.168.1.1
192.168.1.1
192.168.1.1
ms-cloud-group
outlook-office - N/A
N/A-N/A

0:04:31 PM-0:04:40 PM
0:024
10
192.168.1.1
192.168.1.1
192.168.1.1
192.168.1.1
ms-cloud-group
Unknown
SJC-Branch 0/4/3
N/A-N/A

INSIGHT - ADVANCED VIEWS

Flow Trend
Upstream Feature
Downstream Feature
Geographic

Hostname: SJC-Branch
Event List
FIRST_PACKET_OUT, ONGOING
Version: 17.13.0.1.2.101414, Input: OutputElement, Output: OutputElement
Selected trace: Verify-CoRt-SaaS-Policy (Trace ID: 22672)
Selected Flow ID: 9350

Ingress Feature

Ingress Report
ZBFW
CEF Forwarding
NAT
SDWAN ACL IN
SDWAN QoS Output
NBAR
QOS
SDWAN App Route Policy
Transmit Report

```

vrf ID      1  08
vrf        1  1
Policy name 1 - config_new-app-attach-vpn08 (CD-5)
Seq        1  1
Pkt Size    1 - ALL_TxRxLen_08
Act Size    1 - ALL_TxRxLen_08
Packets to be sent 1 - 0
SLA ID      1  08
Color name   1  08
Actual color 1 - UNRENDERED_08
Preferred color 1 - new_0801
Tunnel match reason 1 - NET6201_0802023_027
Classification
App ID      1  08
AppID      1  08
Path Type   1 - Client Local Exit
Exit Type   1 - Client Local Exit
Exit Type   1 - Client Local Exit
VRF Label   1  08

```

```

sequenceId: 11
sequenceType: appRoute
sequenceType ipv4
match
  ssaAppList office365_apps
  app:
    ms-lve-accounts
    ms-linc
    ms-linc-audio
    ms-linc-control
    ms-linc-video
    ms-office-365
    ms-office-web-apps
    ms-services
    ms-teams
    ms-teams-audio
    ms-teams-media
    ms-teams-video
    ms-update
    outlook-web-service
    share-point
    skydrive
    skype
    grove
    ms-stream
    ms-teams-app-sharing
  action
    count office365_apps_cr
  action
    cloudSaaS
sequenceId: 21
sequenceType: appRoute
sequenceType ipv4

```

Close

Use Case 2: Troubleshoot Network Quality on a Website

Assume that your users have trouble accessing the Google website and experience slowness after they are able to access.

In this use case, you'll see how to use network-wide path insight to determine the root cause of these issues.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools > Network Wide Path Insight**.
2. Click **New Trace**.

3. In the **Trace Name** field, enter a name for the trace.

In this use case, we use the name **Troubleshooting-Google**.

4. Click **Start**.

Let the trace run for approximately 5 minutes so that it can collect data, then follow these steps to determine the root cause of the issue:

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

A slide-in pane with detailed insight information appears. The **Overview** tab shows that 243 google-services flows are affected by local drop events and provides related detailed information for these flows.

2. In the **Events** area, click the link under “impacted 243 google-services flows” to display the **Completed Flows** tab in the **Insight** area on the **All Trace** tab.

Based on the link that you clicked, the table on the **Completed Flows** tab displays only information for google-services application flows that have a local drop event.

3. To see additional information for a particular flow, click the red X in the **Readout** column for the flow to display the **Flow Readout** slide-in pane.

The **Overview** tab on the **Flow Readout** slide-in pane shows that the flow is affected by a local drop event and provides related detailed information.

Figure 8: View Insight and Readout Information for Flows

The screenshot displays the Cisco Catalyst SD-WAN Network Wide Path Insight interface. The top navigation bar includes 'Tools - Network Wide Path Insight' and a 'Select Resource Group' dropdown. The main content area is divided into two sections: 'TRACE' and 'INSIGHT'.

TRACE Section:

- Buttons: 'New Trace', 'New Auto-on Task'.
- Navigation: 'All Trace', 'Auto-On Task'.
- Search: 'Search Table'.
- Table:

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
Insight Summary Troubleshooting-Google	22896	11 Jul, 2023 04:36:07 PM	11 Jul, 2023 04:42:45 PM	SITE_3	10	N/A	disabled	stopped	View Insight Delete
Insight Summary Verify-CoR-SaaS-Policy	22672	10 Jul, 2023 05:04:50 PM	10 Jul, 2023 06:05:57 PM	SITE_3	10	N/A	disabled	stopped	View Insight Delete

- Footer: '2 Records', 'Items per page: 5', '1 - 2 of 2'.

INSIGHT Section:

- Selected trace: Troubleshooting-Google (Trace Id: 22896).
- Navigation: 'Applications', 'Completed Flows'.
- Filter: 'Filter: None'.
- Search: 'Search by Domain, Application, Readout, etc.'.
- Timeline: Jul 11, 2023, 4:36:07 PM to Jul 11, 2023, 4:42:08 PM.
- Readout Legend: Error (red X), Warning (yellow triangle), Information (blue circle), Synthetic Traffic (purple circle).

Figure 9: Flow Insight Information

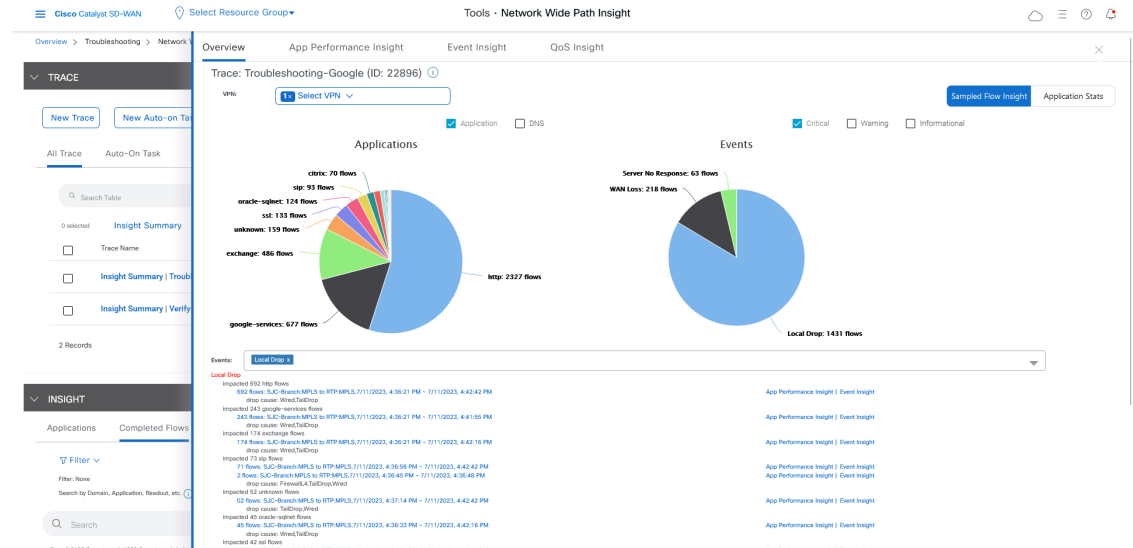
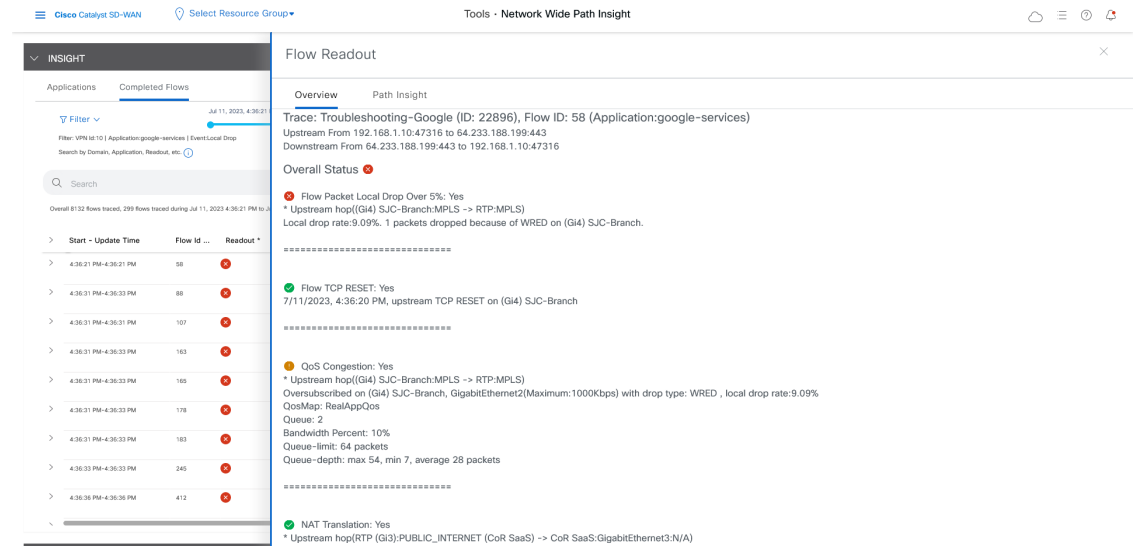


Figure 10: Flow Readout Information



You've now determined that the issue is related to local drop events. These events occur due to packets that are dropped because of network congestion, and they affect the quality of traffic flows on your network. Next, you can use network-wide path insight to answer the following questions that relate to QoS:

- Which queue is google-services traffic sent to?
- What applications besides google-services are consuming the bandwidth on this queue?

With the answers to these questions, you can take steps to reduce the congestion on the queue.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

Use Case 2: Troubleshoot Network Quality on a Website

2. In the **Insight Summary** slide-in pane, choose the **QoS Insight** tab.
3. In the **Applications** field, choose all applications to see which applications are consuming bandwidth on which queue, then choose the **google-services** application to see which queue is used by this application.

You can see that Google applications use queue 2, but many other applications also use this queue. These applications using the same queue are causing congestion.

Using the information that you found, you can reduce congestion and address the issues that your users experience when they visit the Google website by performing any of the following actions:

- Adjust the QoS policy for the queue,
- Move the Google application to another queue
- Move other applications to another queue

Figure 11: View QoS Information

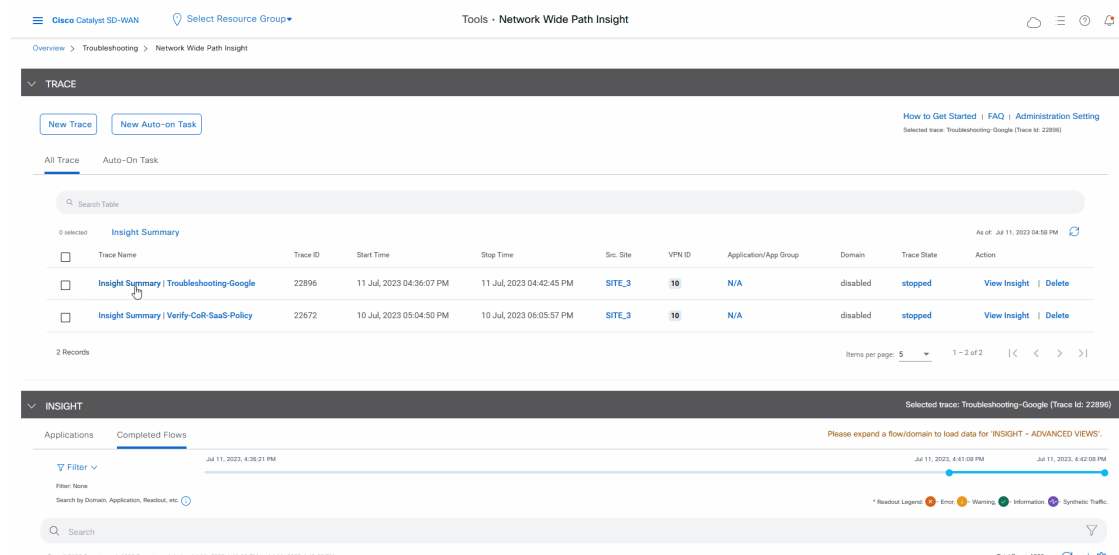


Figure 12: QoS Information for All Applications

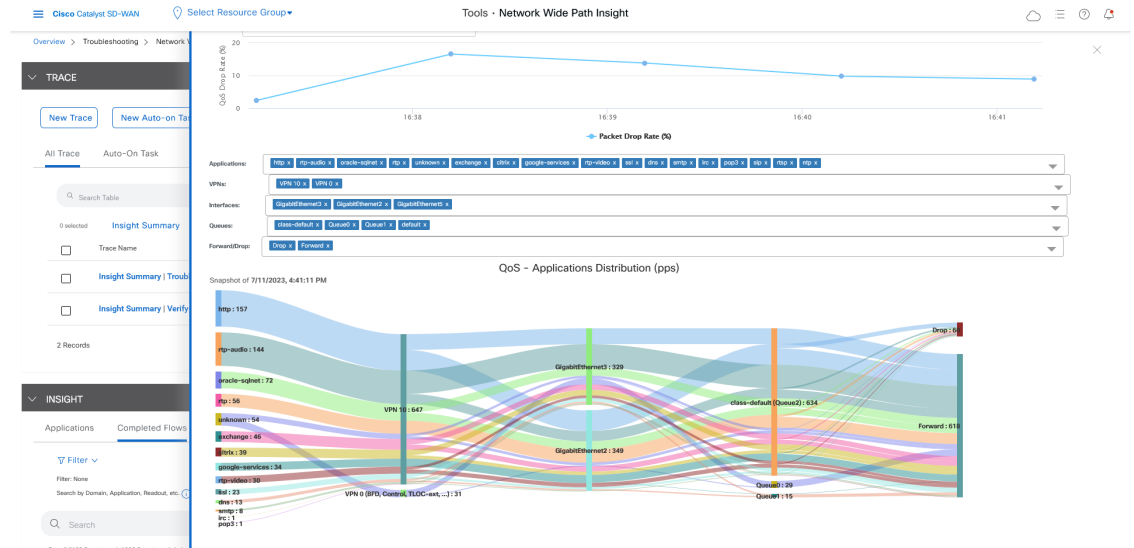


Figure 13: QoS Information for the google-services Application

