



CHAPTER 36

Working with Network Analysis

This chapter describes how to use the Network Analysis (PONG) feature in Cisco Data Center Network Manager for LAN (DCNM-LAN).

This chapter includes the following sections:

- [Information About Network Analysis, page 36-1](#)
- [Licensing Requirements for Network Analysis, page 36-1](#)
- [Prerequisites for Network Analysis, page 36-2](#)
- [Guidelines and Limitations for Network Analysis, page 36-2](#)
- [Using the Network Analysis Feature, page 36-2](#)
- [Related Documents, page 36-8](#)
- [Feature History for Network Analysis, page 36-8](#)

Information About Network Analysis

The Network Analysis feature provides you with information to track and monitor the latency between two specified switches in a specified time interval. With Network Analysis, you can determine the health of the network by examining the delay between the two specified points in the network.

The Network Analysis feature:

- Supports real time and historical network analysis between two user specified devices or ports. The user specifies the required monitoring intervals.
- Supports an archive of historical Network Analysis measurements for the following:
 - End to end round trip time.
 - Switching delay at each hop.
 - Link delay between hops per path.
- Provides reports that contain the resulting statistical information as a chart or summary table.

Licensing Requirements for Network Analysis

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|----------------|---|
| Cisco DCNM-LAN | The Network Analysis feature requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> . |

Prerequisites for Network Analysis

Network Analysis has the following prerequisite:

- Network Analysis only pertains to the devices that DCNM-LAN has discovered.

Guidelines and Limitations for Network Analysis

The Network Analysis feature has the following configuration guidelines and limitations:

- Specify the IP addresses for devices to monitor the network path between two end hosts or between a host and a server. This allows monitoring of the ingress port of the source connected switch to the egress port of the target switch connected to the end host or server.
- Specify the IP addresses for switches, VLAN, and optional interface information to monitor the path between them.
- Specify the threshold level for the round trip time to help evaluate the path latency results.

Using the Network Analysis Feature

This section includes the following topics:

- [Using Network Analysis, page 36-2](#)
- [Using the New Path Latency Session Wizard, page 36-4](#)
- [Viewing Session Statistics, page 36-7](#)

Using Network Analysis

You can use Network Analysis to specify the scope of the analysis and to view the information about the analysis.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane. Each row in the table is a path latency session. You are able to view the sessions that you have created as well as the sessions created by other users. See [Table 36-1](#).

Users with administrator privileges are allowed to modify other users' sessions.

Table 36-1 Information in Summary Pane

| Column | Description |
|--------------------------------|--|
| Session ID | Unique ID of the session created by the user. The ID is updated after the user deploys the session. |
| Session Name | Unique name entered by user for the path latency session. |
| Source Switch | IP address of the source switch from which path latency is monitored. |
| Destination Switch | IP address of the destination switch to which the path latency is monitored. |
| VLAN | VLAN ID through which the actual traffic flows (1 to 4094). |
| Class of Service (CoS) | Optional value used to filter the traffic monitoring based on class of service value (0 to 7). CoS values are shown in Table 36-2 . |
| Round Trip Time (microseconds) | Minimum, maximum, average and latest value of the round trip time (two way path: source <-> destination) of all the RTT latencies calculated up until current time. |
| Forward Delay (microseconds) | Minimum, maximum, average and latest value of the forward delay (forward path: source -> destination) of all the forward delay latencies calculated to the current time. |
| Reverse Delay (microseconds) | Minimum, maximum, average and latest value of the reverse delay (reverse path: destination -> source) of all the reverse delay latencies calculated to the current time. |
| Owner | Creator of the session. |
| Success Percentage | Success percentage of the packets traversed from source to destination during the specified time interval. |
| Scheduled At | Date and time when the monitoring was started. |
| Status | Column that specifies: <ul style="list-style-type: none"> • Session created • Monitoring started • Monitoring stopped |

Table 36-2 CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type |
|---------------|-------------------------|
| 0 | Background |
| 1 | Best Effort |
| 2 | Excellent Effort |
| 3 | Critical Applications |
| 4 | Video, < 100 ms latency |
| 5 | Voice, < 10 ms latency |

Table 36-2 CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type |
|---------------|------------------|
| 6 | Internet Control |
| 7 | Network Control |

Step 2 Above the Summary pane, click the **Configure New Rule** link to set a threshold rule for one of the following parameters.

- Round trip time
- Forward delay
- Reverse delay



Note Clicking **Configure New Rule** links you to Threshold Rules of the DCNM-LAN Server Administration feature.

Step 3 Above the Summary pane, click the **Set Global Threshold** link to set a global threshold rule for the following parameters:

- Round trip time
- Forward delay
- Reverse delay

The global threshold setting is applied to all the sessions in the Summary Table.

Step 4 Above the Summary pane, click the **VLAN-CoS** button to view the sessions grouped by VLAN-CoS.

Using the New Path Latency Session Wizard

You can use the New Path Latency Session wizard to create a new session.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane.

Step 2 In the Summary pane, right-click and choose **New Path Latency Session** in the context menu.

The New Path Latency Session wizard appears.

Step 3 In the Select Session Monitor Option of Interest screen, enter the following:

- Session Name
(Length: 1 to 256 characters)
- VLAN
(Value: 1 to 4094)
- Class of Service (CoS)

Table 36-3 CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type |
|---------------|-------------------------|
| 0 | Background |
| 1 | Best Effort |
| 2 | Excellent Effort |
| 3 | Critical Applications |
| 4 | Video, < 100 ms latency |
| 5 | Voice, < 10 ms latency |
| 6 | Internetwork Control |
| 7 | Network Control |

Step 4 In the Select Option section, choose one of the following options:

- Monitor latency between source VDC and destination VDC.
- Monitor latency between source and destination VDC including source switching delay.
- Monitor latency between source and destination VDC including destination switching delay.
- Monitor latency between source and destination VDC including both switching delays.

Under the Monitor latency between source VDC and destination VDC option, you can additionally choose to measure the latency between switches that have Fabric Path mode connectivity. The latency measurements are measured between the source and destination switches but do not include the switching delay of both the end switches.

**Note**

For the switches that are in a classical ethernet cloud, the wizard allows you to choose their VDC MAC addresses/IP addresses/hostnames in the following wizard screen.

Click **Next** to continue.

Step 5 In the Select Source and Destination Switch screen, do the following:

- Choose the source switch by clicking on the ellipses next to the Select Source Switch field. Highlight the device in the screen that appears and click **OK** to enter your selection.
- Choose the destination switch by clicking on the ellipses next to the Select Destination Switch field. Highlight the device in the screen that appears and click **OK** to enter your selection.

Depending on the earlier selection that you made in the Select Option section of the wizard, [Table 36-4](#) list the required and optional information that you must enter in the Select Source and Destination Switch screen.

Table 36-4 Required and Optional Information

| Option | Required | Optional |
|--|---|---|
| Monitor latency between source VDC and destination VDC | <ul style="list-style-type: none"> Source and destination | <ul style="list-style-type: none"> Egress/outbound interface through which the packet flows out from the source. |
| Monitor latency between source and destination VDC including source switching delay | <ul style="list-style-type: none"> Source and destination Inject/ingress interface through which the packet needs to be injected from the source switch. Also requires the source static MAC address associated with the interface. | <ul style="list-style-type: none"> N/A |
| Monitor latency between source and destination VDC including destination switching delay | <ul style="list-style-type: none"> Source and destination Egress/outbound interface through which the packet terminates at the destination switch. Also requires the destination static MAC address associated with the interface. | <ul style="list-style-type: none"> Egress/outbound interface through which the packet flows out from the source. |
| Monitor latency between source and destination VDC including both switching delays | <ul style="list-style-type: none"> Source and destination Inject/ingress interface through which the packet needs to be injected from the source switch. Also requires source static MAC address associated with the interface. Egress/outbound interface through which the packet terminates at the destination switch. Also requires the destination static MAC address associated with the interface. | <ul style="list-style-type: none"> N/A |

**Note**

You can enter any arbitrary unique static MAC address that points to the selected interface. To configure a new static MAC address, use one of the following recommended addresses to avoid any conflict with globally administered MAC addresses (associated with any other host/devices):

- X2XX.XXXX.XXXX
- X6XX.XXXX.XXXX
- XAXX.XXXX.XXXX
- XEXX.XXXX.XXXX

where X is a hexadecimal value.

Click **Next** to continue.

Step 6 In the dialog box that appears, click **OK** to start input verification.

The Input Verification screen appears and the results are displayed.

Input verification verifies the following:

- Path latency measurement between specified devices.
- Packet traversal between the specified devices.

If the verification fails, you must specify the information that you entered earlier in the wizard.

[Table 36-5](#) lists the additional settings that are available in the Input Verification window:

Table 36-5 *Input Verification Settings*

| Setting | Description | Value |
|------------------------|---|---|
| Monitor Interval | Interval of time between data collection points. | 0.5 - 5 minutes (Default: 5 minutes) |
| End Time | Time of session termination | N/A |
| Calculate Jitter | Variance of inter packet RTT delay | Default: unchecked |
| No. of Packets to send | Packet count to send for the session to measure latency. To calculate jitter (inter packet delay variance), more than 1 packet has to be sent. | 1 -5 packets (Default: 1 packet) |

Click **Finish** after a successful verification and to enter the settings.

Viewing Session Statistics

You can view session statistics from the Summary pane.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane.

Step 2 Right-click a session and choose **Go To Statistics** in the context menu.

The statistics for the session appear as a chart and a table of detailed information in the Details pane.

Step 3 In the Details pane, click the Path Latency tab to display RTT information about each path.

Step 4 In the Details pane, right-click to display a context menu of additional statistical displays:

- Path specific switching delay—Switching delay of all the switches traversed in each path.
- Path specific link delay—Link delay at each hop traversed in each path.
- Switching delay of each switch across different paths traversed in the session.
- Link delay of each link across different paths traversed in the session.

Step 5 In the Details pane, click the **Session Report** tab to display overall statistical information about the session.

The information can be exported as an Excel .xls file by clicking the export button near the top of the table.

Related Documents

For additional information related to the topology map, see the following sections:

| Related Topic | Document Title |
|------------------|--|
| Device discovery | Chapter 29, “Administering Device Discovery” |

Feature History for Network Analysis

[Table 36-6](#) lists the release history for this feature.

Table 36-6 *Feature History for Topology*

| Feature Name | Releases | Feature Information |
|--------------------------|----------|---|
| Network Analysis support | 5.2(0) | Support for Network Analysis was added. |