



# Monitor

---

This section contains context-sensitive Online Help content for the **Web Client > Monitor** tab.

- [Monitoring Switch, page 1](#)
- [Monitoring SAN, page 5](#)
- [Monitoring LAN, page 14](#)
- [Monitoring Report, page 18](#)
- [Monitoring Configuration, page 21](#)
- [Exploring Endpoint Locator Details, page 24](#)

## Monitoring Switch

The Switch menu includes the following submenus:

### Viewing Switch CPU Information

#### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > CPU**.  
You see the CPU pane. This pane displays the CPU information for the switches in that scope.
  - Step 2** You can use the drop-down to filter the view by 24 Hours, Week, Month and Year.
  - Step 3** In the **Switch** column, click the switch name to view the [Switch Dashboard](#).
  - Step 4** Click the chart icon in the **Switch** column to view the CPU utilization. You can also change the chart timeline to 24 hours, Week, Month and Year. You can choose the chart type and chart options to show as well.
-

## Viewing Switch Memory Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Memory**.  
You see the memory panel. This panel displays the memory information for the switches in that scope
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** Click the chart icon in the **Switch** column to see a graph of the memory usage of the switch.
- Step 4** In the **Switch** column, click the switch name to view the [Switch Dashboard](#).
- Step 5** You can use the drop-down to view the chart in different time lines. Use the chart icons to view the memory utilization chart in varied views.
- 

## Viewing Switch Traffic and Errors Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Traffic**.  
You see the **Switch Traffic** panel. This panel displays the traffic on that device for the past 24 hours.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the switch name to view the Switch Dashboard section..
- 

## Viewing Switch Temperature

Cisco DCNM includes the module temperature sensor monitoring feature, using which you can view the sensor temperature of a switch. You can choose an interval by which to filter the sensor list. The default interval is **Last Day**. Note that only sensors that have historical temperature data will be shown in the list. You can choose between Last 10 Minutes, Last Hour, Last Day, Last Week, and Last Month.



### Note

It is not necessary to configure the LAN or SAN credentials under the **Configure > Credentials Management > LAN Credentials** screen to fetch the temperature monitoring data from the switches.

---

### Procedure

---

- Step 1** From the menu, choose **Monitor > Switch > Temperature**. The **Switch Temperature** window is displayed with the following columns.

- **Scope**—The sensor belongs to a switch, which is part of a fabric. The fabric it belongs to is shown as its scope. When the scope selector at the top of Cisco DCNM is used, the sensor list is also filtered by that scope.
- **Switch Name**—Name of the switch the sensor belongs to.
- **IP Address**—IP Address of the switch.
- **Temperature Module**—The name of the sensor module.
- **Avg/Range**—The first number is the average temperature over the interval specified at the top of the table. The second set of numbers is the range of the temperature over that interval.
- **Peak**—The maximum temperature over the interval

**Step 2** From this list, each row has a chart icon, which you can click. This brings up a chart in the lower portion of the page, which shows historical data for the sensor. The interval for this chart can be changed as well, between 24 hours, 1 week, and 1 month.

---

## Enabling Temperature Monitoring

You can enable the temperature monitoring feature for LAN switches from the LAN Collections screen, and for the SAN switches by setting a few properties under Administration > DCNM Server > Server Properties screens.

### Enabling Temperature Monitoring for LAN Switches

- 1 From the menu bar, choose **Administration > Performance Setup > LAN Collections**.
- 2 Select the **Temperature Sensor** check box.
- 3 Select the type(s) of LAN switches for which you want to collect performance data.
- 4 Click **Apply** to save the configuration

### Enabling Temperature Monitoring for SAN Switches

- 1 From the menu bar, select **Administration > DCNM Server > Server Properties**.
- 2 Navigate to the # **PERFORMANCE MANAGER > COLLECTIONS** area.
- 3 Set the environment fields **pm.collectSanTemperature** & **pm.sanSensorDiscovery** to **TRUE**.
- 4 Click **Apply Changes** to save the configuration.
- 5 Restart Cisco DCNM.

## Viewing Other Statistics

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > User Defined**.  
You see the **Other** window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.  
There are variations to this procedure. In addition to these basic steps, you can also do the following:
- Select the time range, and click **Filter** to filter the display.
  - Click the chart icon in the **Switch** column to see a graph of the performance for this user defined object.  
You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.
  - Use the chart icons to view the traffic chart in varied views.
- 

## Viewing Switch Custom Port Groups Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Custom Port Groups**.  
The Custom Port Groups page shows statistics and performance details for custom port groups.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the switch name to view the [Switch Dashboard](#).
- 

## Viewing Accounting Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Accounting**.  
The fabric name or the group name along with the accounting information is displayed.

- Step 2** Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **User Name**, **Time** and **Description**. Or select **Quick Filter** to search under each column.
- Step 3** You can also select a row and click on the delete icon to delete accounting information from the list.
- Step 4** You can use the **Print** icon to print the accounting details and use the **Export** icon to export the data to a Microsoft Excel spreadsheet.
- 

## Viewing Events Information

You can view the events and syslog from Cisco DCNM Web Client.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Events**.  
The fabrics along with the switch name and the events details are displayed.  
The **Count** column displays the number of times that the same event has occurred during the time period that is shown in the **Last Seen** and **First Seen** columns.  
If you click a switch name displayed in the **Switch** column, Cisco DCNM Web Client displays the switch dashboard.
- Step 2** Select one events in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule. For detailed information about adding event suppressor rules, please refer to [Add Event Suppression Rules](#).
- Step 3** Select one or more events from table and click the **Acknowledge** icon to acknowledge the event information for the fabric.
- Once you have acknowledged the event for a fabric, the acknowledge icon is displayed in the **Ack** column next to the fabric.
- Step 4** You can cancel an acknowledgment for a fabric by selecting the fabric and clicking the **Unacknowledge** icon.
- Step 5** Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **User Name**, **Time** and **Description**. Or select **Quick Filter** to search under each column.
- Step 6** Select a fabric and use the **Delete** icon to delete the fabric and it's event information from the list.
- Step 7** You can use the **Print** icon to print the event details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.
- 

## Monitoring SAN

The SAN menu includes the following submenus:

## Monitoring ISL Traffic and Errors

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > ISLs**.  
You see the **ISL Traffic and Errors** pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

**Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

**Note** **NaN** (Not a Number) in the data grid means that the data is not available.

**Note** It will be empty for non-FCIP ports under the **FCIP Compression Ratio** column.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Refresh** icon from in the upper right corner. The real-time data is updated in every 10 seconds.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

## Viewing Performance Information for NPV Links

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > NPV Links**.  
You see the **NPV Links** window. This window displays the NPV links for the selected scope.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.

**Step 3** Click the chart icon in the **Name** column to see a list of the traffic for the past 24 hours. There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for NPV links:

- You can change the time range for this information by selecting from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- To view real-time information, choose **Real Time** from the drop-down list in the **Chart** menu.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

## Viewing Inventory Information for VSANs

### Procedure

From the menu bar, choose **Monitor > SAN > VSANs**.

You see the **VSAN** window displaying the VSAN details along with the status and **Activated Zoneset** details.

## Monitoring Performance Information for Ethernet Ports

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > Ports**.  
You see the **Ethernet Ports** window.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**. There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the name of an Ethernet port from the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

## Viewing Inventory Information for Host Ports on FC End Devices

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > FC Ports**.  
You see the **Inventory > End Ports** window displaying details of the FC End Devices on the host ports.
- Step 2** Use the drop-down to view All or Warning information for the FC End devices on host ports.
- Step 3** Click the **Show Filter** icon to enable filtering by **Enclosure**, **Device Name** or **VSAN**.
- 

## Viewing Performance Information on All Ports

You can view the performance of devices connected to host ports, storage ports and all ports.

### Procedure

- 
- Step 1** From the menu bar, choose **Performance > End Devices**.  
You see the **End Devices Traffic and Errors** window.
- Step 2** You can choose to display **All** ports, **Host** ports or **Storage** ports from the drop-down list on the upper right corner.
- Step 3** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 4** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 5** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views. To view real-time information, click the refresh icon from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to **Append**, **Predict** and **Interpolate Data**.



**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

---

## Viewing Performance Information for FC Flows

You can view the performance of the **FC Flow** traffic through the Cisco DCNM Web Client.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > FC Flows**.  
You see the **FC Flows** window.
- Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views. To view real-time information, click on the refresh icon from the drop-down list in the upper right corner.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

---

## Viewing Performance Information on Enclosures

You can view the performance of devices connected to the host enclosure.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > Enclosures**.  
You see the **Enclosures Traffic and Errors** window.
- Step 2** You can select to view **Host Enclosures** or **Storage Enclosures** from the drop-down list on the upper right corner.
- Step 3** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 4** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 5** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

---

## Viewing Performance Information on Port Groups

You can view the performance of devices connected to the port groups.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > Port Groups**.  
You see the **Port Group Traffic and Errors** window.
- Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 3** Click the name port group to see the members of that port group.  
There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the port groups:
- To change the time range for this graph, select it from the drop-down list in the upper right corner.
  - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
  - To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

---

## SAN Host Redundancy

The **SAN Host Path Redundancy** check enables you to view the non-redundant host storage paths. It helps you identify the host enclosure errors along with the resolution to fix the errors.



### Note

All fabrics that are discovered must be licensed or this feature will be disabled in the Cisco DCNM Web Client. When the feature is disabled, a notification is displayed stating unlicensed fabrics are discovered.

---

From the menu bar, choose **Monitor > SAN > Host Path Redundancy**.

You can see two parts in this window:

- [Tests to Run](#)
- [Results](#)

## Tests to Run

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > Host Path Redundancy**.
  - Step 2** Under the upper **Tests to Run** area, use the check boxes to select the host redundancy optional checks.
  - Step 3** Check the **Automatically Run Check Every 24 hours** checkbox to enable periodic running of the checker. The checker will run every 24 hours starting 10 minutes after the server starts.
  - Step 4** Check **Limit by VSANs** check box, and select **Inclusion** or **Exclusion**. Enter VSAN or VSAN range in the text field to include or skip the host enclosures that belong to VSAN(s) from the redundancy check.
  - Step 5** Check other optional checks to do the relevant check.
  - Step 6** Click **Clear Results** to clear all the errors displayed.
  - Step 7** Click **Run Tests Now** to run the check at anytime.
  - Step 8** The results are displayed in the below [Results](#) area.
- 

## Results

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > Host Path Redundancy** tab.
  - Step 2** The bottom **Results** area has four tabs that are **Host Path Errors**, **Ignored Hosts**, **Ignored Storage** and **Ignored Host Storage Pairs**.
  - Step 3** Click **Host Path Errors** tab to display the host path redundancy errors table. On the top of the table, the colored **Good**, **Skipped** and **Errored** host enclosure counts, along with the last update time are displayed.
    - a) The **Host Enclosure** column displays the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error. The **Storage Enclosure/Storage Port** column displays the connected storage that is involved the errors. In the **Fix?** column, hover the mouse cursor on the ? icon to view a solution to fix the error.
    - b) Select a row and click **Ignore Hosts** to add the selected row(s) host enclosure to an exclusion list. The errors from that host will no longer be reported and the current errors will be purged from the database.
    - c) Select a row and click **Ignore Storage** to add the selected row(s) storage enclosure to an exclusion list.
    - d) Select a row and click **Ignore Host Storage Pair** to add the selected row(s) host-storage pair enclosure to an exclusion list.
    - e) In the drop-down list next to **Show** on the upper right corner of the table, select **Quick Filter**. Enter the keywords in the column headers of the table to filter the items. Select **All** to display all the items.
    - f) Click the circulation icon on the upper right corner of the table to refresh the table.
    - g) Click the **Print** icon on the upper right corner of the table to print the errors as tables.

h) Click the **Export** icon on the upper right corner of the table to export the table to a Microsoft excel spreadsheet.

**Step 4** Click the **Ignored Hosts** tab to display the list of host enclosures that have been skipped or ignored by the redundancy check along with the reason the host enclosure check was skipped. The following reasons may be displayed:

- Skipped: Enclosure has only one HBA.
- Host was ignored by the user.
- Host ports managed by more than one federated servers. Check can't be run.
- Skipped: No path to storage found.

Select a host enclosure and click the **Delete** button to remove the host from the ignored list and begin receiving errors about a host you had chosen to ignore. However, you can delete entries with message Host was ignored by user.

**Step 5** Click the **Ignored Storage** tab to display the list of storage enclosures that have been selected to be ignored during redundancy check. Select a storage enclosure and click the **Delete** button to remove the storage from the ignored list and begin receiving errors about a storage you had chosen to ignore.

**Step 6** Click the **Ignored Host Storage Pair** tab to display the list of host-storage pairs that have been selected to be ignored during redundancy check. Select a row and click **Delete** to delete the storage pair from the ignored list.

## Slow Drain Analysis

The **Slow Drain Analysis** enables you to view slow drain statistics at the switch level and the port level. You can monitor the slow drain issue within any time frame. You can display the data in a chart format and export the data for analysis also.

The slow drain statistics are stored in the cache memory. Therefore, the statistics will be lost when the server is restarted or a new diagnostic request is placed.



### Note

The jobs run in the background, even after you log off.

To configure and view the slow drain statistics,

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > Slow Drain Analysis**.

**Step 2** In the **Scope** field, select the fabric from the drop-down list.

**Step 3** In the **Duration** drop-down list, select **Once** or **Daily** for scheduled daily job. **Once** will include intervals, such as 10min, 30min, 1hour, and other hours and run the job immediately; while **Daily** will allow user to pick a start up time, and run the job for selected interval. Use the radio button to select the desired Interval to collect data.

Only daily slow drain job will sent out report which can be viewed from **Monitor > Report > View**.

- Step 4** Click the **Play** icon to begin polling.  
The server begins to collect the slow drain statistics based on the scope defined by the user. The **Time Remaining** is displayed in the right-side of the page.
- Step 5** Click the **Stop** icon to stop polling.  
The server maintains the counters in the cache, until a new diagnostic request is placed. You can stop the polling before the time is up.
- Step 6** Click on the arrow next to **Current jobs** to display the slow drain details for the jobs running on the fabric. The **Fabric Name**, the **Status** of polling, **Start**, **End**, and **Duration** icon for each fabric is displayed.
- Step 7** Select the fabric and click **Result**, **Delete** and **Stop** to view, delete and stop the job.
- Step 8** Click on the **Detail** icon to view the saved information.
- Step 9** Click on Interface chart icon to display the slow drain value for the switch port in chart format.
- Step 10** Click on the **Filter** icon to display the details based on the defined value for each column.
- Step 11** Select the **Data Rows Only** checkbox to filter and display the non-zero entries in the statistics.
- Step 12** Click on the **Print** icon to Prints the slow drain details.
- Step 13** Click on the **Export** icon to export the slow drain statistics to a Microsoft Excel spreadsheet.
- 

## Viewing Inventory Information for Regular Zones

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > Regular Zones**.  
You see the **Regular Zones** window displaying the inventory details of the fabrics in the regular zone.
- Step 2** Click the **Settings** icon to choose the displaying columns.
- 

## Viewing Inventory Information for IVR Zones

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Active Zones > IVR Zones**.  
You see the IVR Zones window displaying the inventory details of the fabrics in the IVR zone.
- Step 2** Click the **Settings** icon to choose the display column.
-

# Monitoring LAN

The LAN menu includes the following submenus:

## Monitoring Performance Information for Ethernet

### Procedure

**Step 1** From the menu bar, choose **Monitor > LAN > Ethernet**.

You see the **Ethernet** window.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the name of an Ethernet port from the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

## Monitoring ISL Traffic and Errors

### Procedure

**Step 1** From the menu bar, choose **Monitor > LAN > Link**.

You see the **ISL Traffic and Errors** pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

**Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

**Note** NaN (Not a Number) in the data grid means that the data is not available.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Real Time** from the drop-down list in the **Chart** menu.
- To export the data into a spreadsheet, choose **Export** from the drop-down list in the **Chart** menu and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

## Monitoring a vPC

The virtual port channel (vPC) feature enables you to view the links that are physically connected to different devices as a single port channel. A vPC is an extended form of a port channel which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. Traffic is distributed among two single device vPC end points. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.



**Note**

To view the vPC in **vPC Performance**, both primary and secondary device should be designated to the user. If either one kind of switch is not designated, vPC information will not displayed.

Cisco DCNM **Web Client** > **Monitor** > **vPC** will display only consistent vPCs displays both the consistent and inconsistent vPCs.

You can identify the inconsistent vPCs and resolve the inconsistencies in each vPC by using the Cisco DCNM **Web Client** > **Configure** > **Deploy** > **vPC Peer** and **Web Client** > **Configure** > **Deploy** > **vPC**.

[Table 1: vPC Performance, on page 16](#) displays the following vPC configuration details in the data grid view.

**Table 1: vPC Performance**

Column	Description
Search box	Enter any string to filter the entries in their respective column.
<b>vPC ID</b>	Displays vPC ID's configured device.
<b>Domain ID</b>	Displays the domain ID of the vPC peer switches.
<b>Multi Chassis vPC EndPoints</b>	Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain.
<b>Primary vPC Peer - Device Name</b>	Displays the vPC Primary device name.
<b>Primary vPC Peer - Primary vPC Interface</b>	Displays the primary vPC interface.
<b>Primary vPC Peer - Capacity</b>	Displays the capacity for the primary vPC peer.
<b>Primary vPC Peer - Avg. Rx/sec</b>	Displays the average receiving speed of primary vPC peer.
<b>Primary vPC Peer - Avg. Tx/sec</b>	Displays the average transmitting speed of primary vPC peer.
<b>Primary vPC Peer - Peak Util%</b>	Displays the peak utilization percentage of primary vPC peer.
<b>Secondary vPC Peer - Device Name</b>	Displays the vPC secondary device name.
<b>Secondary vPC Interface</b>	Displays the secondary vPC interface.
<b>Secondary vPC Peer - Capacity</b>	Displays the capacity for the secondary vPC peer.
<b>Secondary vPC Peer - Avg. Rx/sec</b>	Displays the average receiving speed of secondary vPC peer.
<b>Secondary vPC Peer - Avg. Tx/sec</b>	Displays the average transmitting speed of secondary vPC peer.
<b>Secondary vPC Peer - Peak Util%</b>	Displays the peak utilization percentage of secondary vPC peer.

You can use this feature as below:



## Monitoring vPC Performance

You can view the relationship among consistent virtual port channels (vPCs). You can view the statistics of all member interfaces and the aggregate of the statistics at the port channel level.

**Note**

This tab only displays consistent vPCs.

### Procedure

- Step 1** From the menu bar, choose **Monitor > LAN > vPC**.  
The **vPC Performance** statistics appears and the aggregated statistics of all vPCs are displayed in a tabular manner.
- Step 2** Click on the **vPC ID** and a window appears.  
You are able to view the vPC topology and **vPC Details**, **Peer-link Details** and **Peer-link Status** table.  
The **vPC Consistency**, **Peer-link Consistency**, and **vPC Type2 Consistency** for the vPC is displayed.
- Click the **vPC Details** tab, you can view the parameter details of vPC **Basic Setting** and **Layer 2 Settings** for both Primary and Secondary vPC devices.
  - Click the **Peer-link Details** tab, you can view the parameter details of peer-link **vPC Global Setting** and **STP Global Settings** for both Primary and Secondary vPC devices.
  - Click the **Peer-link Status** tab, the **vPC Consistency** and **Peer-Link Consistency** status is displayed, as well as the parameter details of **Role Status** and **vPC Peer keep-alive Status** for both Primary and Secondary vPC devices.
- Step 3** Click on the peer-link icon in front of the **Device Name** in the **Primary vPC peer** or **Secondary vPC peer** column to view its member interface.  
A pop-up window displays the member interfaces of the selected device.
- Step 4** Click the **Show Chart** icon of the corresponding interface to view its historical statistics.  
The traffic distribution statistics appear at the bottom of the vPC window. By default, the Cisco DCNM Web Client displays the historical statistics for 24 hours.
- There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for flows:
- To change the time range for this graph, select it from the drop-down list in the upper right corner.
  - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
  - To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#) section to turn on performance data collection.

---

# Monitoring Report

The Report menu includes the following submenus:

## Viewing Reports

You can view the saved reports based on the following selection options:

- **By Template**
- **By User**
- From the menu bar, select **Monitor > Report > View**.

You see the **View Reports** window displaying the **View Reports** by tree on the left pane.

### Procedure

---

- Step 1** In the left pane, expand **By Template** or **By User** folder.
  - Step 2** Select the report you wish to view. You can view the report in the main screen or you can select the report in the **Report** column to view the HTML version of the report in a new browser.
  - Step 3** To delete a specific report, select the check box and click the **Delete** icon.
  - Step 4** To delete all reports, check the check box in the header, and click the **Delete** icon.
- Note** If you have multiple fabrics, you can select the DCNM-SAN group in the Scope to view Host to Storage connectivity of multiple fabrics in a single report. The report is divided into two sections:
- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
  - A detailed information for the device of the module. The table contains details about the tests failed.
- 

## Generating a Report

You can generate reports based on a selected template or you can schedule the report to run at a specified time.

### Procedure

---

- Step 1** From the menu bar, select **Monitor > Report > Generate**. You see the **Generate Report** window.

- Step 2** In the configuration window, use the drop-down to define the scope for report generation. In the **Scope** drop-down, you can select a scope group with dual fabrics, the traffic data generated by hosts and storage end devices are displayed side-by-side which enables you to view and compare traffic data generated on dual fabrics. To view this report, in the **Other Predefined** folder, select **Traffic by VSAN** (Dual Fabrics). Click Options to select the **Device Type** and **Fabrics**. Click **Save** to save the configuration.
- Step 3** In the pane on the left hand, expand the folders and select the report.
- Step 4** (Optional) In the pane on the right hand, you can edit the **Report Name**.
- Step 5** (Optional) Check the **Export to Csv/Excel** check box to export the report in to a Microsoft Excel spreadsheet.
- Step 6** In the **Repeat** radio buttons, if you select:
- **Never** - The report is generated only during the current session.
  - **Once** - The report is generated on a specified date and time apart from the current session.
  - **Daily** - The report is generated everyday based on the Start and End date at a specified time.
  - **Weekly** - The report is generated once a week based on the Start and End date at a specified time.
  - **Monthly** - The report is generated once every month based on the Start and End date at a specified time.

When you generate a report for Network Configuration Audit, the daily job generates a report for the selected devices for last 1 day. Similarly, the weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.

- Step 7** Click the **Create** button to generate a report based on the specifications. You see the report results in a new browser window.

Alternatively, you can view the report by choosing **Monitor > Report > View** and selecting the report name from the report template that you used in the navigation pane.

**Note** The **Start Date** must be at least five minutes earlier than the **End Date**

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
- A detailed information for the device of the module. The table contains details about the tests failed.

## Creating SAN User Defined Reports

You can create custom reports from all or any subset of information obtained by Cisco DCNM-SAN. You create a report template by selecting events, performance, and inventory statistics you want in your report and set the desired SAN, fabrics or VSAN to limit the scope of the template. You can generate and schedule a report of your fabric based on this template immediately or at a later time. DCNM Web Client saves each report based on the report template used and the time you generate the report.

Since the Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete, and modify functionalities

on a single page. You can choose multiple fabrics and VSANs using the new navigation system, which allows you to add new items and categories in the future.

The new design model has three panels:

- **Template** panel - The **Template** panel allows you to add new templates, modify existing templates and delete existing templates.
- **Configuration** panel - The **Configuration** panel allows you to configure a new template when it is added, and modify an existing template. The options in the configuration panel are disabled until you either add a new template or select an existing template. The upper portion of the configuration panel contains many categories that you can choose and configure.
- **User Selection** panel - The **User Selection** panel displays your configuration options in real-time. While the configuration panel can display information pertaining to one category at a time, the **User Selection** panel displays all of your selections or configurations.

Follow the steps to create custom reports

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Report > User Defined**.  
You see the **Create User Defined** window.
- Step 2** In the **Template** panel, under the **Name** column, select **CLICK TO ADD NEW CUSTOM** to edit the **Name** of the new report.  
In the **Configuration** panel:
- Step 3** Click **Scope** to define scope of the report. The default scope will have Data Center, SAN, LAN, and Fabric configurations.
- Step 4** Click **Inventory** and use the checkbox to select the inventory information required in the report. You can also use the drop-down to filter by selecting the Top performance and the timeline required in the report.
- Step 5** Click **Performance** and use the checkbox to select the performance information required in the report.
- Step 6** Click **Health** and use the checkbox to select the health information required in the report.
- Step 7** Click **Save** to save this report template.  
A confirmation message is displayed confirming that the report is saved.
- 

## Deleting a Report Template

### Procedure

---

- Step 1** In the **Template** panel, select the report template that you want to delete.
- Step 2** Click the **Delete** icon to delete the report.
- Step 3** In the confirmation pop-up, click **Yes** to delete the template.
-

## Modifying a Custom Report Template

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > Report > User Defined**.  
You see the **Template**, **Configuration** and **User Selection** panels.
- Step 2** Select a report from the **Template** panel.  
You see the current information about this report in the **User Selection** panel.
- Step 3** Modify the information in the **Configuration** panel.
- Step 4** Click **Save** to save the report template.  
A confirmation message is displayed confirming that the report is saved.
- Note** You cannot change the scope for an existing report. You must generate a new report for a new scope.
- 

## Viewing Scheduled Jobs Based on a Report Template

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > Report > Jobs**.  
You see the **Report Jobs** window displaying details of the reports scheduled for generation along with its status.
- Step 2** Select the checkbox for a specific report and click the **Delete** Job icon to delete a report.
- 

## Monitoring Configuration

The Configuration menu includes the following submenus:

## Monitoring Archives

A user with network operator role can view configuration archives for a switch and their details in the **Archives** window.

The following tables describe the icons and fields that are displayed in this window.

**Table 2: Archive Operations**

Icon	Description
Compare	Allows you to compare two configuration files either from different devices or on the same device.
View/Edit	Allows you to view or edit a configuration file.

**Table 3: Archive Field and Description**

Field Name	Description
Device Name	Displays the device name Click on the arrow next to the device to view the configuration files.
IP Address	Displays the IP address of the device.
Group	Displays the group of the device.
Configuration	Displays the configuration files archived for that device.
Archive Time	Displays the time at which the device configuration files were archived. The format is Day:Mon:DD:YYYY HH:MM:SS.
Size	Displays the size of the archived file.
Golden	Shows whether the current version is a Golden backup or not.

This section contains the following:

## Compare Configuration Files

This feature allows you to compare one version of a configuration file with another version of the same configuration file in the same device, or the configuration files of two different devices.  
Perform the following task to compare configuration files.

### Procedure

- 
- Step 1** In the Cisco DCNM web client home page, choose **Monitor > Configuration > Archives**.
- Step 2** In the **Archives** area, click the arrow adjacent the name of the device whose configuration files you want to view. The list of configuration files is displayed.
- Step 3** Check the check box next to configuration files and select two configuration files to compare. The first file you select is designated as source and the second configuration file is designated as the target file.
- Step 4** Click **Compare**.  
The **View Config Diff** page displays the difference between the two configuration files.  
The Source and Target configuration files' content are displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration or choose **Changed** to view the configuration differences between the configuration files.  
The differences in the configuration files are shown in a table, with legends.  
Red—Deleted configuration details  
Green—Newly added configuration  
Blue—Modified configuration details
- 

## View or Edit Configuration

You can view an archived configuration file, or you can edit and save this file on your local system. The changes made to the archived configuration file is applied only to the file saved in your local system. The archived configuration file on the DCNM host server remains unchanged.

Perform the following task to view or edit the configuration file for the devices.

### Procedure

- 
- Step 1** In the web client home page, choose **Monitor > Configuration > Archives**.
- Step 2** In the **Archives** area, click the arrow adjacent the name of the device whose configuration files you want to view. The list of configuration files are displayed.
- Step 3** Click the radio button adjacent the corresponding file you want to view or edit.
- Step 4** Click the **View/Edit** configuration icon.  
The **View/Edit** configuration window appears showing the configuration file content in the right column.
- Step 5** Edit the configuration file as required.
- Step 6** Click **Save** to apply the changes and download the configuration file on your local system, or click **Cancel** to discard changes.
-

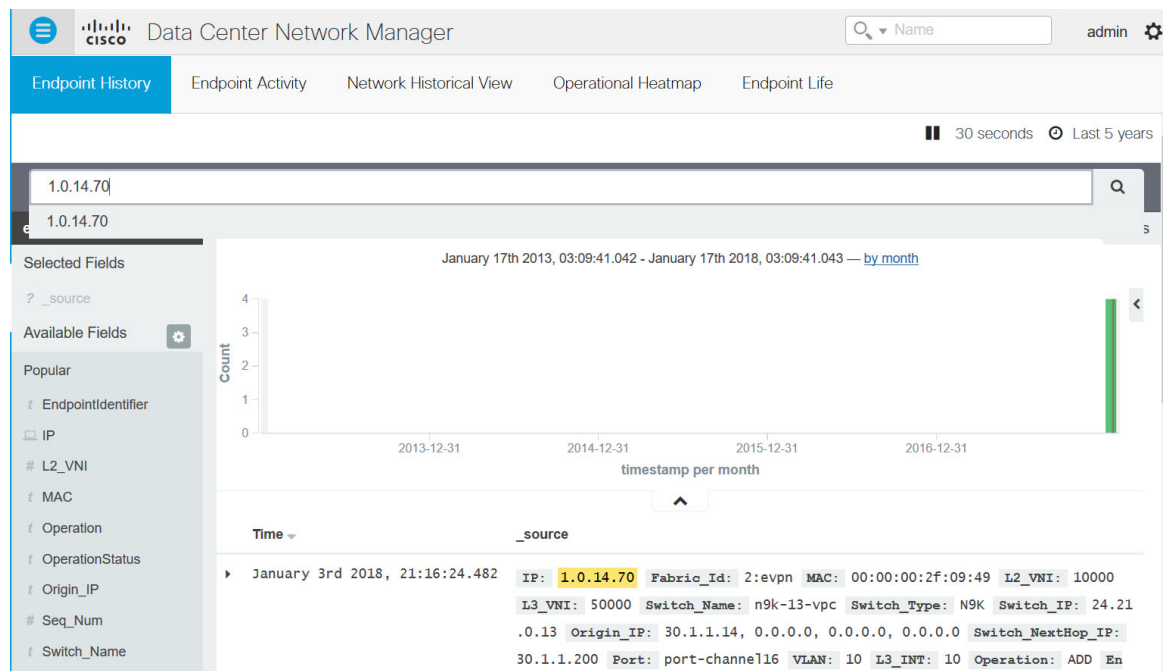
# Exploring Endpoint Locator Details

## Procedure

From the menu bar, choose **Monitor > Endpoint Locator > Explore**. The Endpoint Locator dashboard appears.

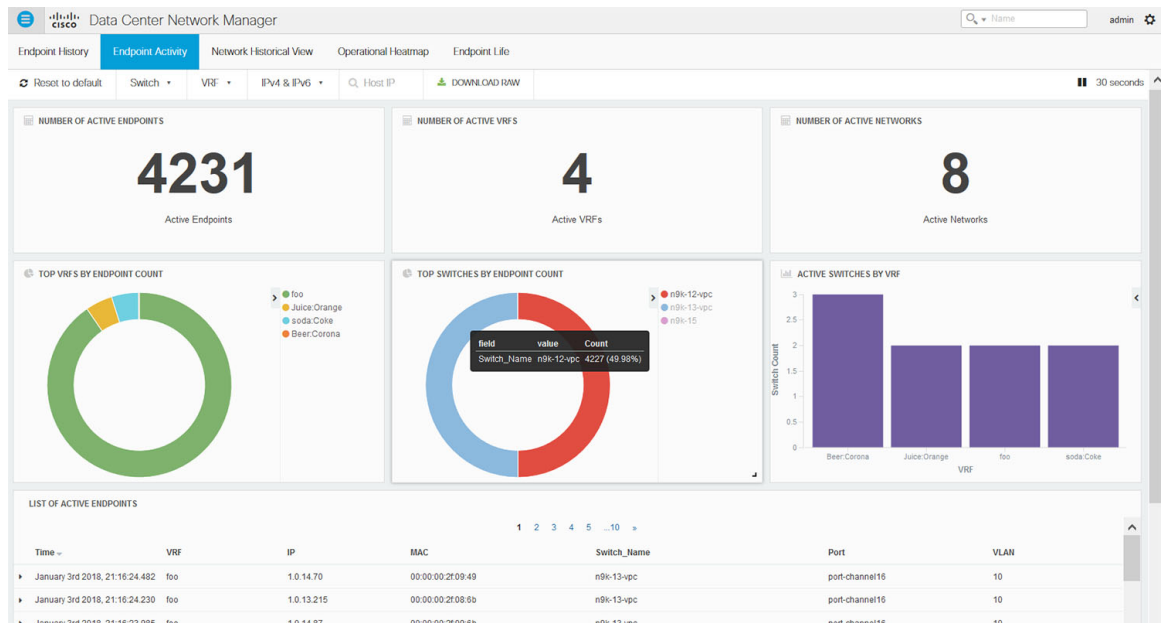
The Endpoint Locator Dashboard displays the following information:

- **Endpoint History**—Real time plot displaying Endpoint events for the period specified in the relative or absolute date range. A user can search for a specific metric value in the search bar. Search is supported on any of the fields as specified under the “Available Fields” column on the menu on the left. A sample screenshot of the endpoint history based on an IP address specified in the search field is depicted below.



- **Endpoint Activity**—This view displays the current state of the active endpoints in the fabric. The number of active endpoints including the number of active VRFs and active networks are listed in the top 3 tiles. The break-up of active endpoints is also available on a per VRF as well as a per switch basis. This is depicted by the first two tiles in the second row. If there is at least one active endpoint in a given VRF behind a switch, then that VRF is considered as active on that switch. Note that the VRF may be configured on a number of switches but it is only considered active and justifies burning resources on the switch, if there is at least one active endpoint in that VRF behind that switch. In that sense, the “ACTIVE SWITCHES BY VRF” tile can provide a good insight for the network administrator into removing extraneous VRF configurations from switches where it may not be needed. At the bottom of the dashboard, there is a data table that provides a list of endpoints with context information such as the VRF, IP, MAC, Switch, VLAN, Port etc. By default, the endpoint information is refreshed every 30 seconds. However, the refresh interval may be changed as desired.





Users can search for specific endpoints using various search filters such as VRF, switch, IPv4/IPv6 address etc. Multiple filters may be applied at the same time. The entire dashboard view across all tiles and the data table, are updated as soon as the search filters are applied. The search results can be downloaded in csv format by clicking on the “DOWNLOAD RAW” icon. A sample snippet of the downloaded csv file from a search result is shown below:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	A
1	Fabric_Id	IP	MAC	L2_VNI	L3_VNI	Switch_No	Switch_Type	Switch_IP	Origin_IPv4	Origin_IPv6	Origin_IPv4	Switch_NextHop_IP	Port	VLAN	L3_INT	Operation	EndpointT	Timestamp	Seq_Num	VRF	Br_Domain	Cluster	Valid	Operation	RouteDist	EndpointIdentifier			
2	evpn	1.0.0.231	00:00:00:2e:ee:8b	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.231:10000						
3	evpn	1.0.0.232	00:00:00:2e:ee:8d	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.232:10000						
4	evpn	1.0.1.196	00:00:00:2e:fd:45	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.196:10000						
5	evpn	1.0.1.198	00:00:00:2e:fd:49	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.198:10000						
6	evpn	1.0.0.226	00:00:00:2e:ee:81	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.226:10000						
7	evpn	1.0.0.230	00:00:00:2e:ee:89	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.230:10000						
8	evpn	1.0.1.199	00:00:00:2e:fd:4b	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.199:10000						
9	evpn	1.0.1.200	00:00:00:2e:fd:4d	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.200:10000						
10	evpn	1.0.1.203	00:00:00:2e:fd:53	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.203:10000						
11	evpn	1.0.1.204	00:00:00:2e:fd:55	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.1.204:10000						
12	evpn	1.0.2.188	00:00:00:2e:fd:35	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.2.188:10000						
13	evpn	1.0.2.194	00:00:00:2e:fd:41	10000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.2.194:10000						
14	evpn	1.0.0.217	00:00:00:2e:ee:6f	10000	50000	n9k-12-vp	N9K	24.21.0.12	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.217:10000						
15	evpn	1.0.0.223	00:00:00:2e:ee:7b	10000	50000	n9k-12-vp	N9K	24.21.0.12	30.1.1.14	0.0.0.0	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	AD0	Wed Jan 0	0	foo	10.30.1.1.200	1	30.1.1.211	(Pv4:1.0.0.223:10000						

It is possible to search based on any of the fields describing the information of each endpoint. For example, if the user wants to know the list of endpoints in a given network, that can be achieved as follows. Recall that each network is represented by a unique 24-bit identifier. This parameter is represented by the field L2\_VNI. Here are the steps:

- Go to the ‘List of endpoints’ data table and click on any row. This will expand the row as shown below:

**LIST OF ACTIVE ENDPOINTS**

1 2 3 4 5 ...10

Time	VRF	IP	MAC	Switch_Name	Port	VLAN
January 3rd 2018, 21:16:24.482	foo	1.0.14.70	00:00:00:2f:09:49	n9k-13-vpc	port-channel16	10

[Link to /api/cache/today/endpoint/evpn%3A1.0.14.70%3A30.1.1.219%3A32777](#)

Table JSON

Br\_Domain: 10

Cluster: 30.1.1.200:0

EndpointIdentifier: IPv4:1.0.14.70:10000

EndpointType: 2:evpn

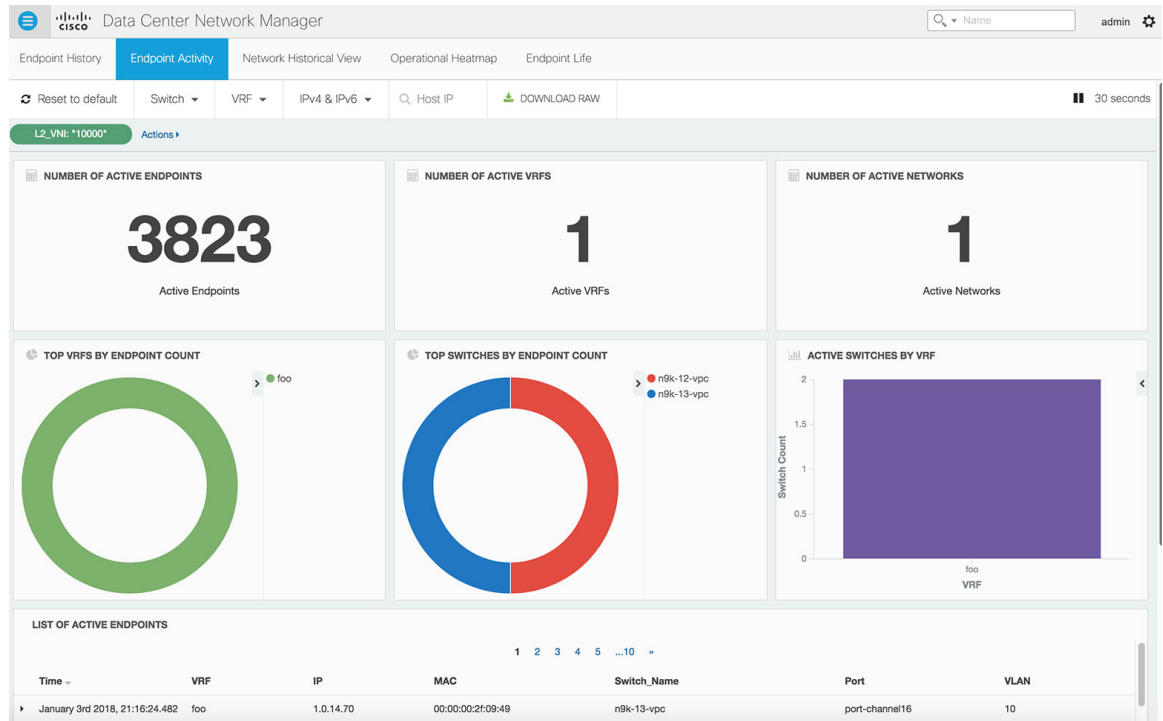
Fabric\_Id: 2:evpn

IP: 1.0.14.70

L2\_VNI: 10000

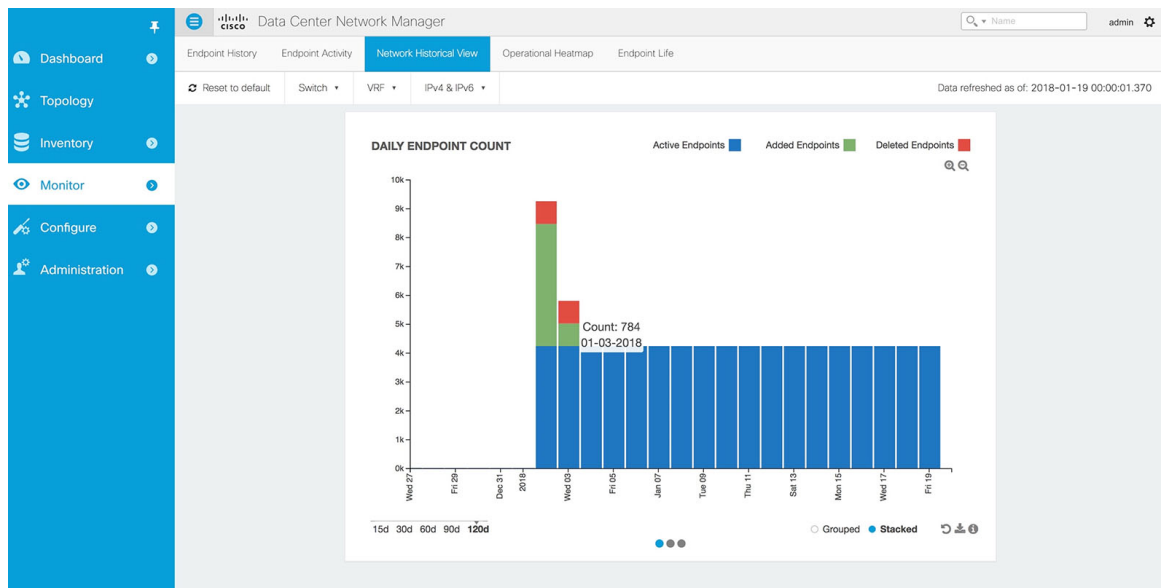
L3\_INT: Filter out value

- Click on the + icon next to the L2\_VNI field. This selects the highlighted value (10000 in this example) and filters the search results based on that. In other words, the information of all active endpoints in the network associated with L2\_VNI 10000 is displayed on the dashboard. If instead, all endpoints that are not in the network L2\_VNI are required, click the – icon next to the L2\_VNI value of 10000. In the same manner, one can choose any combination of fields to get the set of endpoints matching the corresponding selected filter criteria.

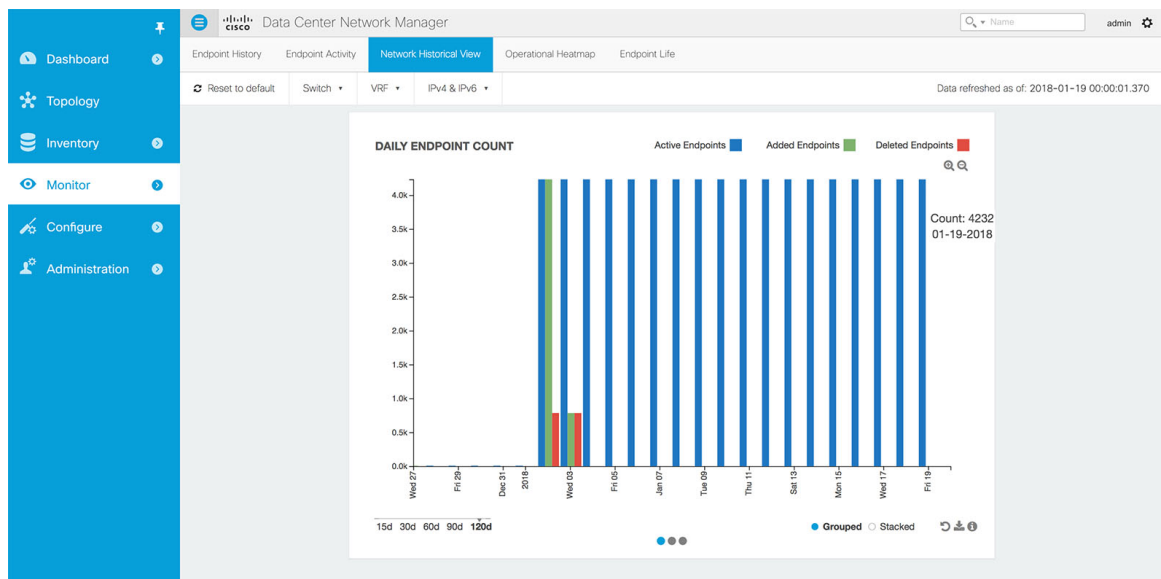


- Network Historical View**— The NHV view displays historical information of endpoints, networks, and VRFs (tenants) captured on a daily basis. These graphs are updated once a day at mid-night based on the DCNM server time. The time at which the data is refreshed/updated is listed at the top right. The idea is to provide a daily report of the Active, Added (New) and Deleted endpoints, networks, and VRFs respectively. If the same endpoint is added and removed on a day, then that contributes to an add count of 1 and a delete count of 1. Users can select one of the 3 dots at the bottom to toggle between the endpoints, networks, & VRF views. There are options to zoom in/out using zoom icons on top right. The users can also select the type of visualization with the choices being – Grouped or Stacked (shown below). Daily reports up to 180 days in the past can be displayed. Active endpoints/networks/VRFs are shown in blue color, deleted ones are shown in red color while the added ones are shown in green color. Every block in all screens is ‘clickable’ and the complete dataset associated with the selection, can be downloaded in csv format.

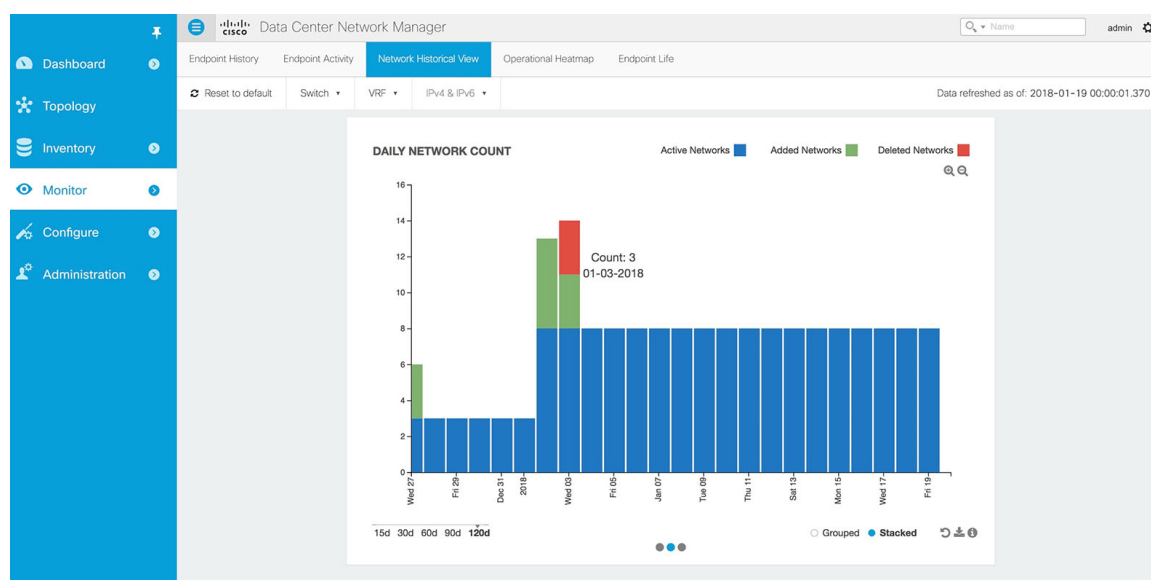
The historic endpoint count in ‘Stacked’ format is shown below:



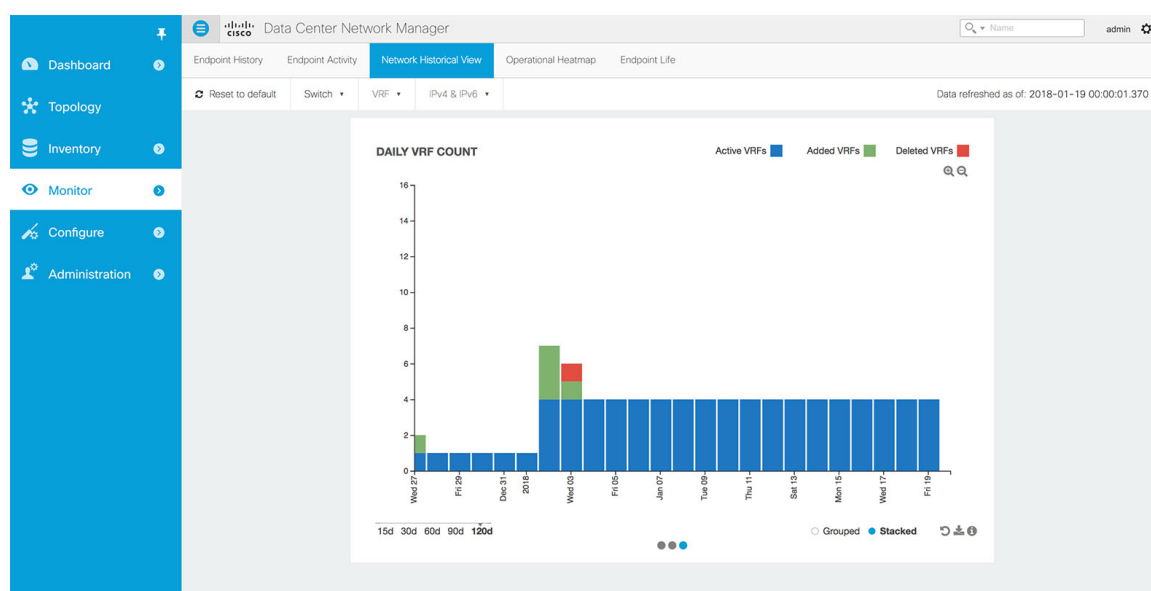
The same representation with the Grouped visualization selection is shown below:



Similarly, the figure below depicts the historic network count in stacked format:



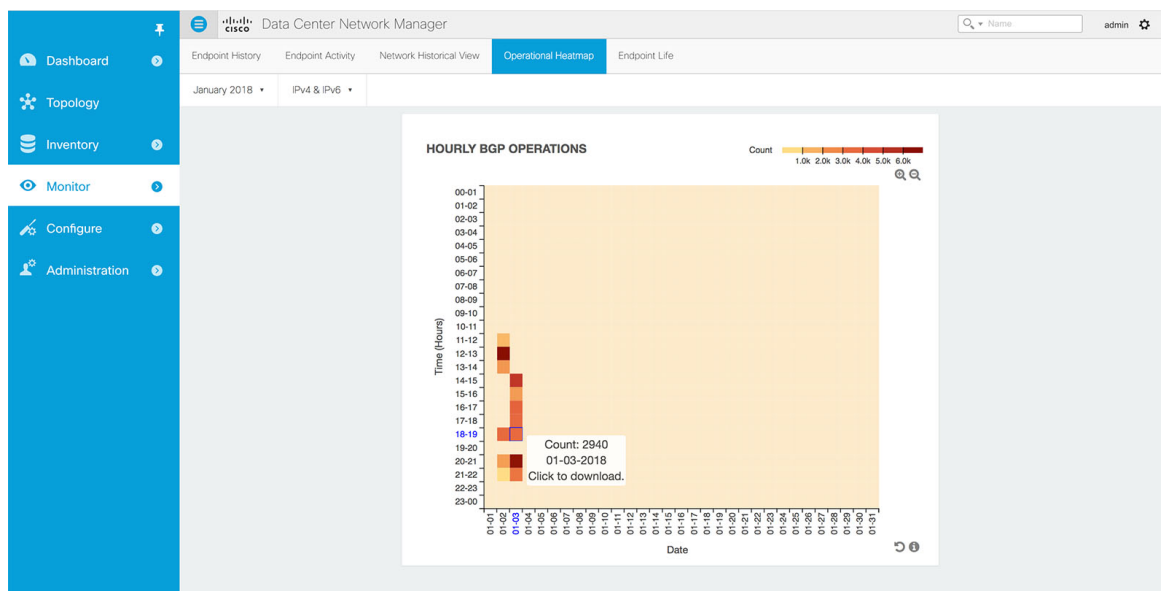
Along the same lines, the figure below depicts the historic vrf count:



The figure below provides a sample screenshot of the endpoints added on 01-03-2018 obtained by clicking on the blue bar for that day.

<

- **Operational Heatmap**—This view displays a heat-map of all endpoint operations occurring in the fabric.



The heat-map is color coded and the intensity of the color varies based on the number of endpoint operations captured on an hourly basis. The break down is available per hour across dates, and user can see the details of operations that occurred during a particular hour on a particular day by clicking on the appropriate square. The figure below depicts the endpoint operations reported by BGP on 01-02-2018 between 12 and 1pm.

< Back to Graph

Complete data set will be available in the downloaded csv. [Download](#)

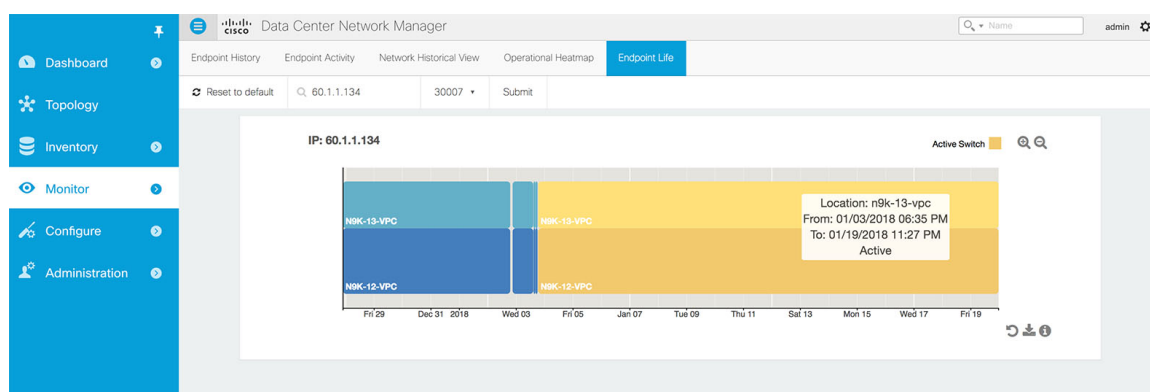
OPERATIONS: 01-02-2018 12:00PM - 1:00PM

Time	VRF	IP	MAC	Switch Name	Operation	VLAN
2018-01-02 12:00:20	foo	1.0.0.231	00:00:00:2e:ee:8b	n9k-13-vpc	ADD	10
2018-01-02 12:00:20	foo	1.0.0.232	00:00:00:2e:ee:8d	n9k-13-vpc	ADD	10
2018-01-02 12:00:24	foo	1.0.1.196	00:00:00:2e:f0:45	n9k-13-vpc	ADD	10
2018-01-02 12:00:25	foo	1.0.1.198	00:00:00:2e:f0:49	n9k-13-vpc	ADD	10
2018-01-02 12:00:08	foo	1.0.0.226	00:00:00:2e:ee:81	n9k-13-vpc	ADD	10
2018-01-02 12:00:17	foo	1.0.0.230	00:00:00:2e:ee:89	n9k-13-vpc	ADD	10
2018-01-02 12:00:26	foo	1.0.1.199	00:00:00:2e:f0:4b	n9k-13-vpc	ADD	10
2018-01-02 12:00:28	foo	1.0.1.200	00:00:00:2e:f0:4d	n9k-13-vpc	ADD	10
2018-01-02 12:00:32	foo	1.0.1.203	00:00:00:2e:f0:53	n9k-13-vpc	ADD	10
2018-01-02 12:00:33	foo	1.0.1.204	00:00:00:2e:f0:55	n9k-13-vpc	ADD	10

Again, as with the other views, the complete data set can be downloaded in csv format using the Download option. A sample screenshot of a downloaded csv file is shown below:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
	Fabric_ID	IP	MAC	L2_VNI	L3_VNI	Switch_Type	Switch_IP	Orig_IP_1	Orig_IP_2	Orig_IP_3	Switch_Nestlog_IP	Port	VLAN	L3_INT	Operation	EndpointT	Timestamp	Seq_Num	VRF	Br_Domain	Cluster	Valid	Operation	RouteID	EndpointID	Filter		
1	evpn	1.0.0.231	00:00:00:2e:ee:8b	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.231	100000			
2	evpn	1.0.0.232	00:00:00:2e:ee:8d	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.232	100000			
3	evpn	1.0.1.196	00:00:00:2e:f0:45	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.196	100000			
4	evpn	1.0.1.198	00:00:00:2e:f0:49	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.198	100000			
5	evpn	1.0.0.226	00:00:00:2e:ee:81	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.226	100000			
6	evpn	1.0.0.230	00:00:00:2e:ee:89	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.230	100000			
7	evpn	1.0.1.199	00:00:00:2e:f0:4b	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.199	100000			
8	evpn	1.0.1.200	00:00:00:2e:f0:4d	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.200	100000			
9	evpn	1.0.1.203	00:00:00:2e:f0:53	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.203	100000			
10	evpn	1.0.1.204	00:00:00:2e:f0:55	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.1.204	100000			
11	evpn	1.0.2.188	00:00:00:2e:f2:35	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.2.188	100000			
12	evpn	1.0.2.194	00:00:00:2e:f2:41	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.2.194	100000			
13	evpn	1.0.0.217	00:00:00:2e:ee:f	100000	50000	n9k-12-vp	N9K	24.21.0.12	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.217	100000			
14	evpn	1.0.0.223	00:00:00:2e:ee:7b	100000	50000	n9k-12-vp	N9K	24.21.0.12	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.223	100000			
15	evpn	1.0.0.236	00:00:00:2e:ee:87	100000	50000	n9k-13-vp	N9K	24.21.0.13	30.1.1.14	0.0.0.0	0.0.0.0	30.1.1.200	port-chan	10	10	ADD	Wed Jan 0	0	foo	10	30.1.1.200	1	30.1.1.211	IPv4-1.0.0.236	100000			

- Endpoint Life**—This view displays a time line of a particular endpoint in its entire existence within the fabric. Specifically, given an identity of an endpoint in terms of its IP address and VRF/Network-identifier, the output displays the list of switches that an endpoint was present under including the associated start and end dates. This view is essentially the network life view of an endpoint. If the endpoint is viewed as active by the network, it will have a band here. If an endpoint is dual-homed, then there will be 2 horizontal bands reporting the endpoint existence, one band for each switch (typically the VPC pair of switches). As endpoints move within the network, for example with VM move, this view provides a succinct and intuitive pictorial view of this activity.



The underlying data that drives this view can also be downloaded in csv format (shown below) by clicking on download icon on right bottom corner.

	A	B	C	D	E	F
1	Switch Name	VRF	EndPointIdentifier	Start Timestamp	End Timestamp	Active
2	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Dec 27 2017 21:41:33 GMT+0530 (India Standard Time)	Tue Jan 02 2018 18:56:32 GMT+0530 (India Standard Time)	
3	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Dec 27 2017 21:41:49 GMT+0530 (India Standard Time)	Tue Jan 02 2018 18:56:33 GMT+0530 (India Standard Time)	
4	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Tue Jan 02 2018 20:54:21 GMT+0530 (India Standard Time)	Wed Jan 03 2018 14:25:02 GMT+0530 (India Standard Time)	
5	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Tue Jan 02 2018 20:54:21 GMT+0530 (India Standard Time)	Wed Jan 03 2018 14:24:45 GMT+0530 (India Standard Time)	
6	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 14:35:40 GMT+0530 (India Standard Time)	Wed Jan 03 2018 16:09:09 GMT+0530 (India Standard Time)	
7	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 14:35:44 GMT+0530 (India Standard Time)	Wed Jan 03 2018 16:09:10 GMT+0530 (India Standard Time)	
8	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 16:15:18 GMT+0530 (India Standard Time)	Wed Jan 03 2018 18:02:49 GMT+0530 (India Standard Time)	
9	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 16:15:18 GMT+0530 (India Standard Time)	Wed Jan 03 2018 18:02:48 GMT+0530 (India Standard Time)	
10	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 18:35:09 GMT+0530 (India Standard Time)		TRUE
11	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Jan 03 2018 18:35:12 GMT+0530 (India Standard Time)		TRUE

