Monitor

This chapter contains the following topics:

Inventory

This chapter contains the following topics:

Viewing Inventory Information for Switches

To view the inventory information for switches from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Inventory > Switches**.

The **Switches** window with a list of all the switches for a selected Scope is displayed.

Step 2 You can also view the following information.

- **Group** column displays the switch group to which the switch belongs.
- In the **Device Name** column, select a switch to display the Switch Dashboard.
- **IP Address** column displays the IP address of the switch.
- **WWN/Chassis ID** displays the Worldwide Name (WWN) if available or chassis ID.
- **Health** displays the health situation of the switch.

Note To refresh and recalculate the latest health data for all the switches on Cisco DCNM, click the **Recalculate Health** button above the switches table.

- **Status** column displays the status of the switch.
- **# Ports** column displays the number of ports.
- **Model** column displays the model name of the switch.
- **Serial No.** column displays the serial number of the switch.
- **Release** column displays the switch version.
- **License** column displays the DCNM license that is installed on the switch.
- **Up Time** column displays the time period for which the switch is active.

Step 3 In the **Health** column, the switch health is calculated by the capacity manager based on the following formula in the server.properties file.

The function to implement is:

calculate(x, x1, y, y1, z).

@param x: Total number of modules.

@param x1: Total number of modules in warning.

@param y: Total number of switch ports.

@param y1: Total number of switch ports in warning.

@param z: Total number of events with severity of warning or above.

Step 4 The value in the **Health** column is calculated based on the following default equation.

((x-x1)*1.0/x) *0.4 + ((y-y1)*1.0/y)*0.3 + ((z*1.0/1000>=1) ? 0: ((1000-z)*1.0/1000)*0.3).

In the above formula, the switch health value is calculated based on the following:

- Percentage of Warning Modules (Contributes 40% of the total health).
- Percentage of Warning Ports (Contributes 30% of the total health).
- Percentage of events with severity of Warning or above (Contributes 30% of the total health. If there are more than 1000 warning events, the event health value is 0).

You may also have your own health calculation formula by implementing the common interface class: com.cisco.dcbu.sm.common.rif.HealthCalculatorRif. Add the `.jar` file to the DCNM server and modify the health.calculator property to point to the class name you have created.

The default Java class is defined as: health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculator.

- Capacity Manager calculates health only for the license switches. If the health column does not display a value, the switch either does not have a license or it has missed the capacity manager daily cycle.
- If the switch is unlicensed, click **Unlicensed** in the DCNM License column. The **Administration** > **License** window appears which allows you to assign a license to the user.
- The capacity manager runs two hours after the DCNM server starts. So, if you discover a device after two hours of the DCNM start time, the health will be calculated 24 hours after this DCNM start time

Viewing System Information

The switch dashboard displays the details of the selected switch.

Procedure

Step 1 From the Cisco DCNM home page, choose **Monitor > Inventory > Switches**.

An inventory of all the switches that are discovered by Cisco DCNM Web UI is displayed.

Step 2 Click a switch in the **Device Name** column.

The **Switch** dashboard that corresponds to that switch is displayed along with the following information:

Step 3 Click the **System Information** tab. This tab displays detailed system information such as group name, health, module, time when system is up, serial number, the version number, contact, location, DCNM license, status, system log sending status, CPU and memory utilization, and VTEP IP address are displayed. Click **Health** to access the Health score screen, which includes health score calculation and health trend. The popup contains Overview, Modules, Switch Ports, and Events tabs.

- (Optional) Click **SSH** to access the switch through Secure Shell (SSH).
- (Optional) Click **Device Manager** to view a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, a Cisco Nexus 7000 Series switch chassis, or a Cisco Nexus 9000 Series switch chassis including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.
- (Optional) Click **HTTP** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.
- (Optional) Click **Accounting** to go to the Viewing Accounting Information window pertaining to this switch.
- (Optional) Click **Backup** to go to the Viewing a Configuration window.
- (Optional) Click **Events** to go to the Viewing Events Registration window.
- (Optional) Click **Show Commands** to display the device show commands. The Device Show Commands page helps you to view commands and execute them.
- (Optional) Click **Copy Running Config to Startup Config** to copy the running configuration to the startup configuration.

VXLAN

You can view VXLANs and their details under the **VXLAN** tab.

To view VXLANs, choose **Inventory > View > Switches**, and then click a switch name in the **Device Name** column.

The following table describes the fields that are displayed:

Table 1: The VXLAN Tab

Field	Description
VNI	Displays the Layer 2 (network) or Layer 3 (VRF) VXLAN VNI that is configured on a switch.
Multicast address	Displays the multicast address that is associated with the Layer 2 VNI, if applicable.
VNI Status	Displays the status of the VNI.
Mode	Displays the VNI modes: Control Plane or Data Plane.
Type	Displays whether the VXLAN VNI is associated with a network (Layer 2) or a VRF (Layer 3).
VRF	Displays the VRF name that is associated with the VXLAN VNI if it is a Layer 3 VNI.
Mapped VLAN	Displays the VLAN or Bridge domain that is mapped to VNI.

FEX

The Fabric Extender feature allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch that it is attached to. A Fabric Extender is connected to the switch through physical Ethernet interfaces or a Port Channel. By default, the switch does not allow the attached Fabric Extender to connect until it has been assigned a chassis ID and is associated with the connected interface. You can configure a Fabric Extender host interface port as a routed or Layer 3 port. However, no routing protocols can be tied to this routed interface.

Note FEX feature is available on LAN devices only. Therefore, you will see FEX on Cisco DCNM **Inventory Switches**. FEX is also not supported on Cisco Nexus 1000V devices.

Note 4x10G breakout for FEX connectivity is not supported on Cisco Nexus 9500 Switches.

Note The Fabric Extender may connect to the switch through several separate physical Ethernet interfaces or at most one port channel interface.

This section describes how to manage Fabric Extender (FEX) on Cisco Nexus Switches through Cisco DCNM.

You can create and manage FEX from Cisco DCNM **Inventory > Switches**.

Note FEX tab is visible only if you choose a LAN device.

The following table describes the fields that appear on this page.

Table 2: FEX Operations

Field	Description
Show	Allows you to view various configuration details for the selected FEX ID. You can select the following from the drop-down list. • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module The variables for respective show commands are displayed in the Variables area. Review the Variables and click **Execute**. The output appears in the **Output** area. You can create a show template for FEX. Select template type as SHOW and sub type as FEX.

Table 3: FEX Field and Description

Field	Description
Fex Id	Uniquely identifies a Fabric Extender that is connected to a Cisco NX-OS device.
Fex Description	Description that is configured for the Fabric Extender.
Fex Version	Specifies the version of the FEX that is associated with the switch.
Pinning	An integer value that denotes the maximum pinning uplinks of the Fabric Extender that is active at a time.
State	Specifies the status of the FEX as associated with the Cisco Nexus Switch.
Model	Specifies the model of the FEX.
Serial No.	Specifies the configured serial number. **Note** If this configured serial number and the serial number of the Fabric Extender are not the same, the Fabric Extender will not be active.

Field	Description
Port Channel	Specifies the port channel number to which the FEX is physically connected to the Switch.
Ethernet	Refers to the physical interfaces to which the FEX is connected.
vPC ID	Specifies the vPC ID configured for FEX.

Add FEX

To add single-home FEX from the Cisco DCNM Web UI, perform the following steps:

Before you begin

You can add a Fabric Extender (FEX) to the Cisco Nexus Switches through the Cisco DCNM Web Client. If the FEX is physically connected to the switch, FEX will become online after it is added. If the FEX is not physically connected to the switch, the configuration is deployed to the switch, which in turn enables FEX when connected.

Note You can create only single homed FEX through **Inventory > Switches > FEX > Add FEX**. To create a dual-homed FEX, use the vPC wizard through **Configure > Deploy > vPC**.

Ensure that you have successfully discovered LAN devices and configured LAN credentials before you configure FEX.

Procedure

Step 1 Choose **Inventory > Switches > FEX**.

The **FEX** window is displayed.

Step 2 Click the **Add** FEX icon.

Step 3 In the General tab, in the **PORTCHANNEL** field, enter the interface port channel number which is connected to the FEX.

Step 4 In the **INT_RANGE** field, enter the interface range within which the FEX is connected to the switch.

Note Do not enter the interface range, if the interfaces are already a part of port channel.

Step 5 In the **FEX_ID** field, enter the ID for FEX that is connected to a Cisco NX-OS device.

The identifier must be an integer value between 100 to 199.

Step 6 Click **Add**.

The configured Single-home FEX appears in the list of FEXs associated to the device.

Edit FEX

To edit and deploy FEX from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > Switches > FEX**.

The **FEX** window is displayed.

Step 2 Select the FEX radio button that you must edit. Click **Edit** FEX icon.

Step 3 In the Edit Configuration window, from the Policy drop-down list, select **Edit_FEX** to edit the FEX configuration.

Step 4 Edit the **pinning** and **FEX_DESC** fields, as required.

Note If you initially configured port 33 on the parent switch as your only fabric interface, all 48 host interfaces are pinned to this port. If you provision another port, for example 35, then you must perform this procedure to redistribute the host interfaces. All host interfaces are brought down and host interfaces 1 to 24 are pinned to fabric interface 33 and host interfaces 25 to 48 are pinned to fabric interface 35.

Step 5 Click **Preview**.

You can view the generated configuration for the selected FEX ID. The following is a configuration example for FEX ID 101.

```
fex 101
pinning max-links 1
description test
```

Step 6 After you review the configuration summary on the Preview window, on the Edit Configuration screen, click **Deploy** to deploy the FEX for the switch.

VDCs

This section describes how to manage Virtual Device Contexts (VDCs) on Cisco Nexus 7000 Switches through Cisco DCNM.

Users with the network administrator (network-admin) role can create Virtual Device Contexts (VDCs). VDC resource templates limit the amount of physical device resources available to the VDC. The Cisco NX-OS software provides a default resource template, or you can create resource templates.

You can create and manage VDCs from Cisco DCNM **Inventory > Switches > VDCs**. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click an active Cisco Nexus 7000 Switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.

The following table describes the fields that appear on this page.

Table 4: VDC Operations

Field	Description
Add	Click to add a new VDC.

Field	Description
Edit	Select any active VDC radio button and click Edit to edit the VDC configuration.
Delete	Allows you to delete the VDC. Select any active VDC radio button and click Delete to remove the VDC associated with the device.
Resume	Allows you to resume a suspended VDC.
Suspend	Allows you to suspend an active non-default VDC. Save the VDC running configuration to the startup configuration before suspending the VDC. Otherwise, you will lose the changes to the running configuration. **Note** You cannot suspend the default VDC. **Caution** Suspending a VDC disrupts all traffic on the VDC.
Rediscover	Allows you to resume a non-default VDC from the suspended state. The VDC resumes with the configuration that is saved in the startup configuration.
Show	Allows you to view the Interfaces and Resources that are allocated to the selected VDC. In the Interface tab, you can view the mode, admin-status, and operational status for each interface associated with the VDC. In the Resource tab, you can view the allocation of resources and current usage of these resources.

Table 5: Vdc Table Field and Description

Field	Description
Name	Displays the unique name for the VDC
Type	Species the type of VDC. The two types of VDCs are: • Ethernet • Storage
Status	Specifies the status of the VDC.
Resource Limit-Module Type	Displays the allocated resource limit and module type.

Field	Description
HA-Policy • Single Supervisor • Dual Supervisor	Specifies the action that the Cisco NX-OS software takes when an unrecoverable VDC fault occurs. You can specify the HA policies for single supervisor module and dual supervisor module configurations when you create the VDC. The HA policy options are as follows: **Single supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Reload—Reloads the supervisor module. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. **Dual supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. • Switchover—Initiates a supervisor module switchover. The default HA policies for a non-default VDC that you create is restart for a single supervisor module configuration and switchover for a dual supervisor module configuration. The default HA policy for the default VDC is reload for a single supervisor module configuration and switchover for a dual supervisor module configuration.
Mac Address	Specifies the default VDC management MAC address.
Management Interface • IP Address Prefix • Status	Species the IP Address of the VDC Management interface. The status shows if the interface if up or down.
SSH	Specifies the SSH status

Note If you change the VDC hostname of a neighbor device after initial configuration, the link to the old VDC hostname is not replaced with the new hostname automatically. As a workaround, we recommend manually deleting the link to the old VDC hostname.

This chapter includes the following sections:

Add VDCs

To add VDC from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Ensure that you have discovered the physical device using a username that has the network-admin role.

Obtain an IPv4 or IPv6 address for the management interface (mgmt 0) if you want to use out-of-band management for the VDC.

Create a storage VDC to run FCoE. The storage VDC cannot be the default VDC and you can have one storage VDC on the device.

Procedure

Step 1 Choose **Inventory > Switches > VDC**.

The **VDC** window is displayed.

Step 2 Click the **Add** VDC icon.

Step 3 From the drop-down list, select the VDC type.

You can configure the VDC in two modes.

- Configuring Ethernet VDCs
- Configuring Storage VDCs

The default VDC type is Ethernet.

Step 4 Click **OK**.

Configuring Ethernet VDCs

To configure VDC in Ethernet mode from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate Interface tab, select the network interfaces (dedicated interfaces membership) to be allocated to the VDC.

Click **Next**.

Step 3 In the Allocate Resource tab, specify the resource limits for the VDC.

Select the radio button and choose **Select a Template from existing Templates** or **Create a New Resource Template**. VDC resource templates describe the minimum and maximum resources that the VDC can use. If you do not specify a VDC resource template when you create a VDC, the Cisco NX-OS software uses the default template, vdc-default.

- If you choose Select a Template from existing Templates, from the **Template Name** drop-down list, you can select **None**, **global-default**, or **vdc-default**.

  The template resource limits are detailed in the following below:

Table 6: Template Resource Limits

Resource	Minimum	Maximum
Global Default VDC Template Resource Limits		
Anycast Bundled		
IPv6 multicast route memory	8	8 Route memory is in megabytes.
IPv4 multicast route memory	48	48
IPv6 unicast route memory	32	32
IPv4 unicast route memory		
VDC Default Template Resource Limits		
Monitor session extended		
Monitor session mx exception		
Monitor SRC INBAND		
Port Channels		
Monitor DST ERSPAN		
SPAN Sessions		
VLAN		
Anycast Bundled		
IPv6 multicast route memory		
IPv4 multicast route memory		
IPv6 unicast route memory		
IPv4 unicast route memory		

Resource	Minimum	Maximum
VRF		

- If you choose Create New Resource Template, enter a unique **Template Name**. In the Resource Limits area, enter the minimum and maximum limits, as required for the resources.

You can edit individual resource limits for a single VDC through the Cisco DCNM **Web Client > Inventory > Switches > VDC**.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.
- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Configuring Storage VDCs

To configure VDCs in storage mode from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Create a separate storage VDC when you run FCoE on the device. Only one of the VDCs can be a storage VDC, and the default VDC cannot be configured as a storage VDC.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. The shared interface is allocated to both an Ethernet and a storage VDC.

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate FCoE Vlan tab, select the available **Ethernet Vdc** from the drop-down list.

The existing Ethernet VLANs range is displayed. Select **None** not to choose any available Ethernet VDCs.

You can allocate specified FCoE VLANs to the storage VDC and specified interfaces.

Click **Next**.

Step 3 In the Allocate Interface tab, add the dedicated and shared interfaces to the FCoE VDC.

Note The dedicated interface carries only FCoE traffic and the shared interface carries both the Ethernet and the FCoE traffic.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. FCoE VLAN and shared interface can be allocated from same Ethernet VDC.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.

- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Edit VDC

To edit VDC from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Switches** > **VDC**.

The **VDC** window is displayed.

Step 2 Select the VDC radio button that you must edit. Click the **Edit** VDC icon.

Step 3 Modify the parameters as required.

Step 4 After you review the configuration summary on the Summary tab, click **Deploy** the VDC with the new configuration.

Switch On-Board Analytics

For the selected switch, the **Switch On-Board Analytics** dashboard displays the following charts:

Note The graph data cannot be retrieved if correct certificates are not added to the Switch. Ensure that the certificates are valid for nxapi feature and SAN analytics to function properly.

- Top 10 Slowest Ports
- Top 10 Slowest Target Ports
- Top 10 Slowest Flows

- Top 10 Slowest ITLs
- Top 10 Port Traffic
- Top 10 Target Ports Traffic
- Top 10 Flow Traffic
- Top 10 ITL Traffic

The following metrics are supported by the Switch On-Board Analytics charts:

- Read and Write Completion Time—Time that is taken for an IO to complete successfully, that is, the time gap between IO status from a Target and IO command from an Initiator. The following metrics are supported:
  - Read Completion Time Min
  - Read Completion Time Max
  - Write Completion Time Min
  - Write Completion Time Max

  The IO engine tracks the maximum and minimum IO completion time for read and write commands in the context of a switch’s port, target port, flows, initiators, and LUNs.
- Read and Write Initiation Time—Time that is taken for an IO to initiate, that is, the time gap between the first response packet from a Target and IO Command from Initiator. The following metrics are supported:
  - Read Initiation Time Min
  - Read Initiation Time Max
  - Write Initiation Time Min
  - Write Initiation Time Max

  The IO engine tracks the maximum and minimum IO initiation time for read and write commands in the context of a switch’s port, target port, flows, initiators, and LUNs.
- Read and Write IO Bandwidth—Read and write command bandwidth observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO bandwidth is computed at every four second time interval based on the number of bytes read or written.
- Read and Write IO Rate—Read and write command IO rate observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO rate is computed at every four second time interval that is based on the number of IO performed.
- Read and Write IO Size—Read and write command IO size observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The following metrics are supported:
  - Read IO Size Min
  - Read IO Size Max
  - Write IO Size Min
  - Write IO Size Max

The IO engine tracks the maximum and minimum IO size for read and write commands.

Viewing Switch On-Board Analytics

You can view the switch on-board analytics information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The discovered switches are displayed.

Step 2 Click a switch name in the **Device Name** column.

The **Switch** dashboard that corresponds to that switch is displayed.

Step 3 Click the **Switch On-Board Analytics** tab.

This tab displays the Switch On-Board Analytics charts.

Configuring Settings for the Switch On-Board Analytics Charts

Perform the following actions to configure the settings for the switch on-board analytics charts:

- From the **Show Time as** drop-down list, choose time to be shown in the charts. You can choose one of the following options:
  - **Microseconds**
  - **Milliseconds**
  - **Seconds**

  By default, **Microseconds** is chosen.

  Note The **Show Time** drop-down list is applicable only for the top ten slowest ports, target ports, flows, and ITLs.

- From the **Show Flow From** drop-down list, choose whether to show flows from a **Target** or from an **Initiator**. By default, flows from a **Target** are chosen.

  Note The **Show Flow From** drop-down list is applicable only for the charts displaying flows and ITLs.

- From the **Show bandwidth and Size as** drop-down list, choose the traffic information to be shown in the charts. You can choose one of the following options:
  - **Bytes**

- **KB**
- **MB**

By default, **Bytes** is chosen.

- Check the **Filter results** check box, and click either the **by fc port** or **by VSAN** radio button and specify the appropriate values to filter the chart results. The FC port value must be in the **fc** *slot*/*port* format and the VSAN value must be a digit within the allowed VSAN range.

  Click the Filter icon next to the **by fc port** to apply changes.

  Note Filtering results by VSAN is not applicable for the **Top 10 Slowest Ports** or **Top 10 Port Traffic** charts.

- Check the **Single Column** check box to display the charts in a single column instead of double columns.
- Click the **Refresh** icon in the upper-right corner to refresh the charts.

Viewing Switch On-Board Analytics Charts

Perform the following actions to view the charts under the **Switch On-Board Analytics** tab:

- View the charts for the top ten slowest ports, target ports, flows, and ITLs by choosing one of the following variables from the drop-down list:
  - **Read Completion Time**—The read command completion time observed in the context of a switch's port.
  - **Write Completion Time**—The write command completion time observed in the context of a switch's port.
  - **Read Initiation Time**—The read command initiation time observed in the context of a switch's port.
  - **Write Initiation Time**—The write command initiation time observed in the context of a switch's port.

  Note
  - By default, **Read Completion Time** is selected and all the units for time are in **Microseconds**.
  - Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- View the charts for the top ten port traffic, target port traffic, flow traffic, and ITL traffic by choosing one of the following variables from the drop-down list:
  - **Read IO Rate**—The read command data observed in the context of a switch's port.
  - **Write IO Rate**—The write command observed in the context of a switch's port.

- **Read IO Size**—The read command size observed in the context of a switch's port.
- **Write IO Size**—The write command size observed in the context of a switch's port.
- **Read IO Bandwidth**—The read command bandwidth observed in the context of a switch's port.
- **Write IO Bandwidth**—The write command bandwidth observed in the context of a switch's port.

Note

- By default, **Read IO Rate** is selected. The **Read IO Rate** is IO per second. Both **Rate** and **Bandwidth** units are per second over an 8-second range. The **Size** value is for the life of the switch or since the last clear command was run from the CLI.
- The **Read IO Size** and **Read IO Bandwidth** units are in bytes per second. You can change this unit by using the **Show Bandwidth and Size** drop-down list. You can choose from the three options: **Bytes**, **KB**, and **MB**.
- Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- Choose the format to display information from the **Show** drop-down list. You can choose one of the following formats:
  - **Chart**
  - **Table**
  - **Chart and Table**

Note

- To display information in the **Chart and Table** format, enlarge your browser window or check the **Single Column** check box on the upper right corner.
- The default for Top ten Slowest Ports and Top 10 Port Traffic is **Chart and Table**.

- Use the **Chart Type** drop-down list to display information in the **Bar Chart** or **Stacked Bar Chart**.
- Use the **Actions** drop-down list to export information in a CSV or PDF, or print the required information.
- To view a chart or a table in a new window, click the **Detach** icon on the upper-right corner of a chart or a table. After detaching a chart or table, you can view the top 25 slowest ports, target ports, flows, ITLs, or their traffic.

Viewing Inventory Information for Modules

To view the inventory information for modules from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Modules**.

The **Modules** window is displayed with a list of all the switches and its details for a selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of the module.
- **Switch** column displays the switch name on which the module is discovered.
- **Name** displays the module name.
- **ModelName** displays the model name.
- **SerialNum** column displays the serial number.
- **2nd SerialNum** column displays the second serial number.
- **Type** column displays the type of the module.
- **Slot** column displays the slot number.
- **Hardware Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.
- **OperStatus** column displays the operation status of the module.

Viewing Inventory Information for Licenses

To view the inventory information for licenses from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Licenses**.

The **Licenses** window is displayed based on the selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of switches.
- **Switch** column displays the switch name on which the feature is enabled.
- **Feature** displays the installed feature.
- **Status** displays the usage status of the license.
- **Type** column displays the type of the license.

- **Warnings** column displays the warning message.

Monitoring Switch

The Switch menu includes the following submenus:

Viewing Switch CPU Information

To view the switch CPU information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > CPU**.

The **CPU** window is displayed. This window displays the CPU information for the switches in that scope.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last 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 Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year. You can choose the chart type and chart options to show as well.

Viewing Switch Memory Information

To view the switch memory information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Memory**.

The memory panel is displayed. This panel displays the memory information for the switches in that scope.

Step 2 Use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last 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

To view the switch traffic and errors information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Traffic**.

The **Switch Traffic** panel is displayed. This panel displays the traffic on that device for the past 24 hours.

Step 2 Use the drop-down to filter the view by 24 hours, Week, Month, and Year.

Step 3 Click the **Export** icon in the upper-right corner to export the data into a spreadsheet.

Step 4 Click **Save**.

Step 5 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**. Only sensors that have historical temperature data is shown in the list. You can choose between Last ten Minutes, Last Hour, Last Day, Last Week, and Last Month.

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

To view the switch temperature information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 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 that it belongs to is shown as its scope. When the scope selector at the top of Cisco DCNM is used, the sensor list is filtered by that scope.
- **Switch**: 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 that is 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.

A chart is displayed, 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 of LAN switches for which you want to collect performance data.
4. Click **Apply** to save the configuration.

Viewing Accounting Information

To view the accounting information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 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**, **Username**,**Time**, and **Description**. Or select **Quick Filter** to search under each column.

Step 3 You can also select a row and click 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

To view the events and syslog from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 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 the same event has occurred during the time period as shown in the **Last Seen** and **First Seen** columns.

Click a switch name in the **Switch** column to view the switch dashboard.

Step 2 Select an event in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule.

Step 3 Select one or more events from the table and click the **Acknowledge** icon to acknowledge the event information for the fabric.

- After you acknowledge the event for a fabric, the acknowledge icon is displayed in the **Ack** column next to the fabric.

Step 4 Select the fabric and click the **Unacknowledge** icon to cancel an acknowledgment for a fabric.

Step 5 Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **Username**,**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 event information from the list.

Step 7 Click the **Print** icon to print the event details.

Step 8 Click the **Export to Excel** icon to export the data.

Monitoring LAN

The LAN menu includes the following submenus:

Monitoring Performance Information for Ethernet

To monitor the performance information for ethernet from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > Ethernet**.

The **Ethernet** window is displayed.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last 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 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 Thresholds section to turn on performance data collection.

Monitoring ISL Traffic and Errors

To monitor the ISL traffic and errors from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > Link**.

The **ISL Traffic and Errors** window is displayed. 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 Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last 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 endpoints. 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 is isplayed.

Cisco DCNM **Web Client > Monitor> vPC** displays 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 UI > Configure > Deploy > vPC Peer** and **Web Client > Configure > Deploy > vPC**.

Table 7: vPC Performance, on page 25 displays the following vPC configuration details in the data grid view.

Table 7: vPC Performance

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

Column	Description
Secondary vPC Peer - Capacity	Displays the capacity for the secondary vPC peer.
Secondary vPC Peer - Avg. Rx/sec	Displays the average receiving speed of secondary vPC peer.
Secondary vPC Peer - Avg. Tx/sec	Displays the average sending speed of secondary vPC peer.
Secondary vPC Peer - Peak Util%	Displays the peak utilization percentage of secondary vPC peer.

You can use this feature as following:

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.

To view the VPC performance information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > vPC**.

The **vPC Performance** statistics is displayed. The aggregated statistics of all vPCs are displayed in a tabular manner.

Step 2 Click the **vPC ID**.

The vPC topology, **vPC Details**, **Peer-link Details**, and **Peer-link Status** are displayed.

The **vPC Consistency**, **Peer-link Consistency**, and **vPC Type2 Consistency** for the vPC are 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, to 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. The parameter details of **Role Status** and **vPC Peer keep-alive Status** for both Primary and Secondary vPC devices is also displayed.

Step 3 Click 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.

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 print the vPC Utilization data, click the **Print** icon in the upper-right corner. The vPC Utilization page appears.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save File**.

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

Monitoring Endpoint Locator

The Endpoint Locator menu includes the following submenus:

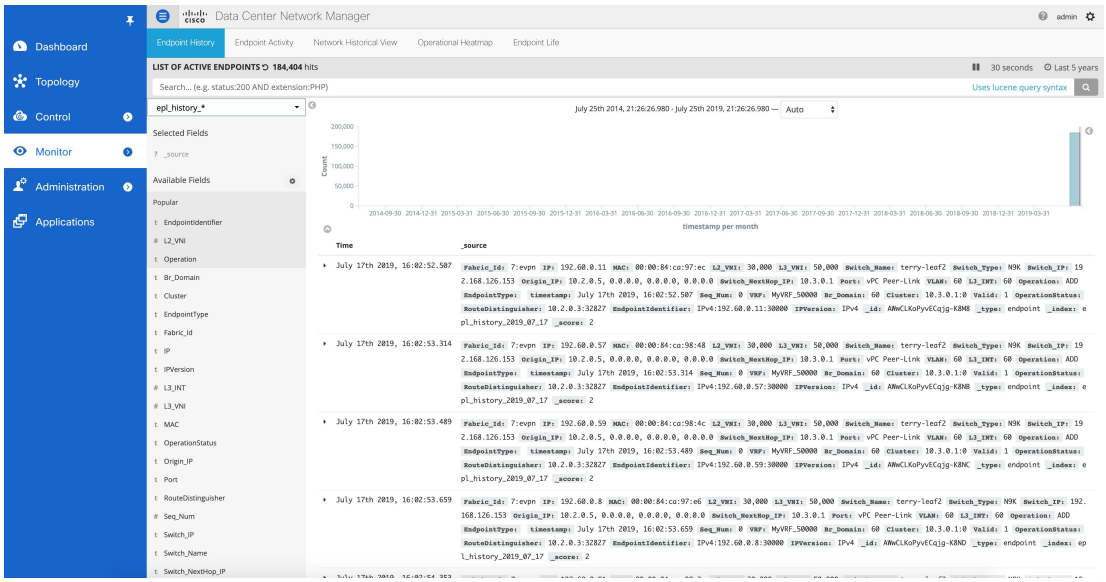
Exploring Endpoint Locator Details

To explore endpoint locator details from the Cisco DCNM Web UI, perform the following steps:

Procedure

Choose **Monitor > Endpoint Locator > Explore**. The Endpoint Locator dashboard appears.
The Endpoint Locator Dashboard displays the following information:

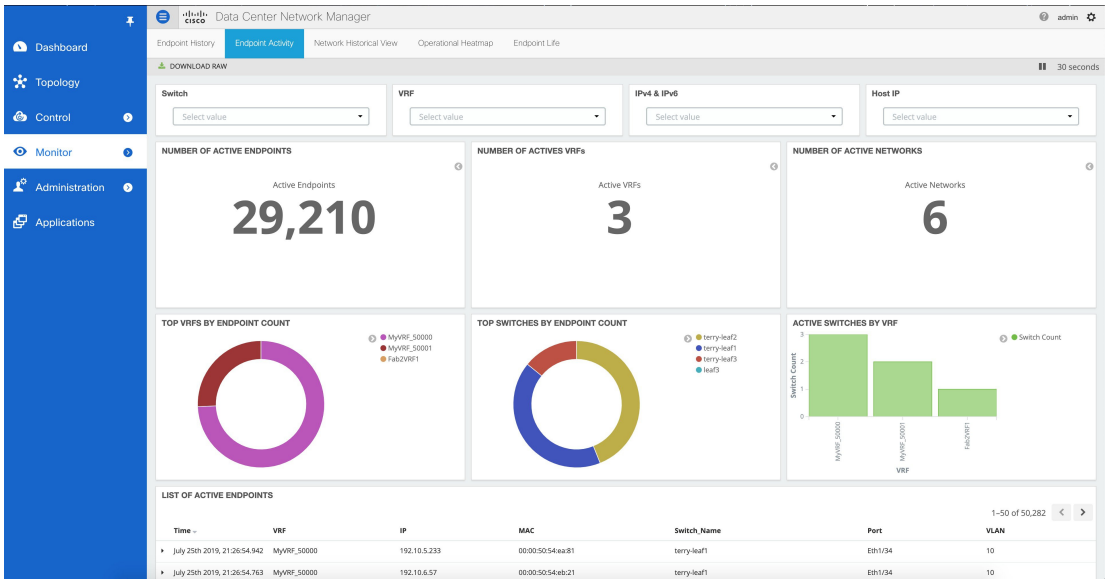
- **Endpoint History**—Real time plot displaying Endpoint events for the period specified in the relative or absolute date range. A user can search for a specific metric value in the search bar. Search is supported on any of the fields as specified under the “Available Fields” column on the menu on the 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.

  Filters - You can filter and view results for a switch, VRF, IPv4 and IPv6 type of address and IP address of an end point. The entire dashboard view across all tiles and the data table, are updated as soon as the search filters are applied.

  Tiles - The number of active endpoints including the number of active VRFs and active networks are listed in the top 3 tiles, just below the filters. The break-up of active endpoints is also available on a per VRF as well as a per switch basis. 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 named LIST OF ACTIVE ENDPOINTS which 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.

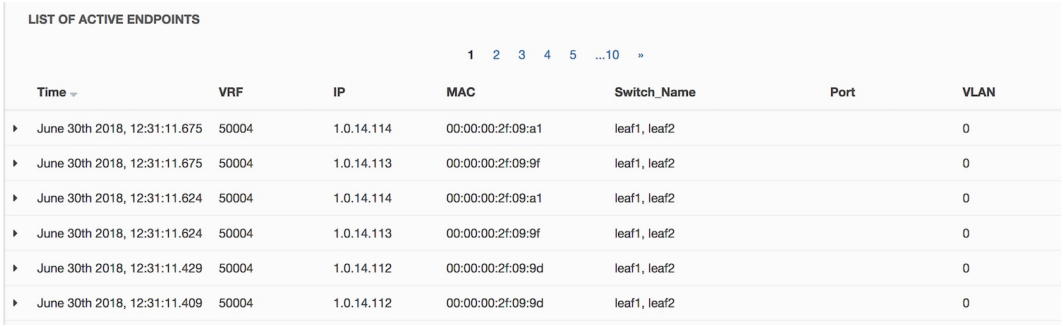


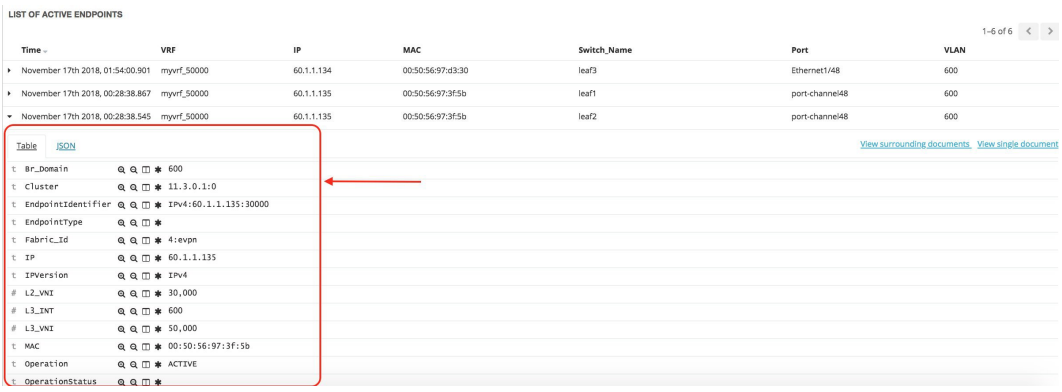
Search results can be downloaded in csv format by clicking on the “DOWNLOAD RAW” icon at the top left part of the screen. A sample snippet of the downloaded csv file from a search result is shown below:

	Fabric_Id	IP	MAC	L2_VNI	L3_VNI	Switch_Nam	Switch_Type	Switch_IP	Origin_IP	Switch_Next	Port	VLAN	L3_INT	Operation	EndpointType	timestamp	Seq_Num	VRF	Br_Domain	Cluster	Valid	Op
2	3:evpn	1.0.14.114	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.6| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
3	3:evpn	1.0.14.113	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.6| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
4	3:evpn	1.0.14.114	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.6| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
5	3:evpn	1.0.14.113	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.6| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
6	3:evpn	1.0.14.112	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
7	3:evpn	1.0.14.112	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
8	3:evpn	1.0.14.111	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
9	3:evpn	1.0.14.111	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
10	3:evpn	1.0.14.109	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
11	3:evpn	1.0.14.110	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
12	3:evpn	1.0.14.110	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
13	3:evpn	1.0.14.109	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
14	3:evpn	1.0.14.108	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
15	3:evpn	1.0.14.108	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
16	3:evpn	1.0.14.107	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.7| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	
17	3:evpn	1.0.14.107	00:00:00:2f:(	30003	50004	leaf1| leaf2	N9K	24.0.80.203	10.1.0.6| 10.	10.2.0.1		0	0	ACTIVE		2018-06-30 12:3:	0	50004	0	10.2.0.1:0	1	

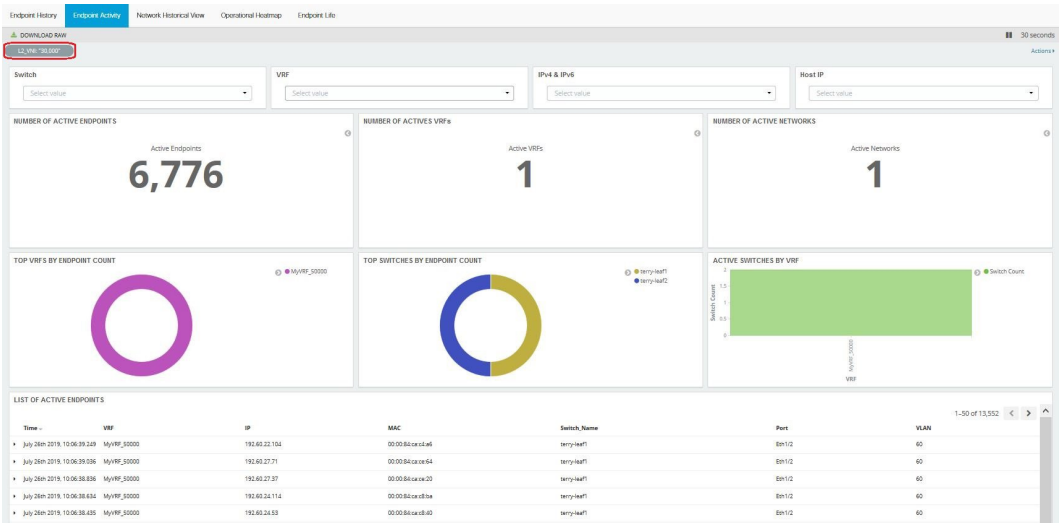
It is possible to search based on any of the fields describing the information of each endpoint. For example, if the user wants to know the list of endpoints in a given network, that can be achieved as follows. Recall that each network is represented by a unique 24-bit identifier. This parameter is represented by the field L2_VNI. Here are the steps:

a. Go to the LIST OF ACTIVE ENDPOINTS data table and click on any row. This will expand the row as shown below:



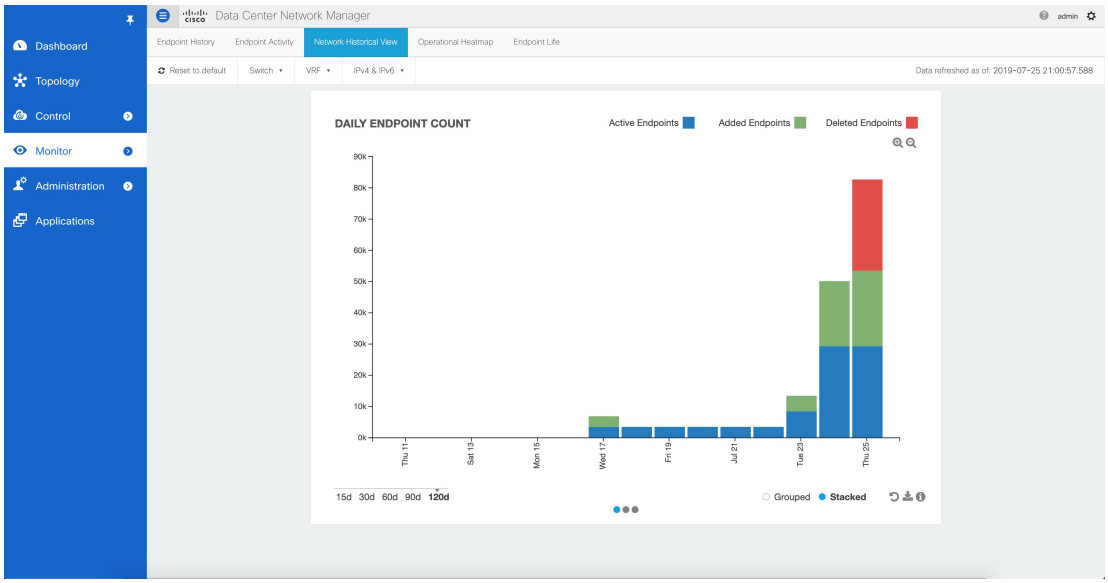


b. Click the **Filter for value +** icon next to the L2_VNI field. This selects the highlighted value (30000 in this example) and filters the search results based on that. In other words, the information of all active endpoints in the network associated with L2_VNI 30000 is displayed on the dashboard. If instead, all endpoints that are not in the network L2_VNI are required, click the – icon next to the L2_VNI value of 30000. In the same manner, one can choose any combination of fields to get the set of endpoints matching the corresponding selected filter criteria.

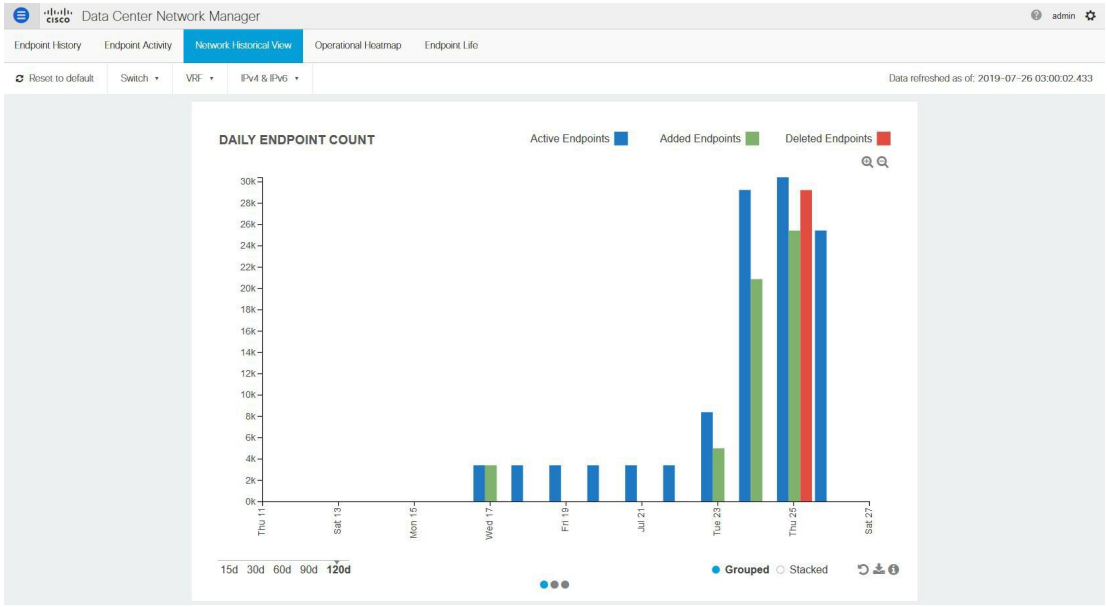


- **Network Historical View**— The NHV view displays historical information of endpoints, networks, and VRFs (tenants) captured on a daily basis. These graphs are updated once a day at mid-night based on the DCNM server time. The time at which the data is refreshed/updated is listed at the top right. 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.

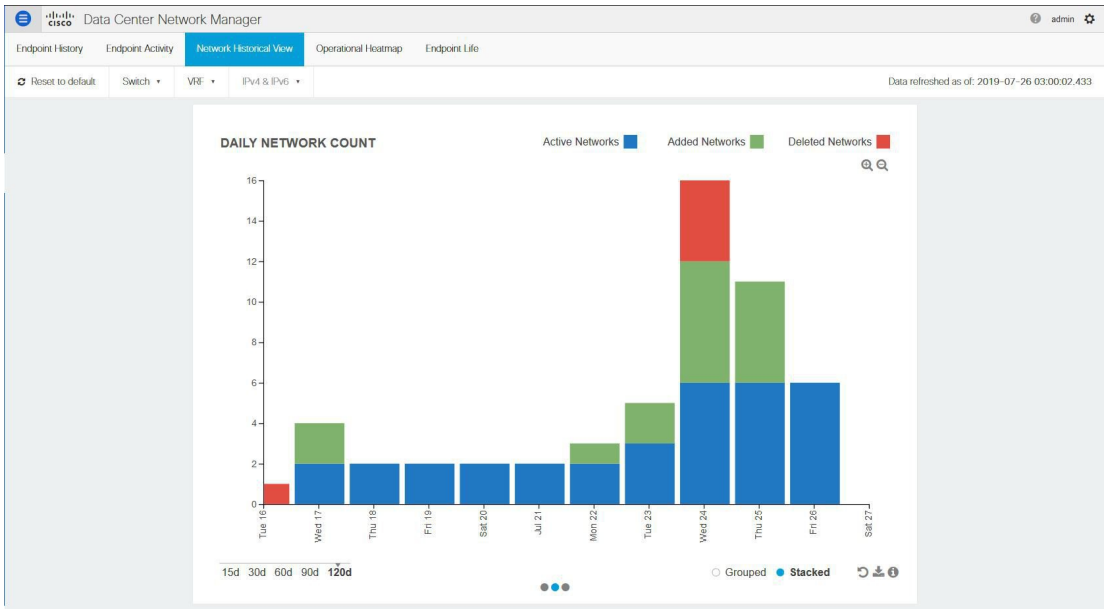
  The historic endpoint count in ‘Stacked’ format is shown below:



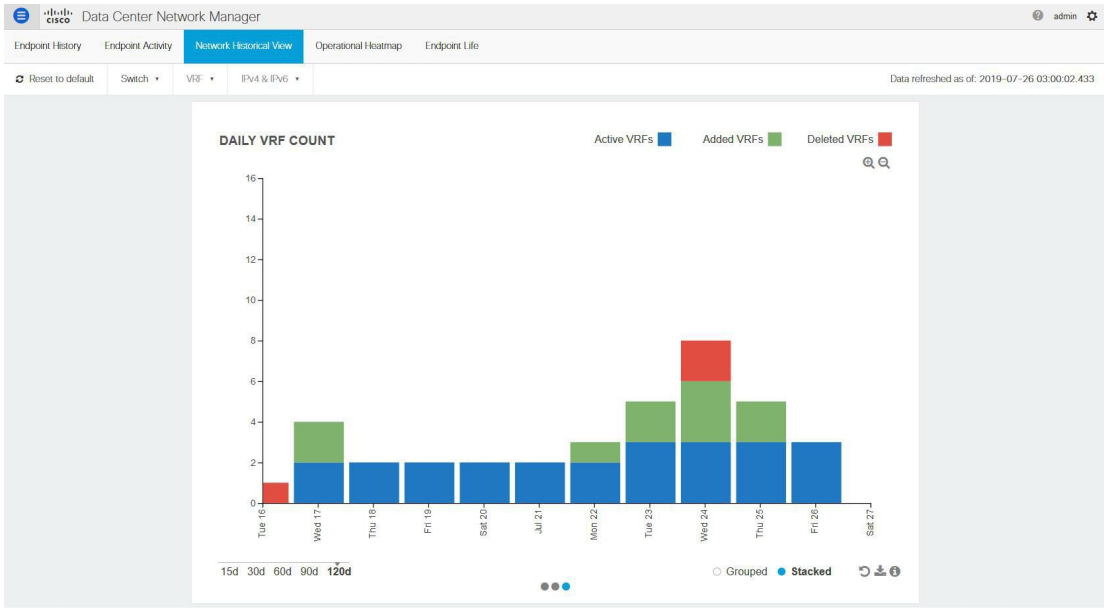
The same representation with the Grouped visualization selection is shown below:



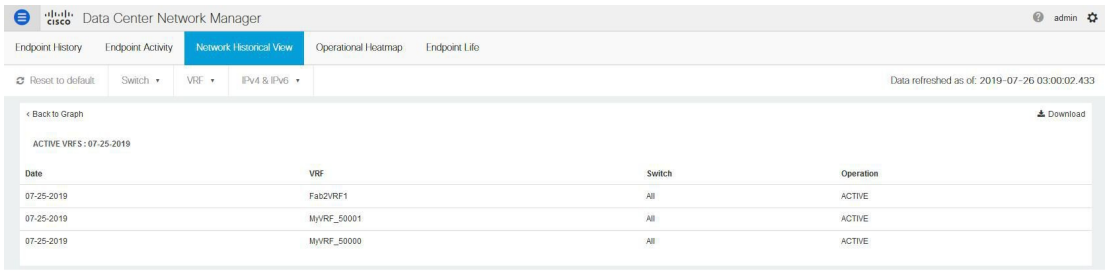
Similarly, the figure below depicts the historic network count in stacked format:



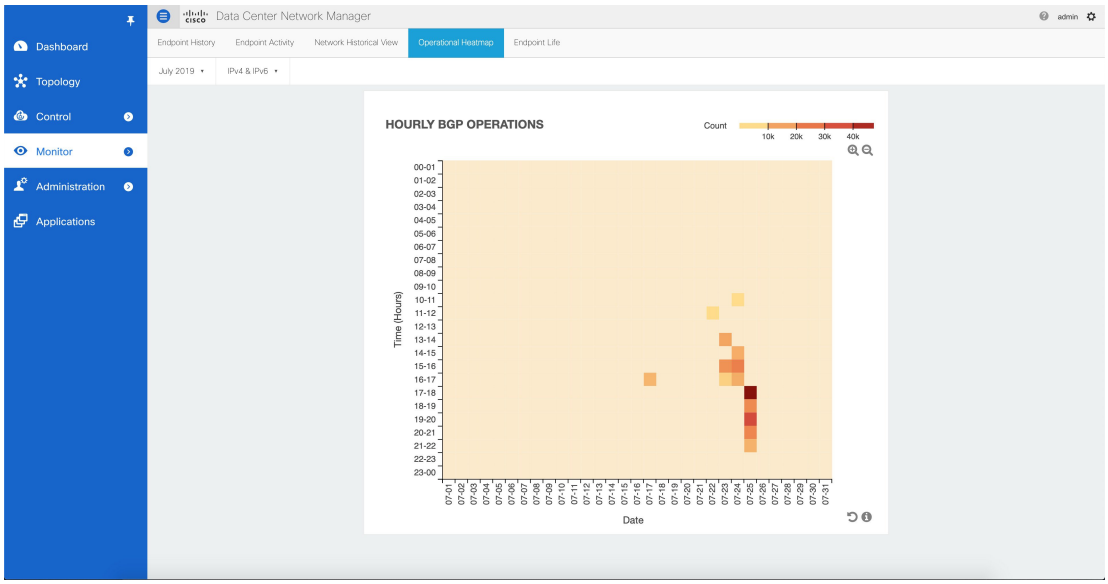
Along the same lines, the figure below depicts the historic vrf count:



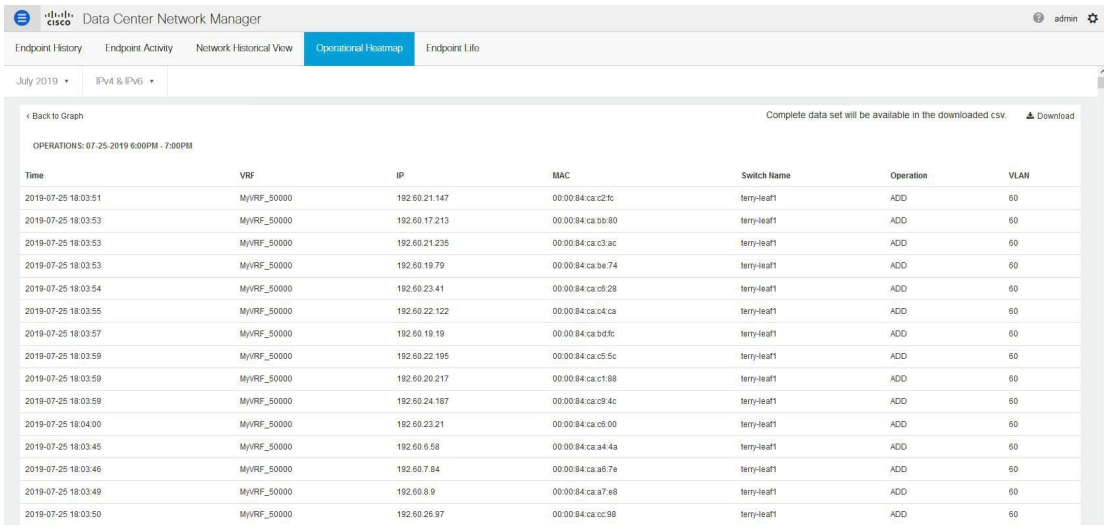
The figure below provides a sample screenshot of the endpoints added on 07-25-2019 obtained by clicking on the blue bar for that day.



- **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.

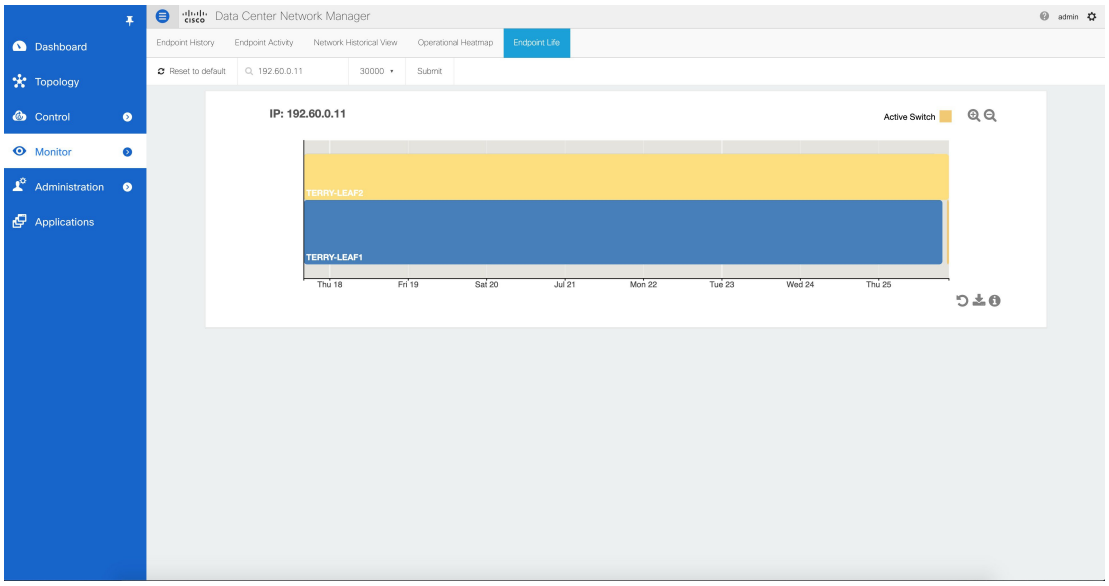


Time	VRF	IP	MAC	Switch Name	Operation	VLAN
2019-07-25 18:03:51	MyVRF_50000	192.60.21.147	00:00:84:ca:c2:fc	terry-leaf1	ADD	60
2019-07-25 18:03:53	MyVRF_50000	192.60.17.213	00:00:84:ca:bb:80	terry-leaf1	ADD	60
2019-07-25 18:03:53	MyVRF_50000	192.60.21.235	00:00:84:ca:c3:ac	terry-leaf1	ADD	60
2019-07-25 18:03:53	MyVRF_50000	192.60.19.79	00:00:84:ca:be:74	terry-leaf1	ADD	60
2019-07-25 18:03:54	MyVRF_50000	192.60.23.41	00:00:84:ca:c6:28	terry-leaf1	ADD	60
2019-07-25 18:03:55	MyVRF_50000	192.60.22.122	00:00:84:ca:c4:ca	terry-leaf1	ADD	60
2019-07-25 18:03:57	MyVRF_50000	192.60.19.19	00:00:84:ca:bd:fc	terry-leaf1	ADD	60
2019-07-25 18:03:59	MyVRF_50000	192.60.22.195	00:00:84:ca:c5:5c	terry-leaf1	ADD	60
2019-07-25 18:03:59	MyVRF_50000	192.60.20.217	00:00:84:ca:c1:88	terry-leaf1	ADD	60
2019-07-25 18:03:59	MyVRF_50000	192.60.24.187	00:00:84:ca:c9:4c	terry-leaf1	ADD	60
2019-07-25 18:04:00	MyVRF_50000	192.60.23.21	00:00:84:ca:c6:00	terry-leaf1	ADD	60
2019-07-25 18:03:45	MyVRF_50000	192.60.6.58	00:00:84:ca:a4:4a	terry-leaf1	ADD	60
2019-07-25 18:03:46	MyVRF_50000	192.60.7.84	00:00:84:ca:a6:7e	terry-leaf1	ADD	60
2019-07-25 18:03:49	MyVRF_50000	192.60.8.9	00:00:84:ca:a7:e8	terry-leaf1	ADD	60
2019-07-25 18:03:50	MyVRF_50000	192.60.26.97	00:00:84:ca:cc:98	terry-leaf1	ADD	60

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:

	Fabric_Id	IP	MAC	L2_VNI	L3_VNI	Switch_Nam	Switch_Type	Switch_IP	Origin_IP.0	Origin_IP.1	Origin_IP.2	Origin_IP.3	Switch_Next	Port	VLAN	L3_INT	Operation	EndpointType	Timestamp	Seq_Num	VRF	Br_Domain	Clust
2	3:evpn	51.1.1.33	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
3	3:evpn	51.1.1.53	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
4	3:evpn	51.1.1.93	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
5	3:evpn	51.1.1.12	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
6	3:evpn	51.1.1.35	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
7	3:evpn	51.1.1.88	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
8	3:evpn	51.1.1.50	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
9	3:evpn	51.1.1.79	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
10	3:evpn	51.1.1.45	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
11	3:evpn	51.1.1.71	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
12	3:evpn	51.1.1.67	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
13	3:evpn	51.1.1.38	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
14	3:evpn	51.1.1.27	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
15	3:evpn	51.1.1.94	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
16	3:evpn	51.1.1.96	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
17	3:evpn	51.1.1.47	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
18	3:evpn	51.1.1.56	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
19	3:evpn	51.1.1.60	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
20	3:evpn	51.1.1.83	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
21	3:evpn	51.1.1.18	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
22	3:evpn	51.1.1.57	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
23	3:evpn	51.1.1.61	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
24	3:evpn	51.1.1.12	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
25	3:evpn	51.1.1.19	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
26	3:evpn	51.1.1.65	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(
27	3:evpn	51.1.1.75	00:00:48:69:/	30009	50002	leaf1, leaf2	N9K	24.0.80.203	10.1.0.7	0.0.0.0	0.0.0.0	0.0.0.0	10.2.0.1		0	0	ADD		Sun Jul 01 2(	0	50002	0	10.2.(

- **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.

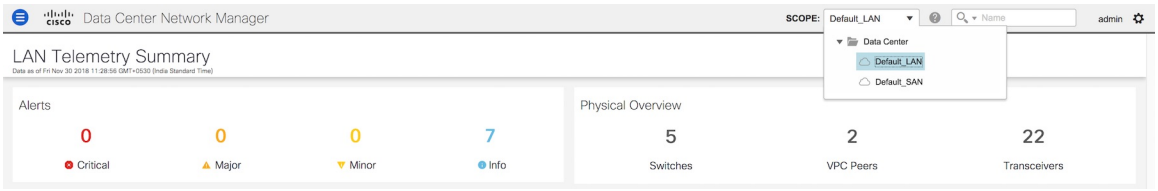
	A	B	C	D	E	F
1	Switch Name	VRF	EndPointIdentifier	Start Timestamp	End Timestamp	Active
2	n9k-12-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Dec 27 2017 21:41:33 GMT+0530 (India Standard Time)	Tue Jan 02 2018 18:56:32 GMT+0530 (India Standard Time)	
3	n9k-13-vpc	Beer:Corona	IPv4:60.1.1.134:30007	Wed Dec 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

LAN Telemetry

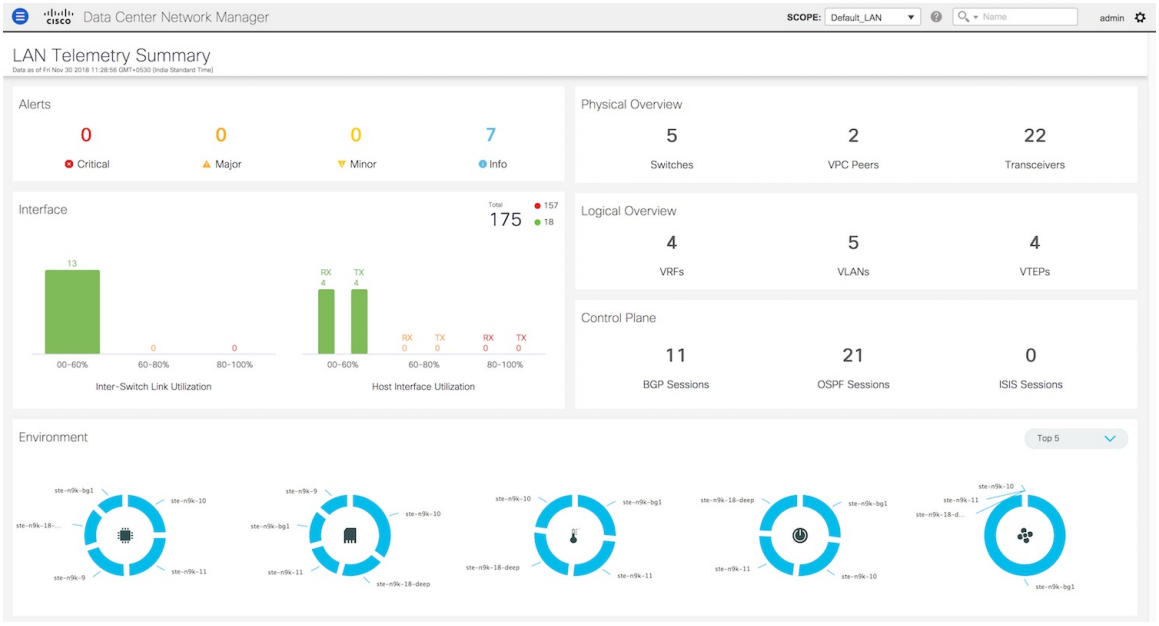
The LAN Telemetry menu includes the following submenus:

Monitoring LAN Telemetry

Once LAN telemetry has been successfully enabled, the LAN Telemetry Summary window is available. You can navigate to the LAN Telemetry Summary window by choosing **Monitor > LAN Telemetry > Explore**. Select the fabric (for example, Default_LAN) for which LAN telemetry has been enabled through the SCOPE at the top.

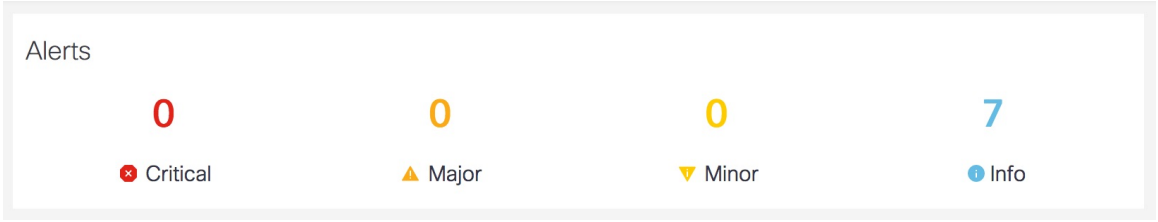


There are six insights (Alerts, Physical Overview, Logical Overview, Control Plane, Interface, and Environment) shown through interactive visualizations depicting different aspects of switch metrics. Click the Alerts, Physical Overview, Logical Overview, Control Plane, and Interface tiles to find more information about the metrics. On the Environment tile, click the donut chart icons to display more information. The Environment tile displays metrics for CPU usage, Memory, Temperature, Power, and Fans.

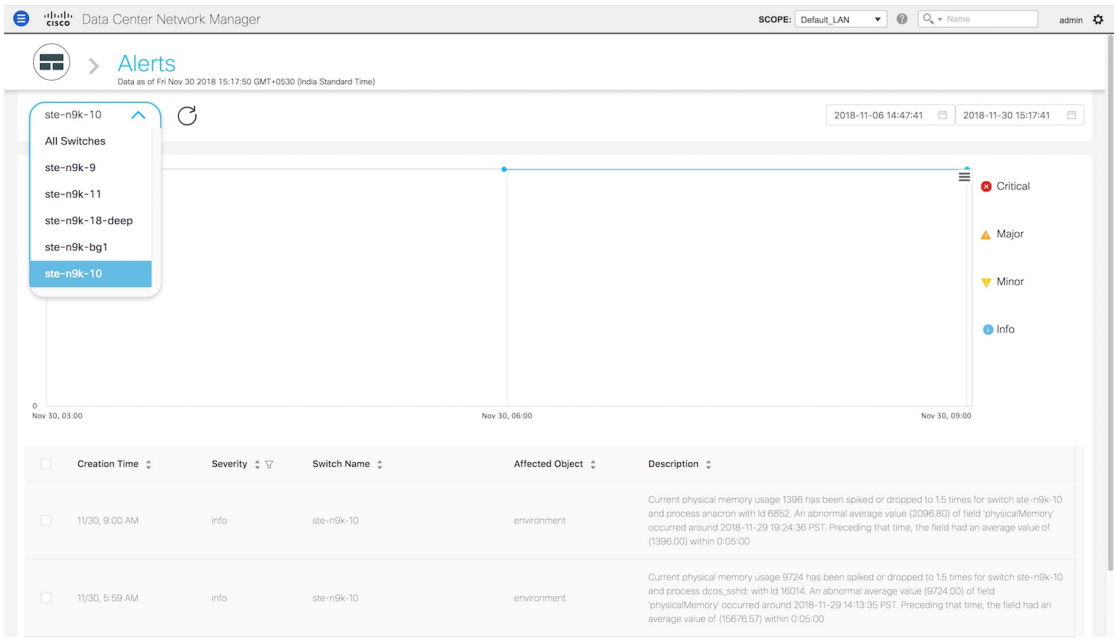


Alerts

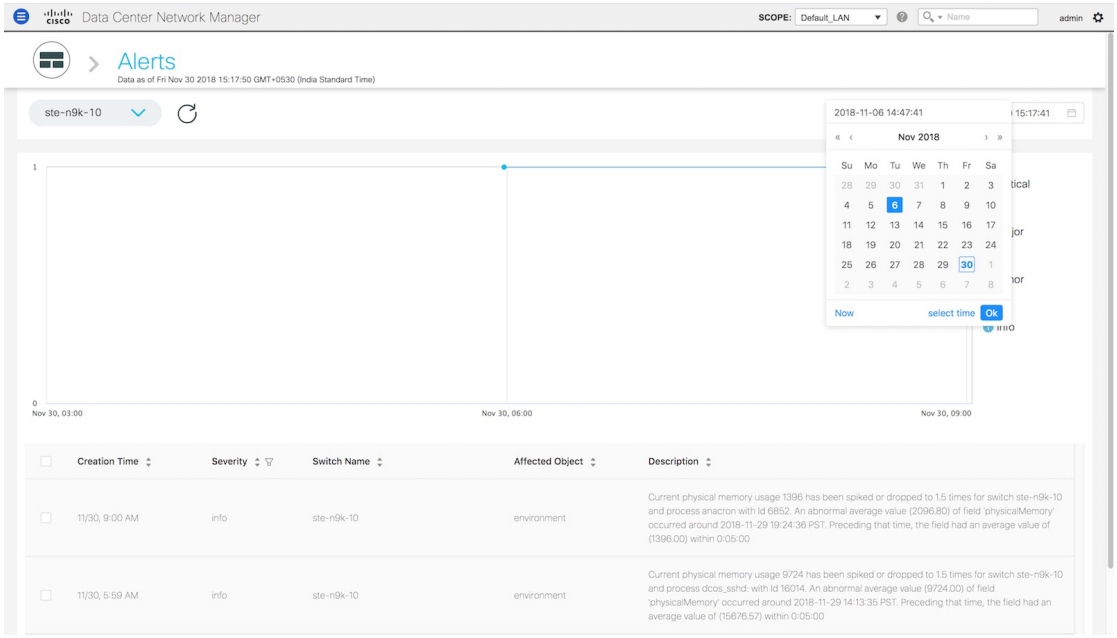
The **Alerts** tile displays the number of alerts that have occurred. The alerts are classified as Critical, Major, Minor, and Info. Each kind of alert is associated with a specific color.



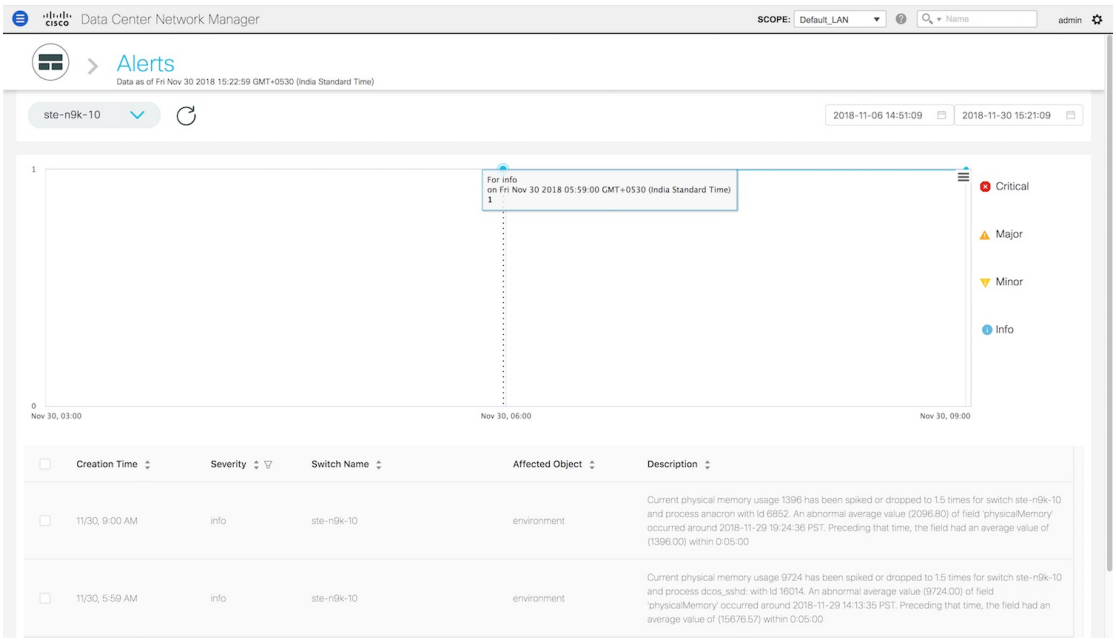
1. Click the **Alerts** tile for more information about the alerts. You can select a specific switch for which you want to display the metrics. You can also select **All Switches** to display metrics for all the switches in the selected fabric.



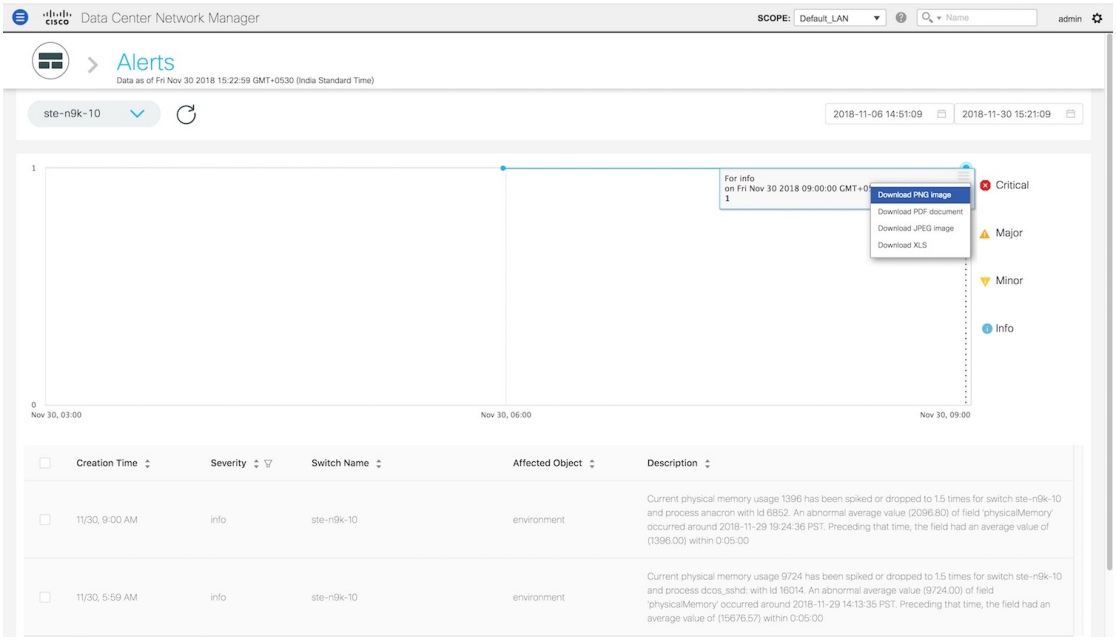
2. You can select a specific time interval to view the alerts that have occurred in that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



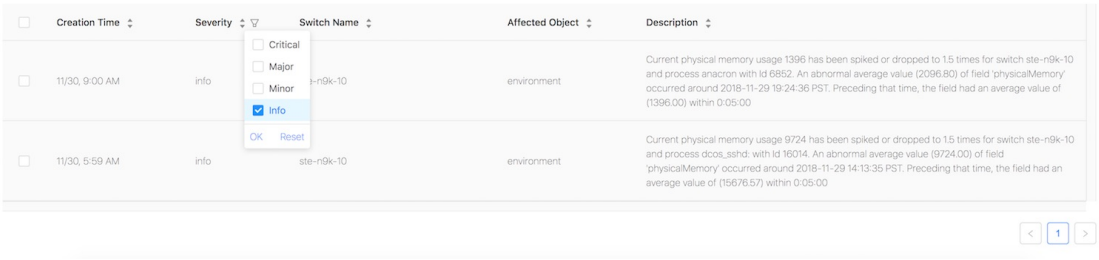
3. Hover over specific points on the graph for the time at which the alert has occurred.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



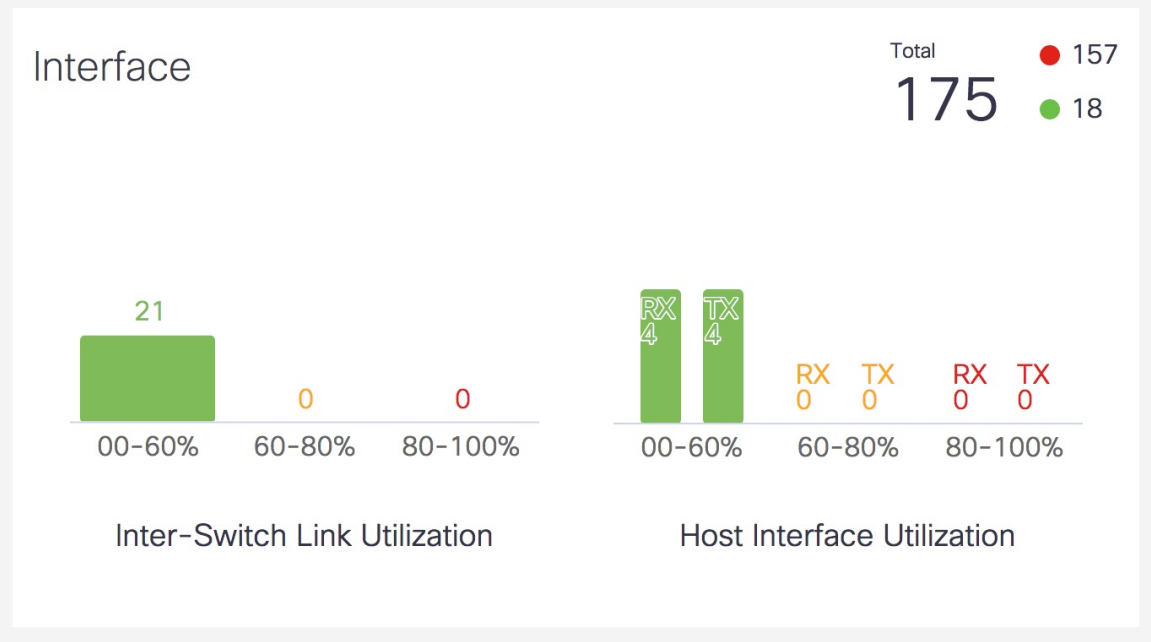
5. The bottom of the page has the following fields: **Creation Time**, **Severity**, **Switch Name**, **Affected Object** and **Description**. These fields provide more information about each alert. Click the filter icon next to Severity to filter the alerts based on severity level.



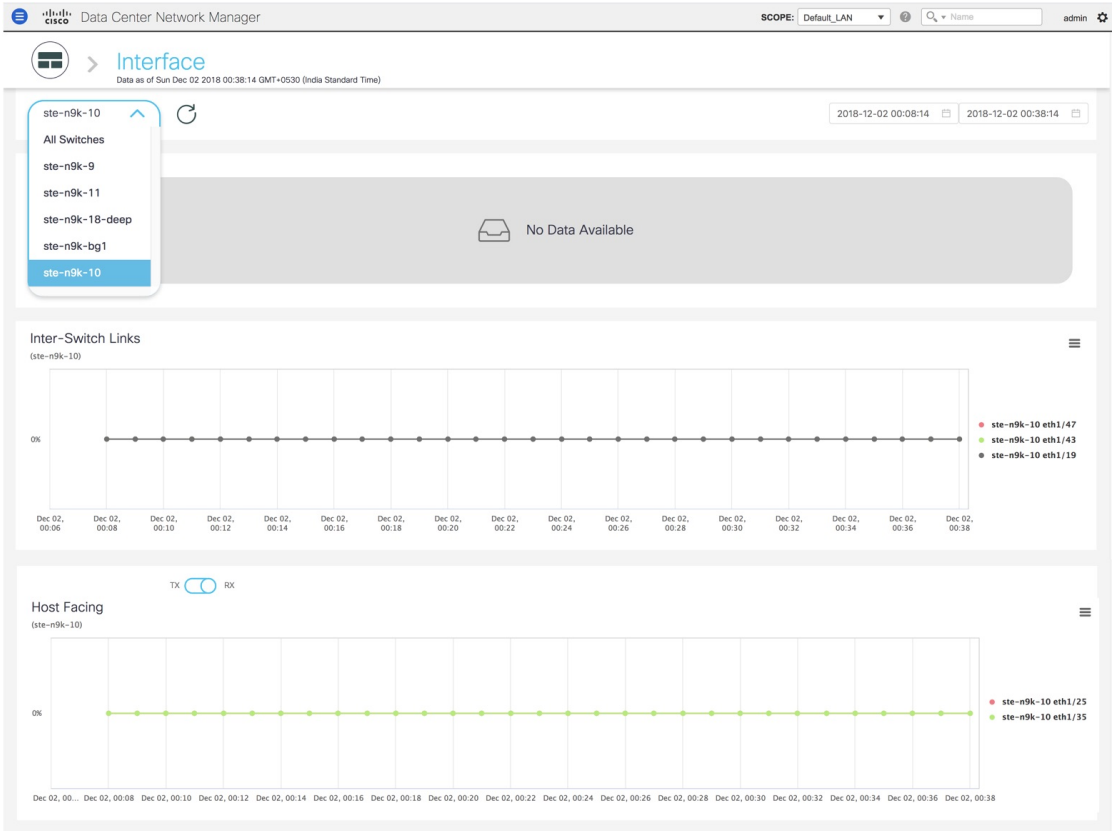
6. Click the icon next to **Alerts** at the top of the window to go back to the LAN Telemetry Summary window.

Interface

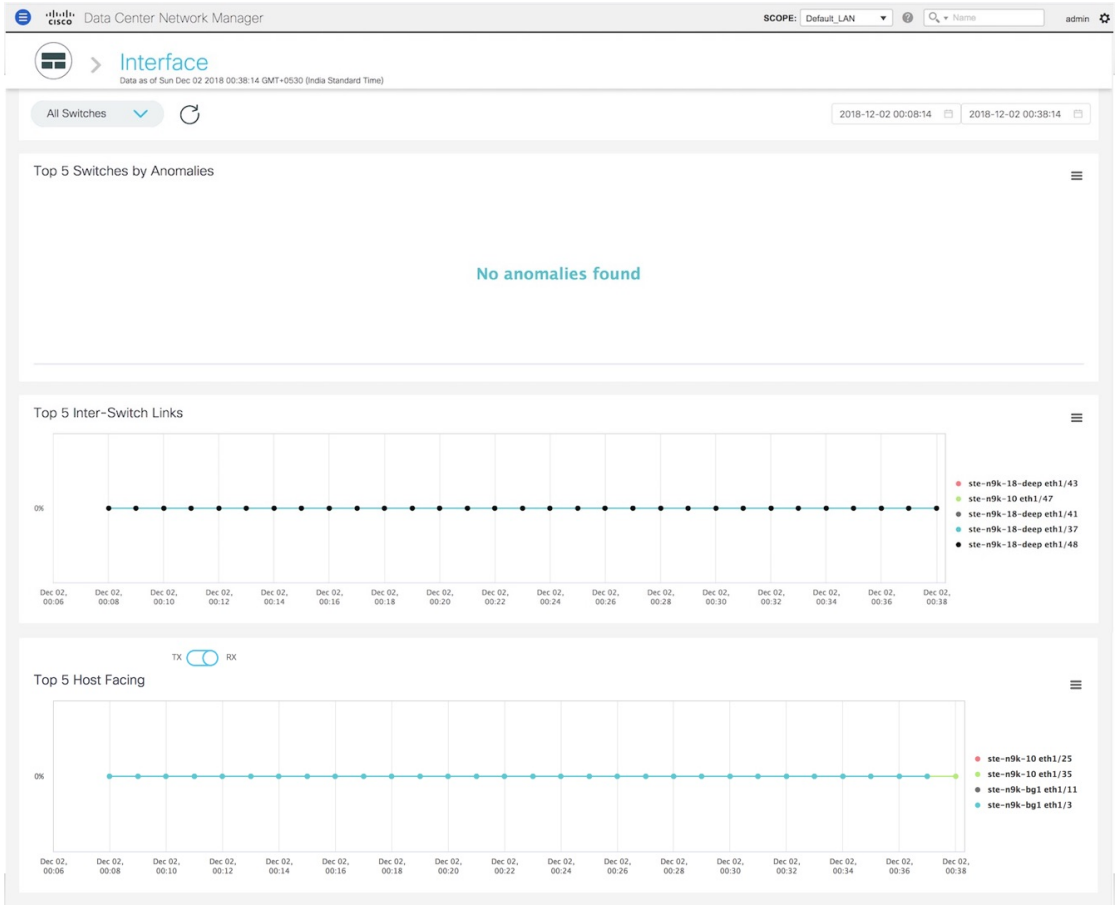
The **Interface** tile displays the Inter-Switch Link Utilization and Host Interface Utilization metrics. It shows the number of Inter-Switch Links in the fabric along with the associated percentage, and the number of host interfaces that are utilized to send and receive data from hosts along with the associated percentage. On the top right of the **Interface** tile, you can see the number of interfaces that are down next to the red dot and the number of interfaces that are up next to the green dot along with the total number of interfaces in the fabric.



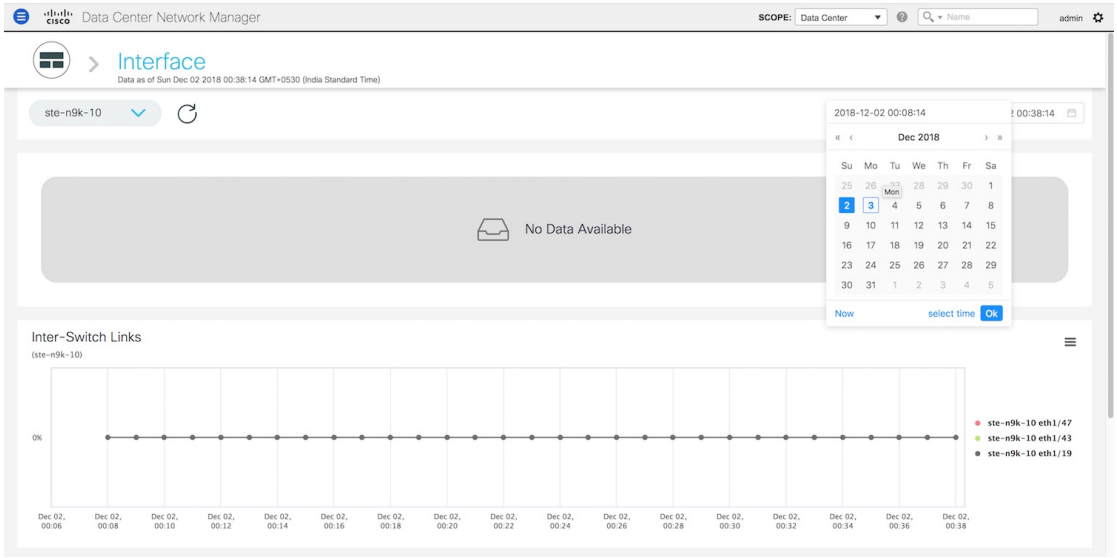
1. Click the **Interface** tile to display more information about the ISLs and Host Interfaces. On the **Interface** window, you can select a specific switch for which you want to display the metrics.



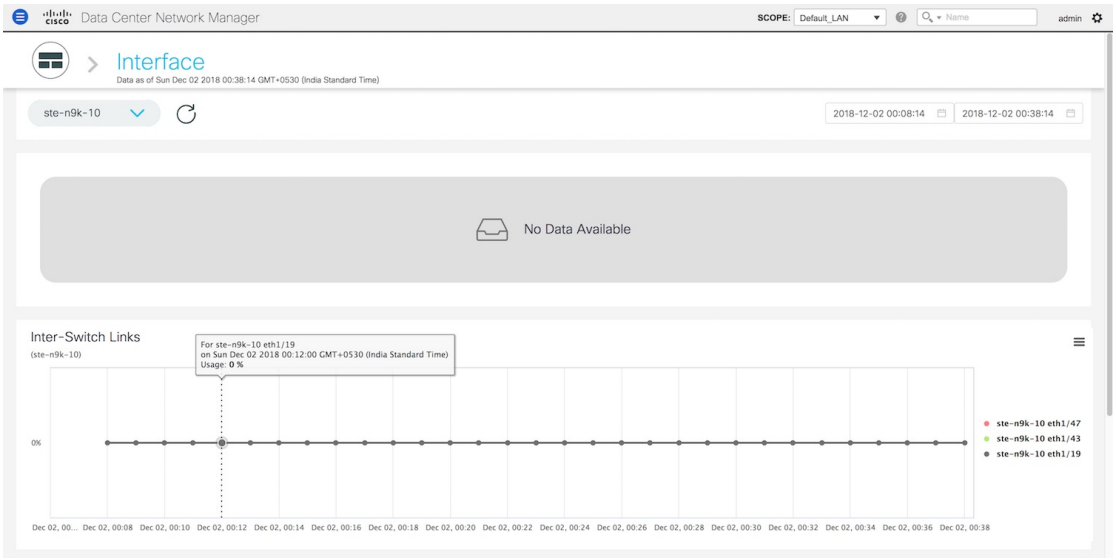
Select **All Switches** to display metrics for all the switches in the selected fabric. This window displays the top five switches based on the number of anomalies, top five ISLs, and the top five host facing links. In the graph displaying the top five switches based on the number of anomalies, each switch has a specific color that is associated with it in the graph. In the graph for the Top 5 Inter-Switch Links and the Top 5 Host Facing links, each switch interface has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches and interfaces on the right of the graphs.



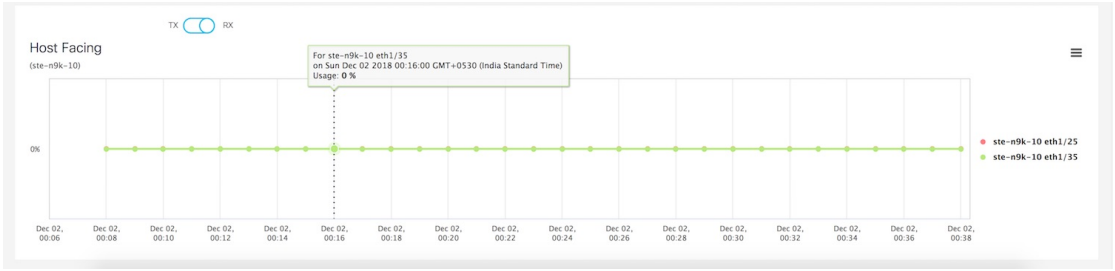
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



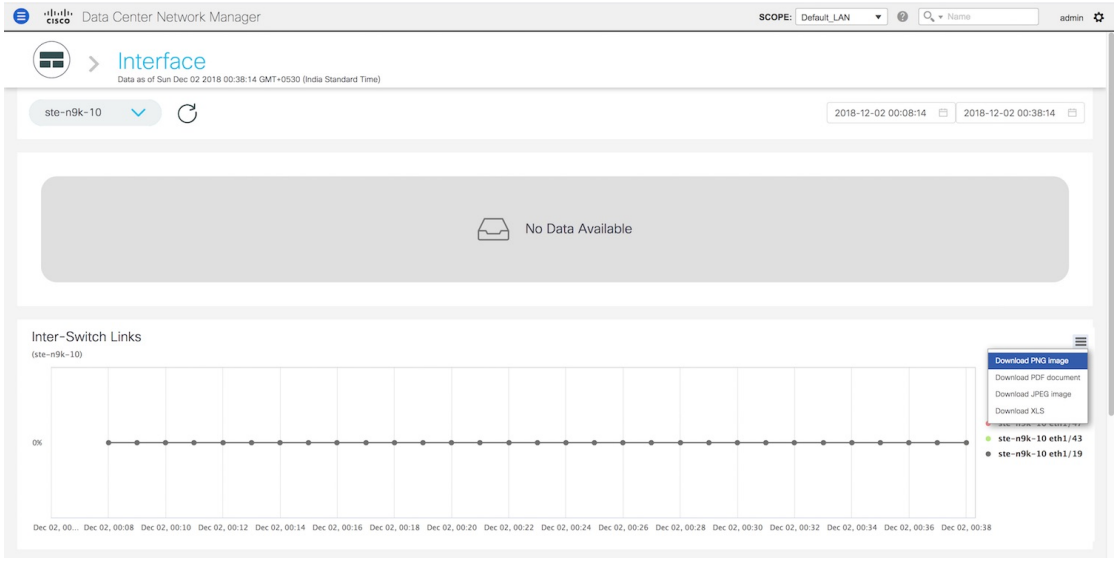
3. Hover over specific points on the respective graphs for more information on the switch anomalies and ISLs at a specific time.



In the graph for Host Facing links, you can toggle between displaying the top five host facing links based on sending traffic (TX) and the top five host facing links based on receiving traffic (RX).



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.

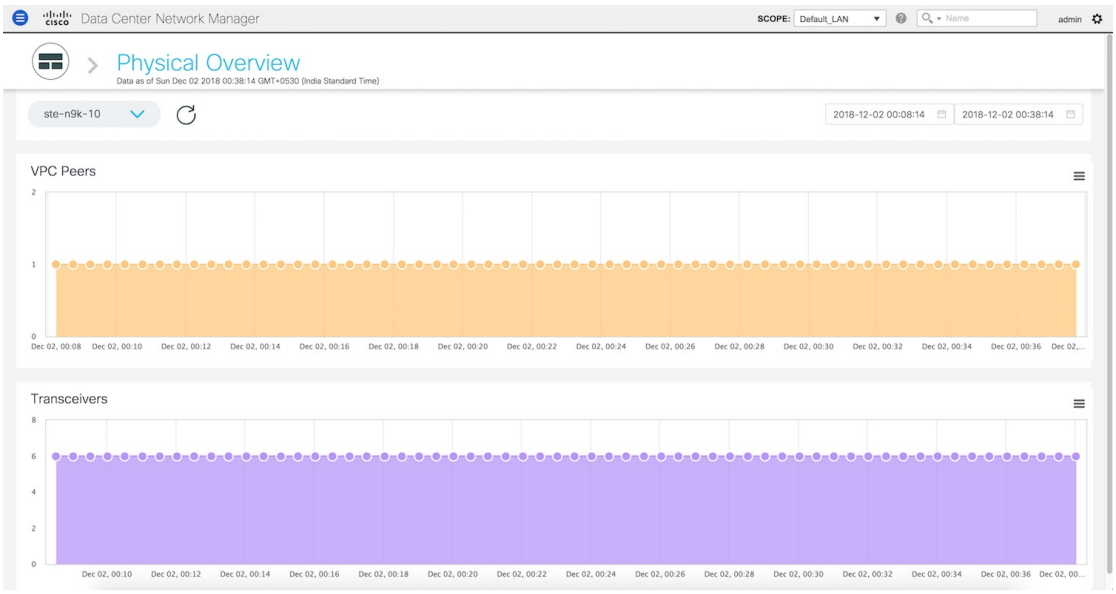


5. Click the icon next to **Interface** at the top of the window to go back to the LAN Telemetry Summary window.

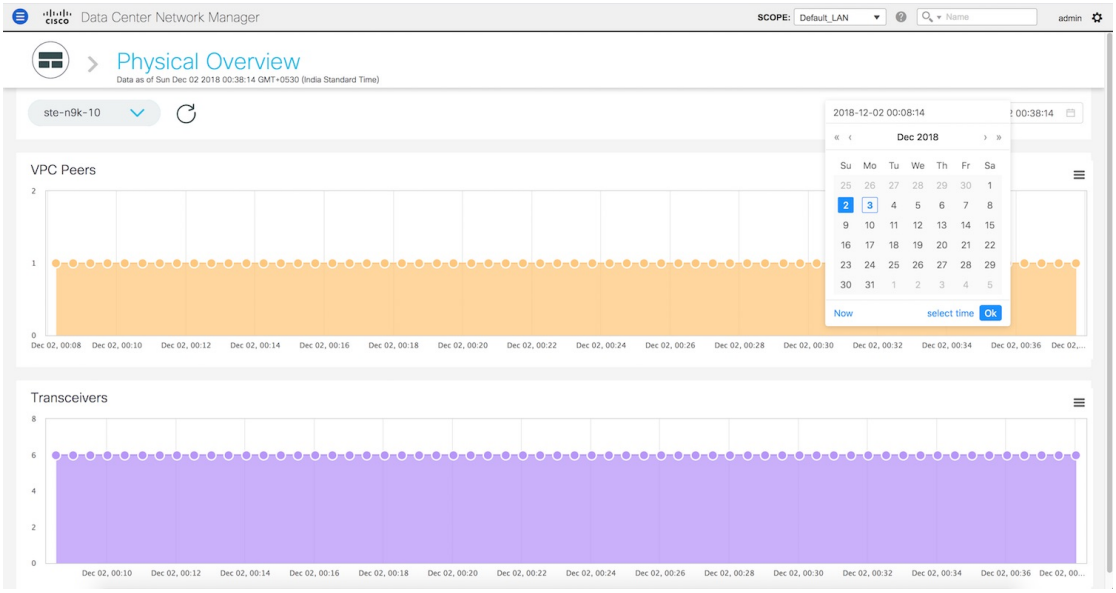
Physical Overview

The **Physical Overview** tile displays the number of switches, Virtual Port Channel (VPC) peers, and Transceivers in the specified fabric.

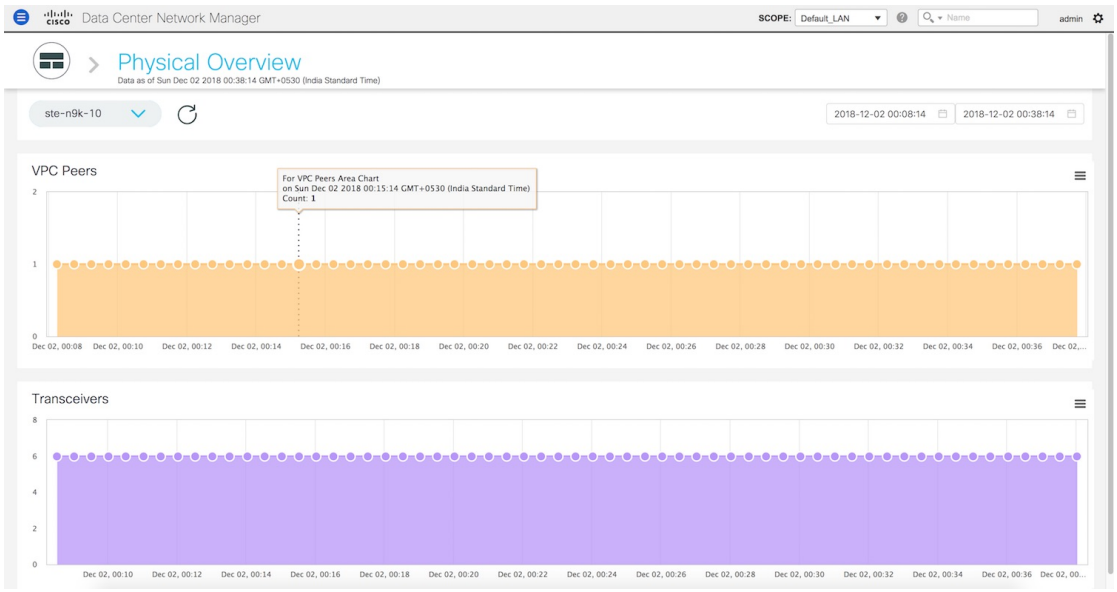
1. Click the **Physical Overview** tile to display more information about the VPC peers and Transceivers. On the **Physical Overview** window, you can select a specific switch from the drop-down list for which you want to display the metrics. You can select **All Switches** to display metrics for all the switches in the selected fabric.



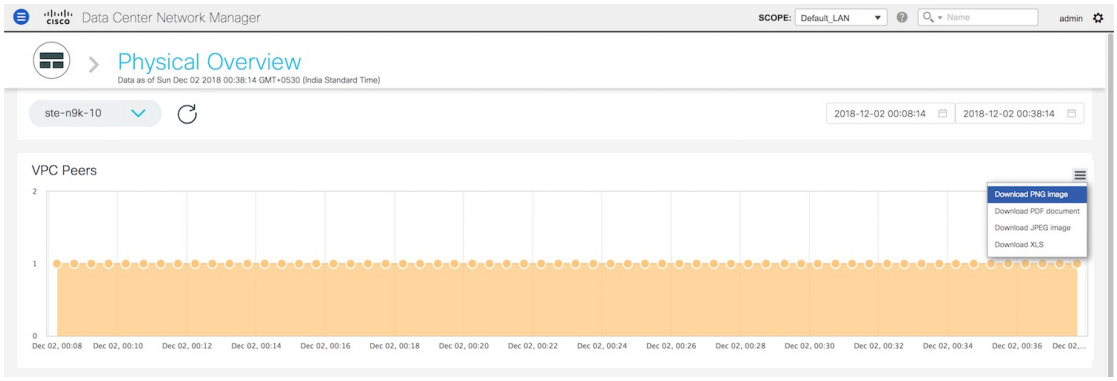
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the respective graphs to display the number of VPC peers and Transceivers that are associated with a switch at a specific time.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



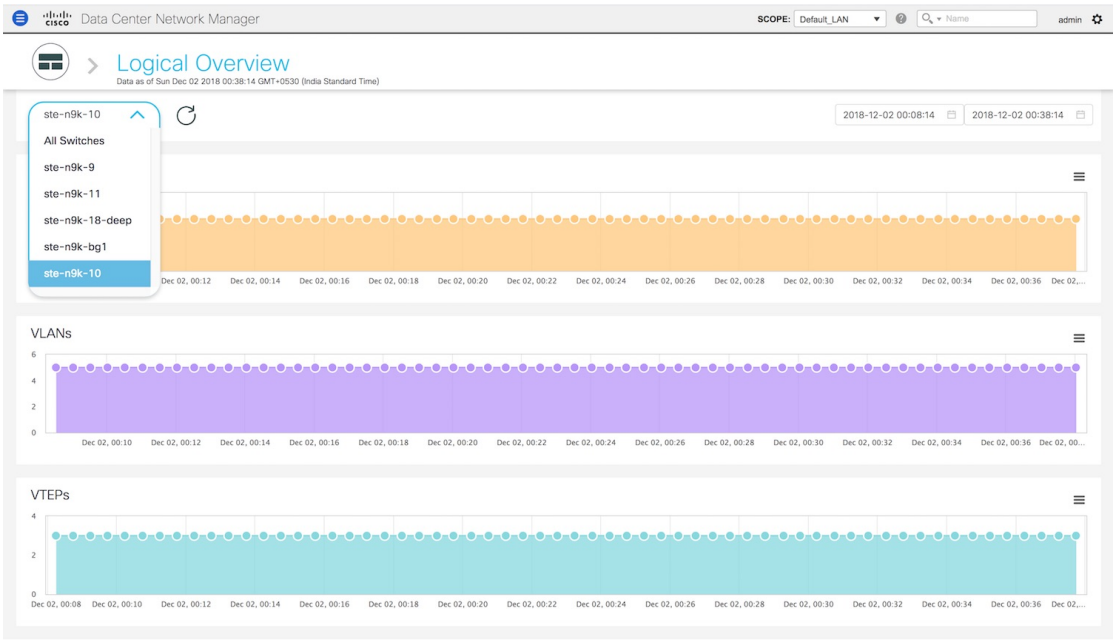
5. Click the icon next to **Physical Overview** at the top of the window to go back to the LAN Telemetry Summary window.

Logical Overview

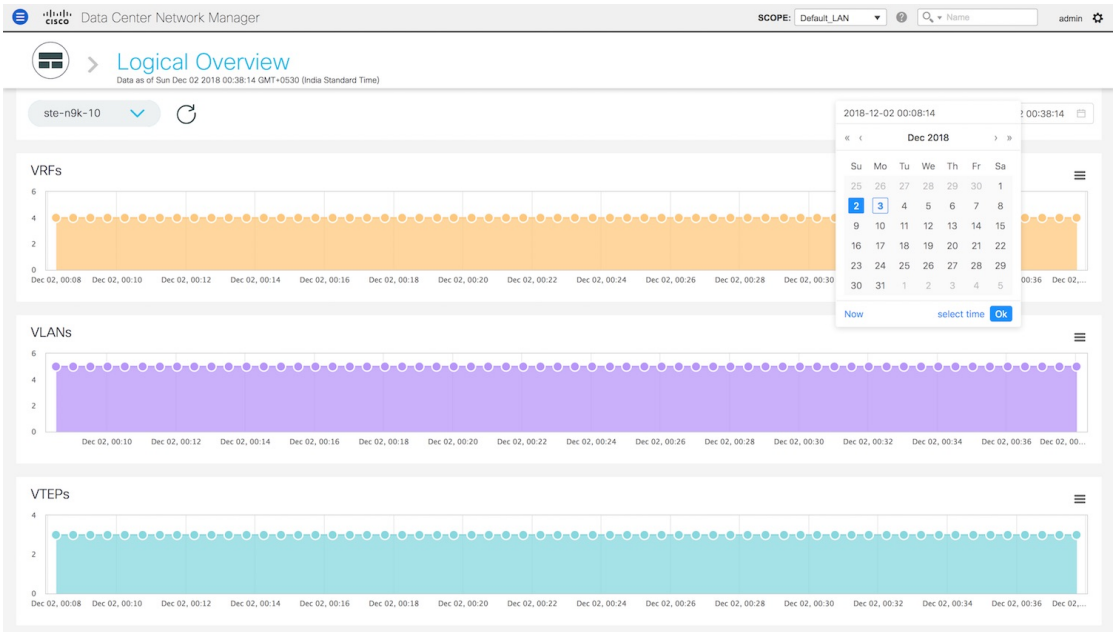
The **Logical Overview** tile displays the number of Virtual Routing and Forwarding instances (VRFs), VLANs, and VXLAN Tunnel Endpoints (VTEPs) in the specified fabric.

1. Click the **Logical Overview** tile to display more information about the VRFs, VLANs, and VTEPs. On the **Logical Overview** window, you can select a specific switch from the drop-down list for which you

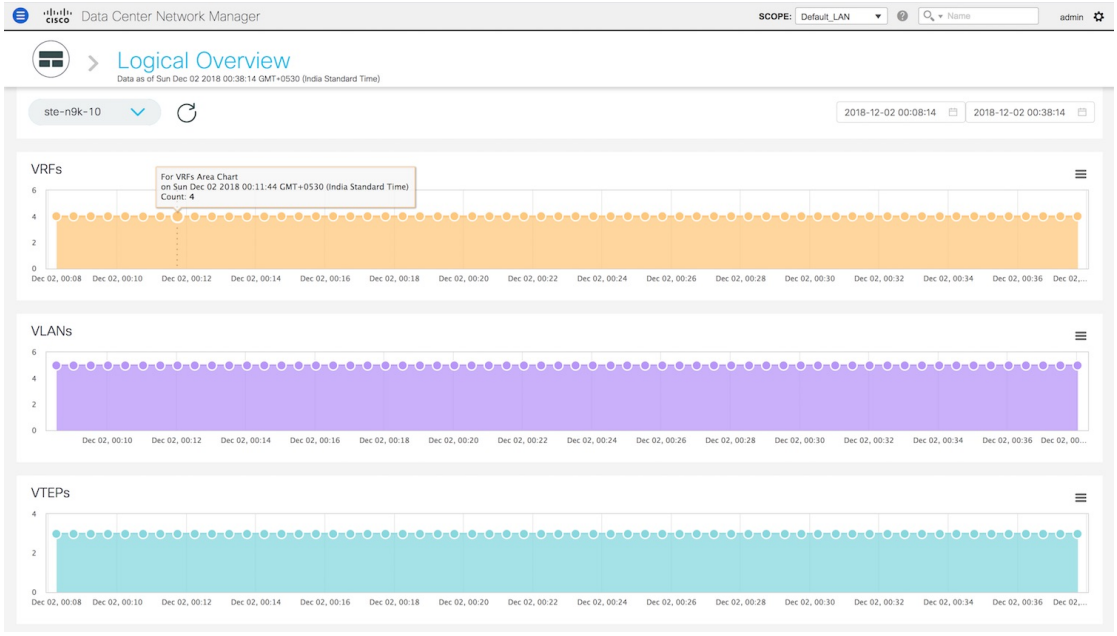
want to display the metrics. You can select **All Switches** to display metrics for all the switches in the selected fabric.



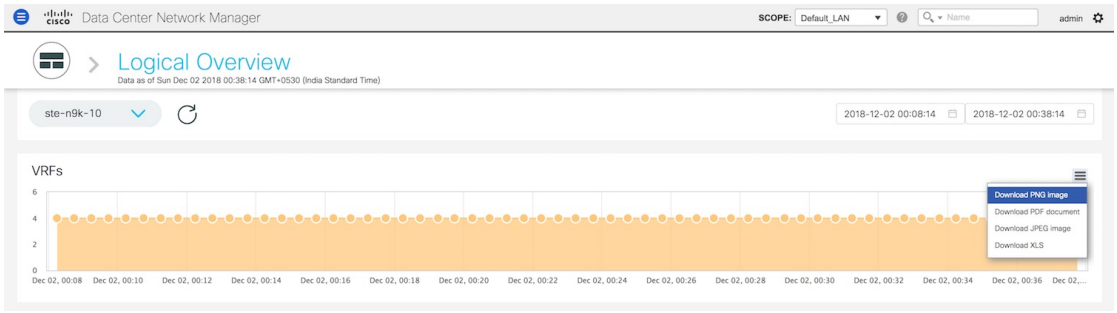
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the respective graphs to display the number of VRFs, VLANs, and VTEPs associated with a switch at a specific time.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.

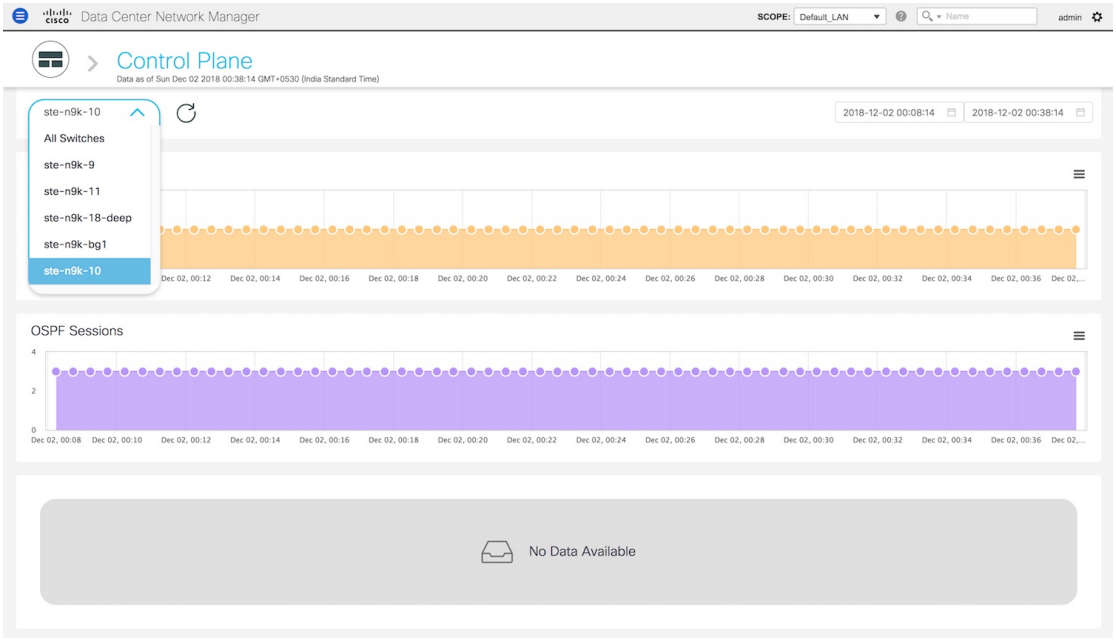


5. Click the icon next to **Logical Overview** at the top of the window to go back to the LAN Telemetry Summary window.

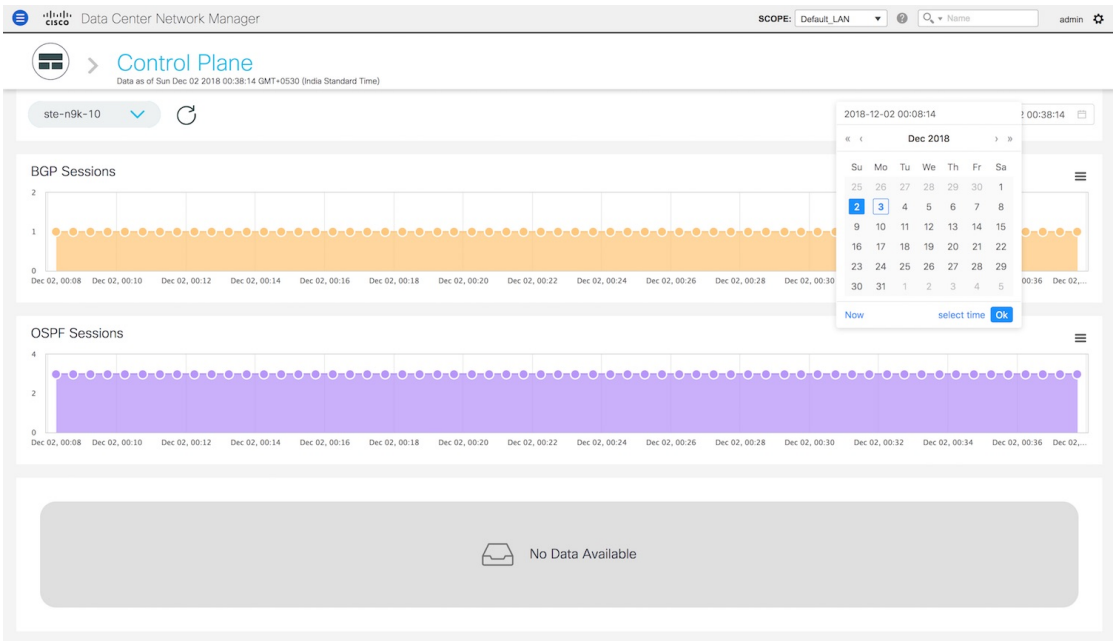
Control Plane

The **Control Plane** tile displays the number of Border Gateway Protocol (BGP) sessions, Open Shortest Path First (OSPF) sessions, and Intermediate System-to-Intermediate System (IS-IS) sessions in the specified fabric.

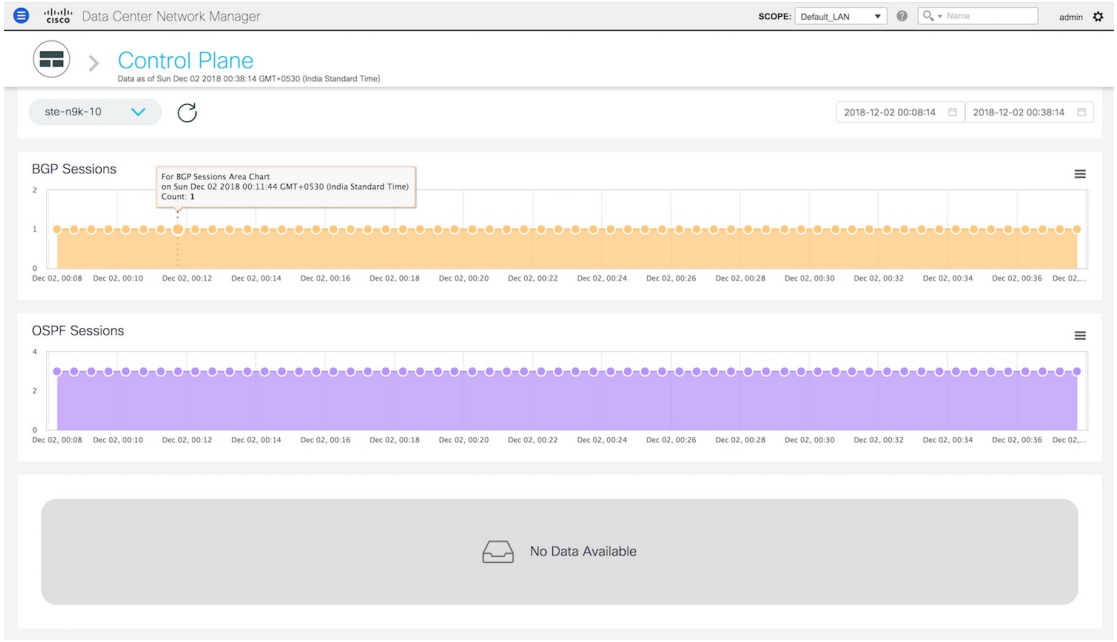
1. Click the **Control Plane** tile to display more information about the BGP sessions, OSPF sessions, and IS-IS sessions. On the **Control Plane** window, you can select a specific switch from the drop-down list for which you want to display the metrics. You can select **All Switches** to display metrics for all the switches in the selected fabric.



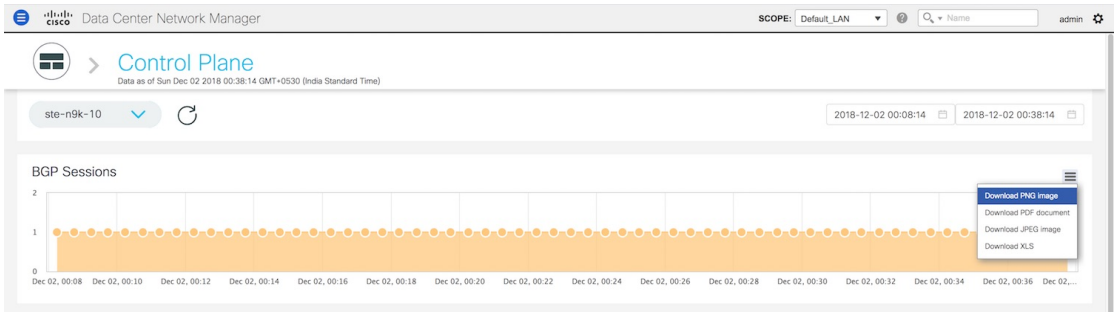
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the respective graphs to display the number of BGP sessions, OSPF sessions, and IS-IS sessions associated with a switch at a specific time.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



5. Click the icon next to **Control Plane** at the top of the window to go back to the LAN Telemetry Summary window.

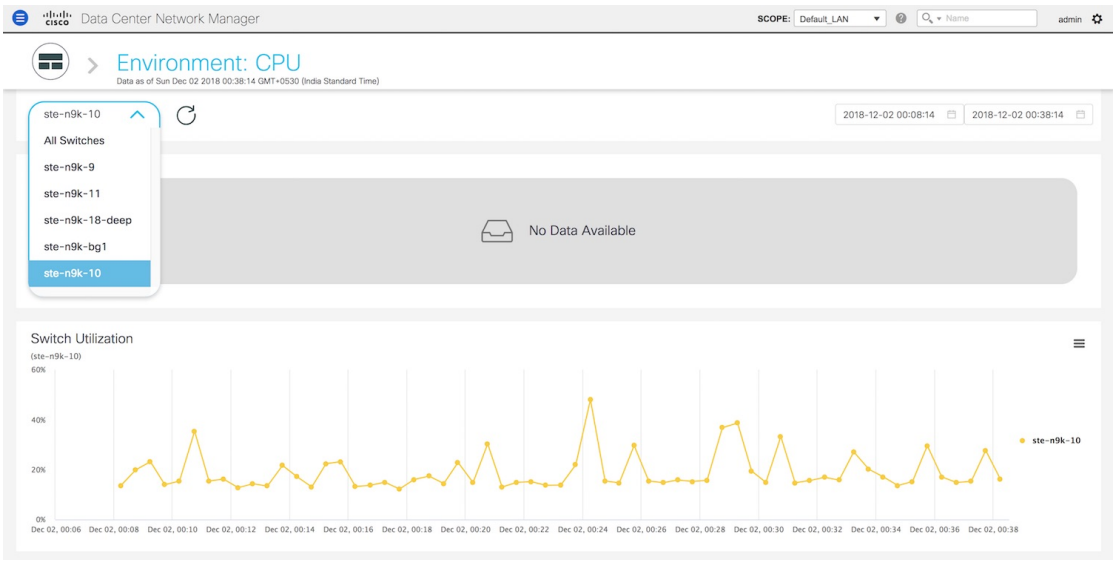
Environment

The **Environment** tile displays metrics for CPU usage, Memory, Temperature, Power, and Fans. On the top right of the **Environment** tile, you can select the Top N switches from the dropdown to display metrics for the top N switches. For example, if **Top 5** is selected, donut charts are plotted for the top five switches based on specific metrics.

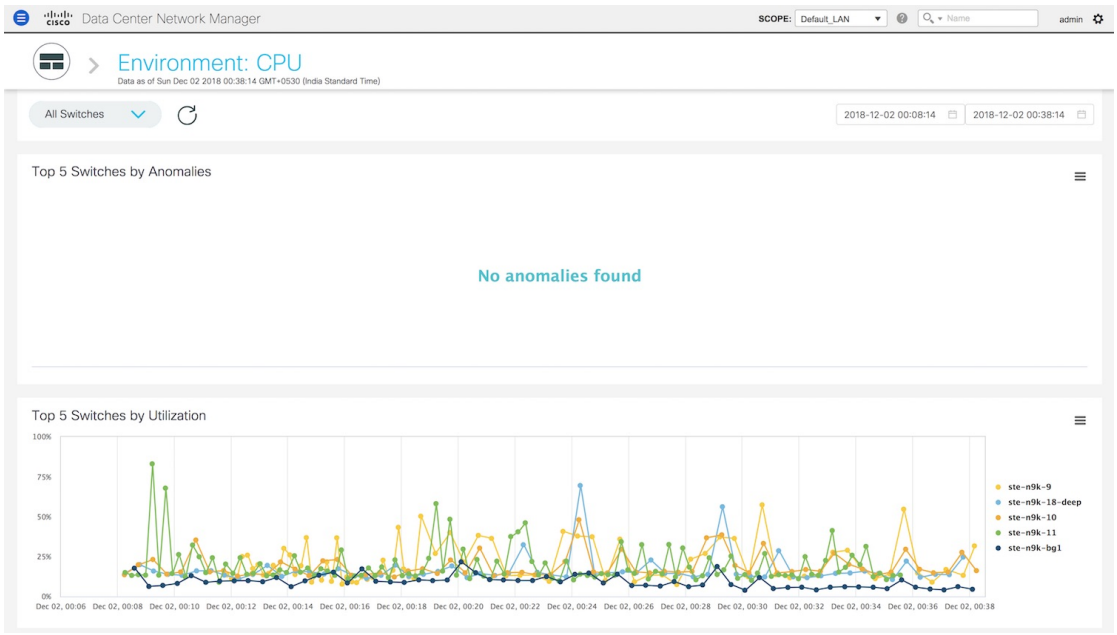
Environment - CPU

The first donut chart shows the proportion of top five or top ten switches based on CPU usage values. When hovered, it shows the switch name and the corresponding metric value.

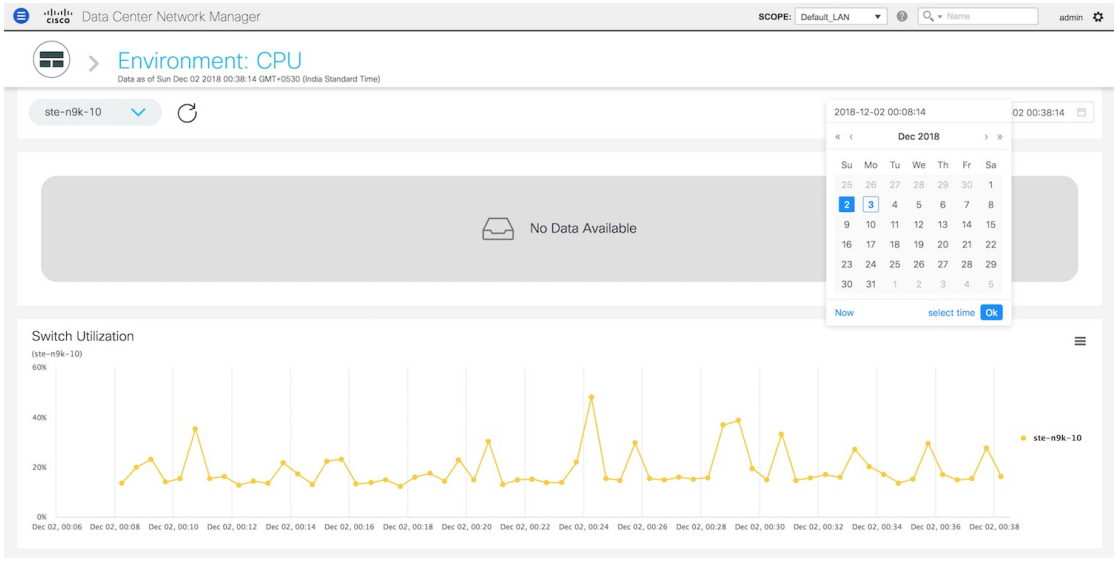
1. Click the CPU usage donut to display more information about CPU usage. On the **Environment: CPU** window, you can select a specific switch from the drop-down list for which you want to display the metrics.



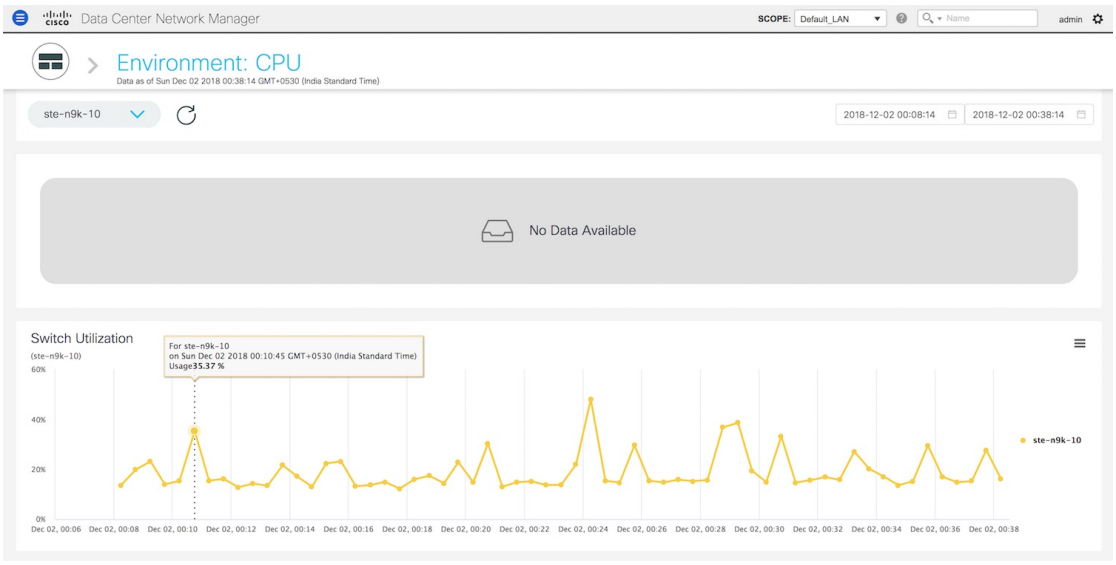
You can select **All Switches** to display metrics for all the switches in the selected fabric. This window displays the top five switches based on the number of anomalies and top five switches based on CPU utilization. Each switch has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches on the right of the graph.



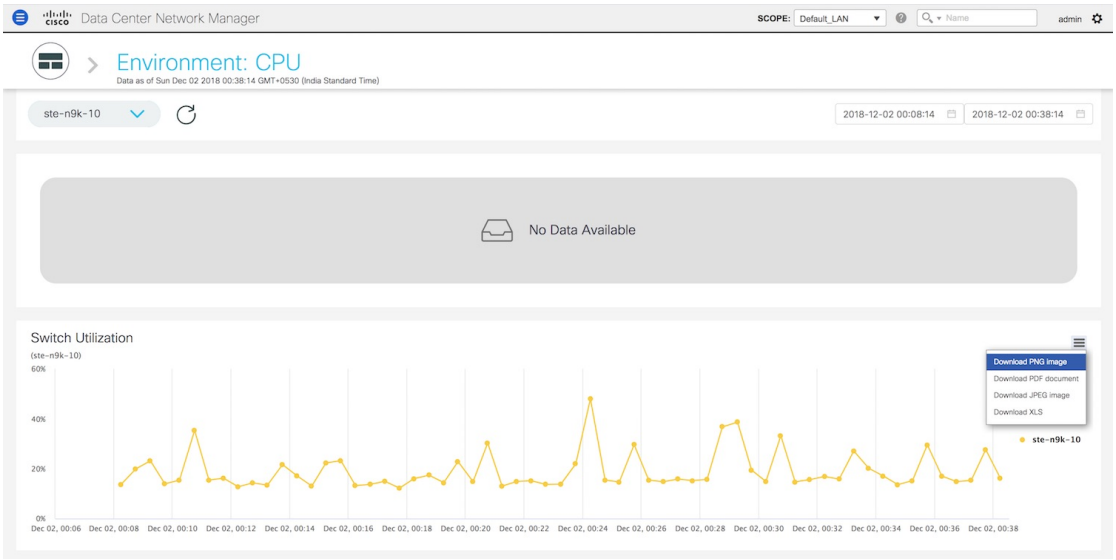
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the graph for more information on CPU utilization at a specific time.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.

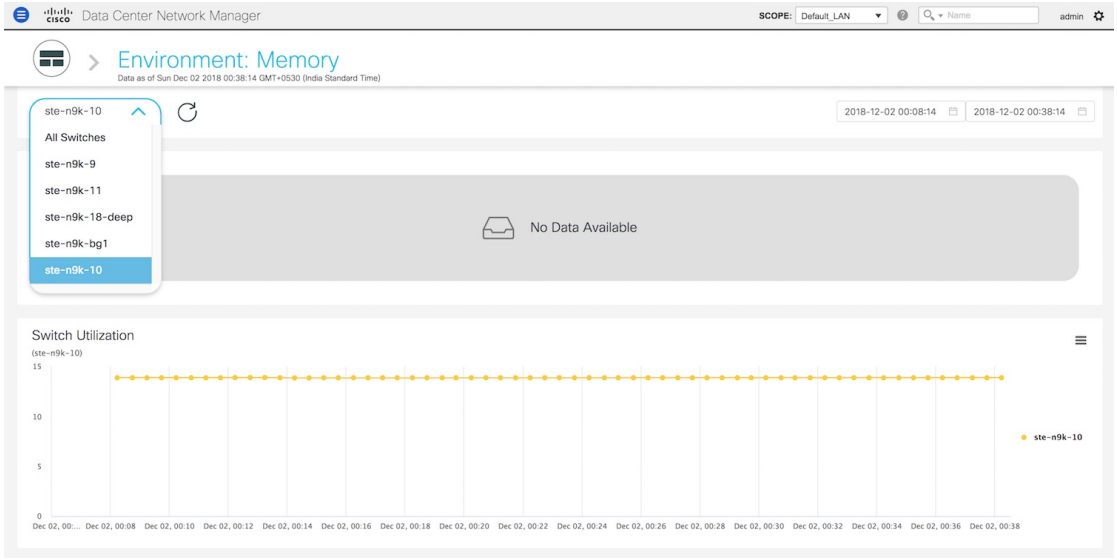


5. Click the icon next to **Environment: CPU** at the top of the window to go back to the LAN Telemetry Summary window.

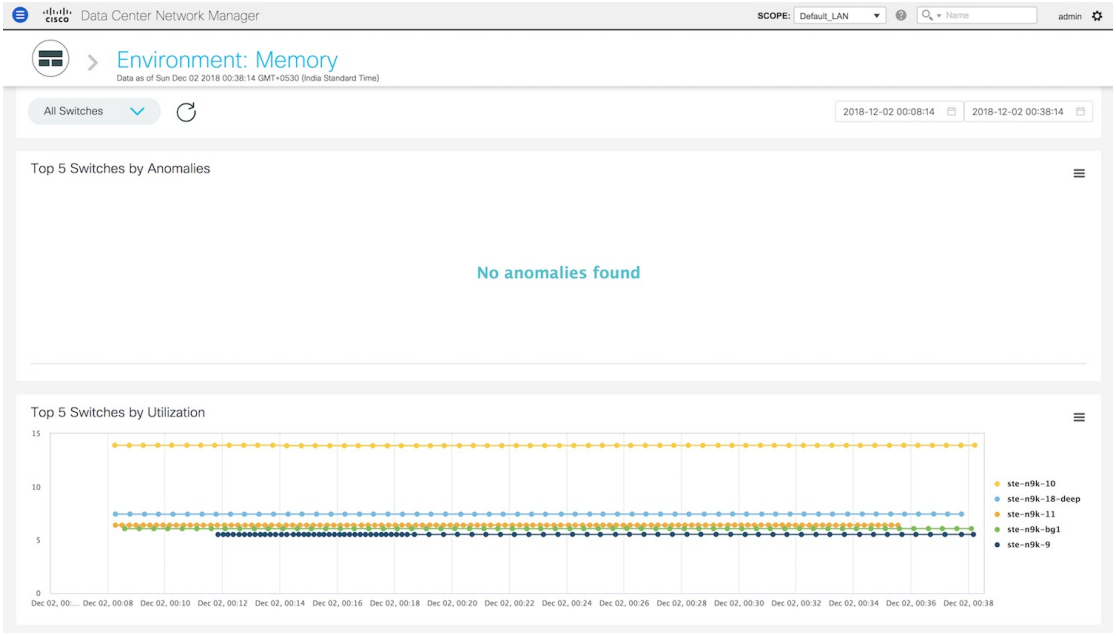
Environment - Memory

The second donut chart shows the proportion of top five or top ten switches based on memory usage values. When hovered, it shows the switch name and the corresponding metric value.

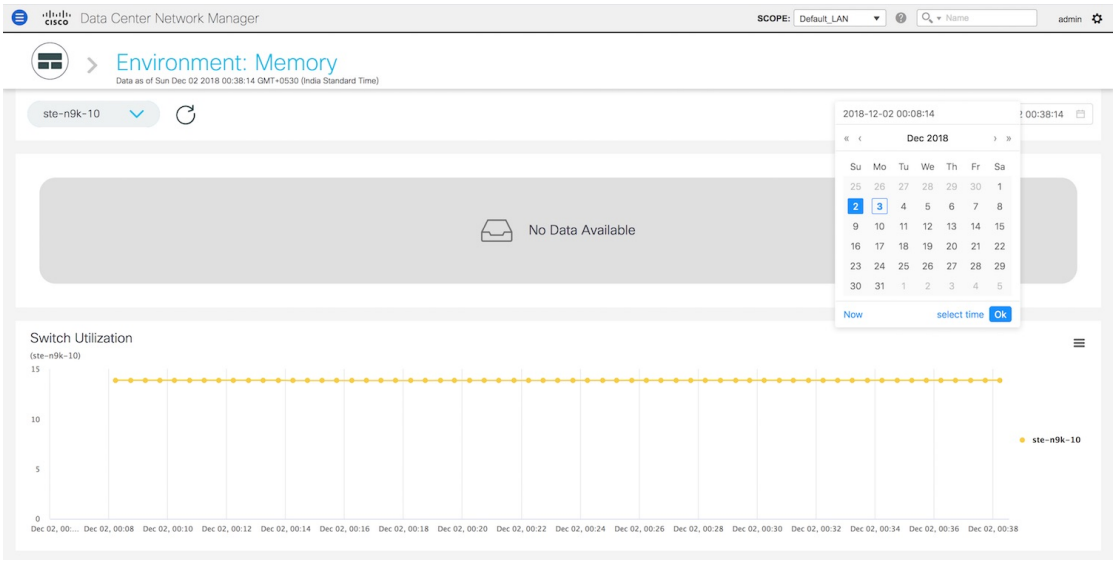
1. Click the memory usage donut to display more information about memory usage. The memory dashboard depicts the actual memory consumption (RAM) on every switch in Gigabytes (GB). On the **Environment: Memory** window, you can select a specific switch from the drop-down list for which you want to display the metrics.



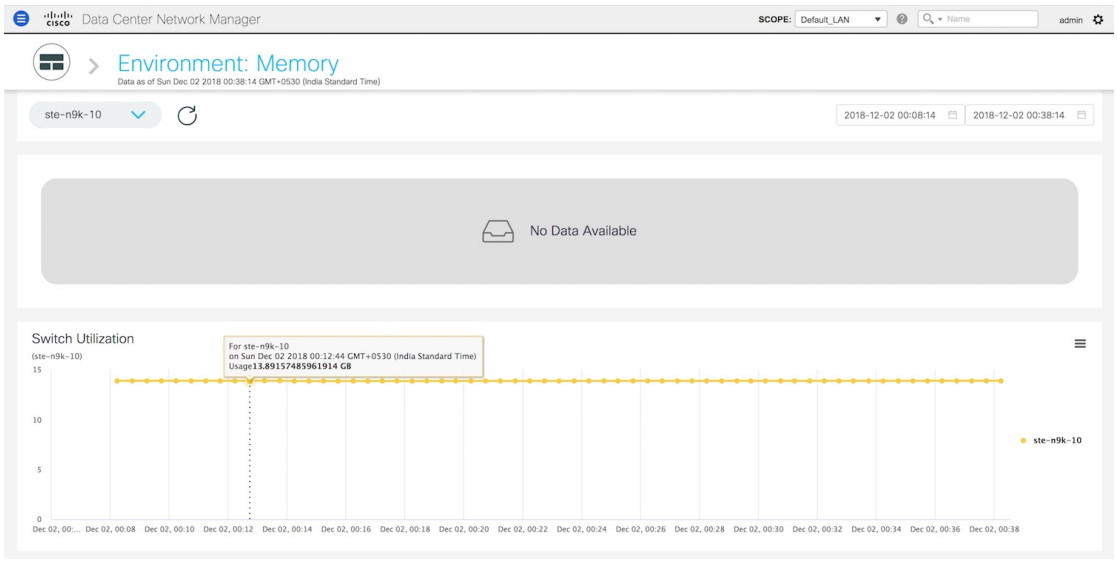
You can select **All Switches** to display metrics for all the switches in the selected fabric. This window displays the top five switches based on the number of anomalies and top five switches based on memory utilization. Each switch has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches on the right of the graph.



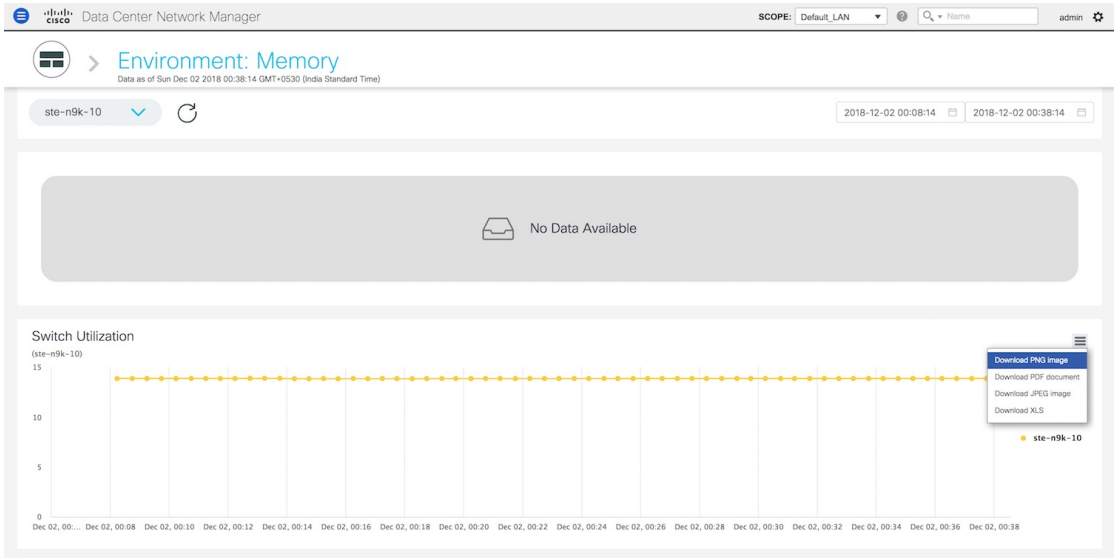
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the respective graphs for more information on memory utilization at a specific time.



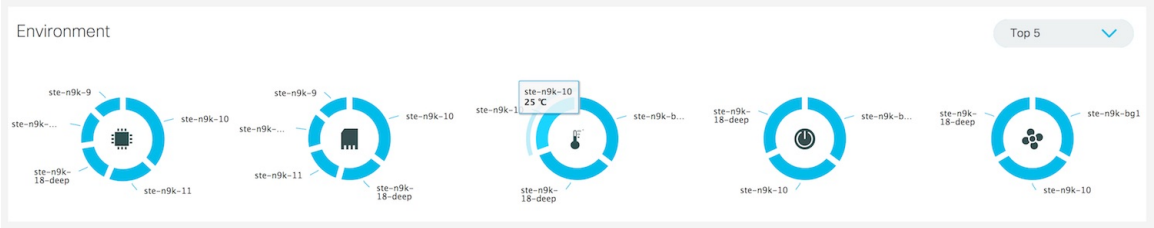
4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



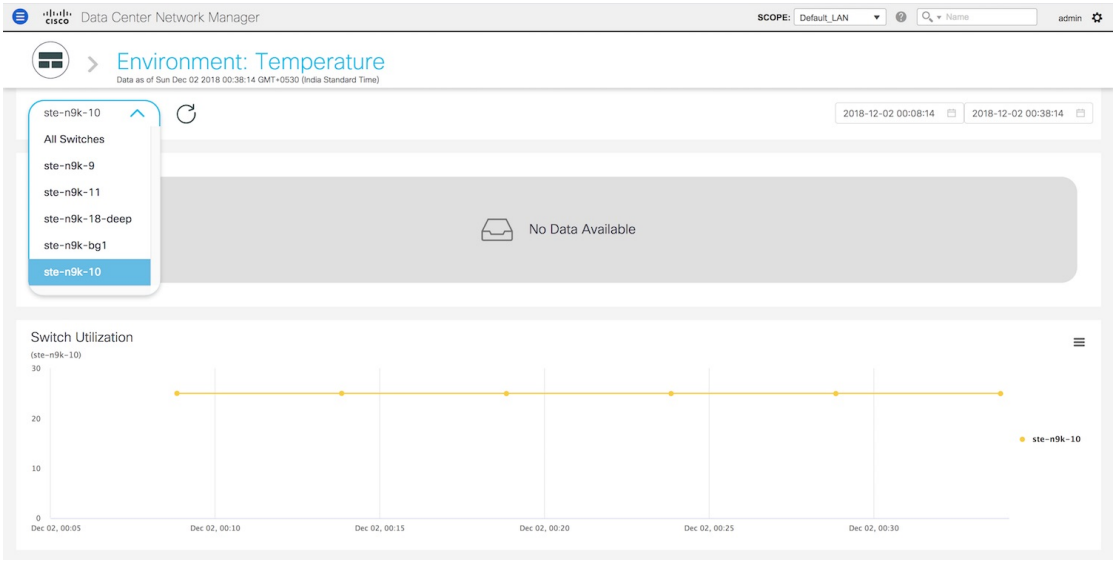
5. Click the icon next to **Environment: Memory** at the top of the window to go back to the LAN Telemetry Summary window.

Environment - Temperature

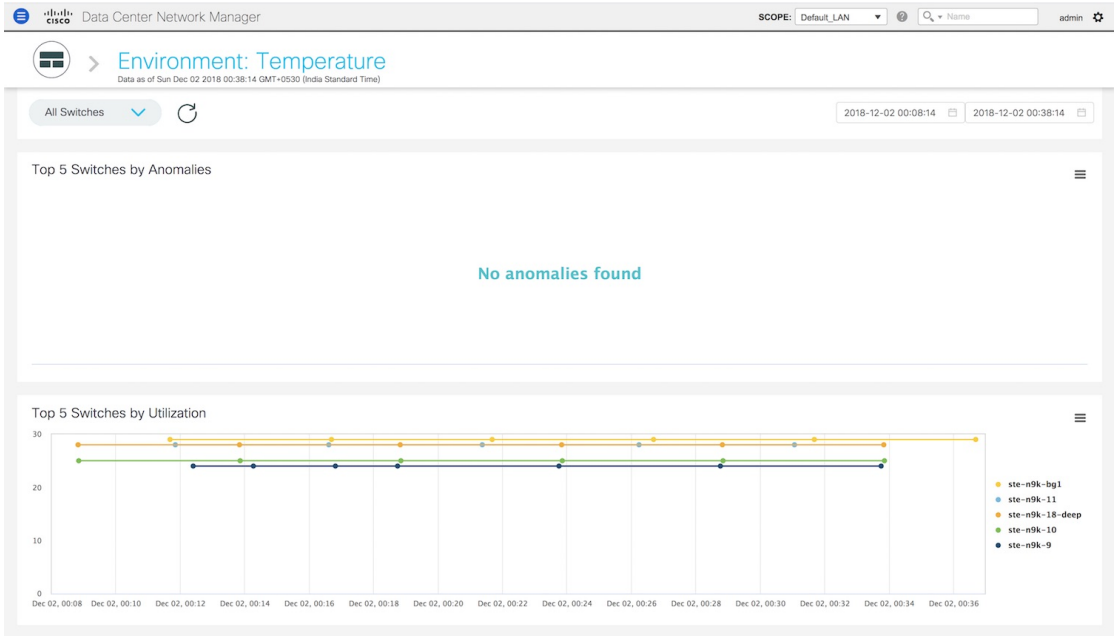
The third donut chart shows the proportion of top five or top ten switches based on temperature levels. When hovered, it shows the switch name and the corresponding metric value.



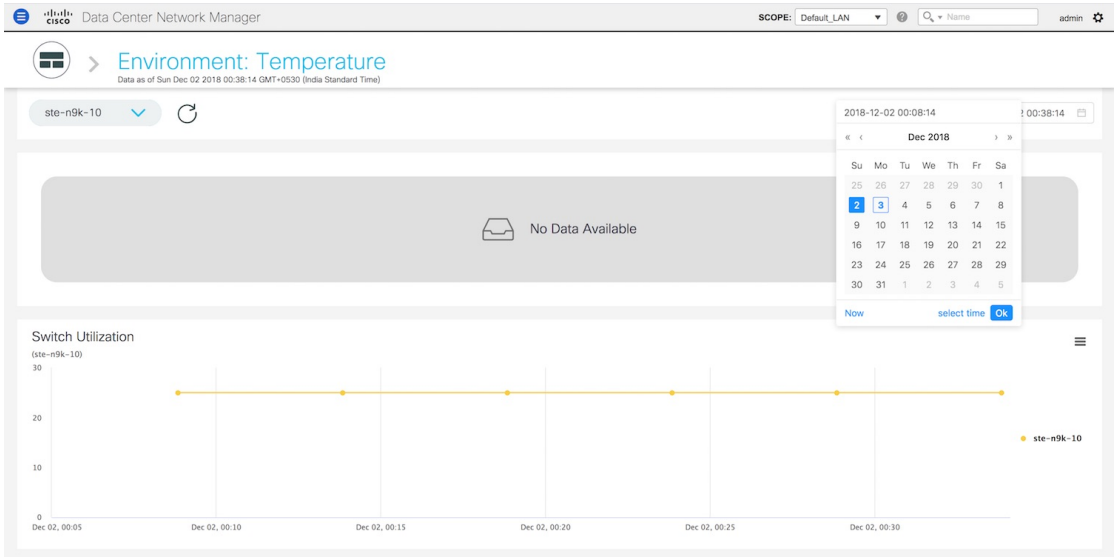
1. Click the temperature levels donut to display more information about temperature levels for the switches in the fabric. On the **Environment: Temperature** window, you can select a specific switch from the drop-down list for which you want to display the metrics.



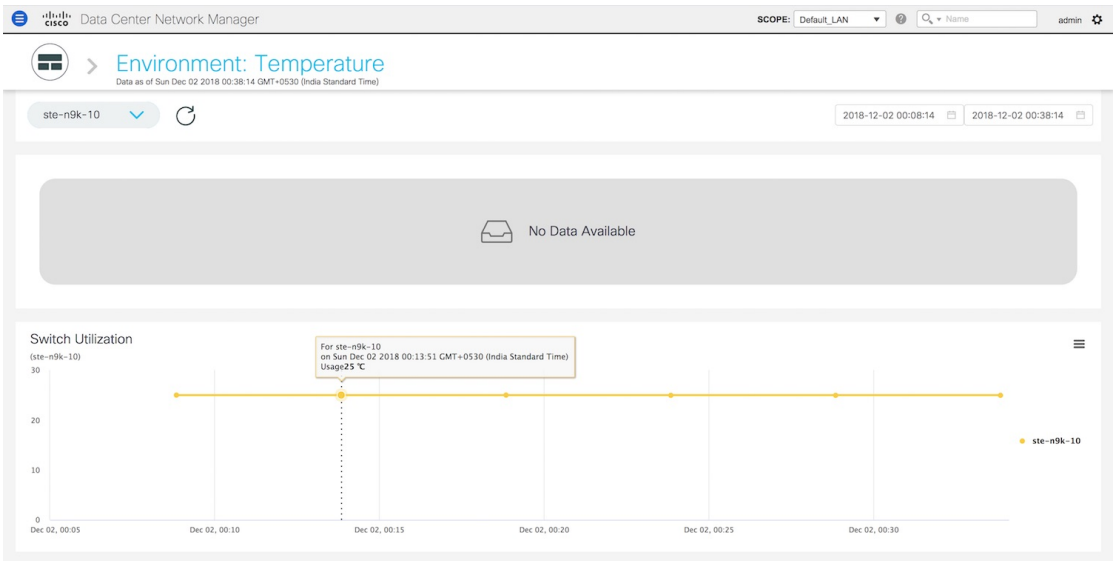
You can select **All Switches** to display metrics for all the switches in the selected fabric. This window displays the top five switches based on the number of anomalies and top five switches based on temperature. Each switch has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches on the right of the graph.



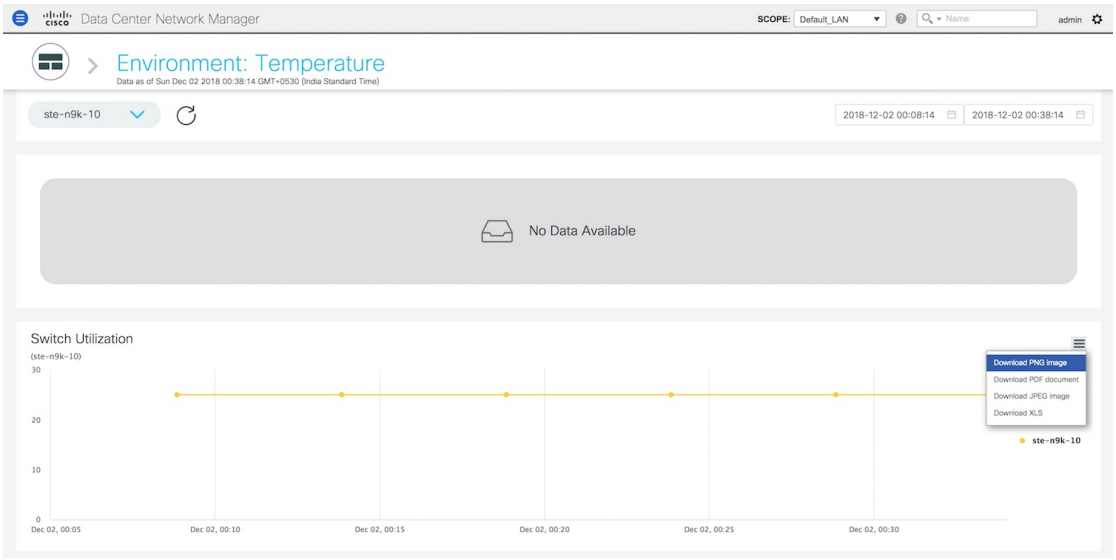
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the graph for more information on the temperature of the selected switch at a specific time.



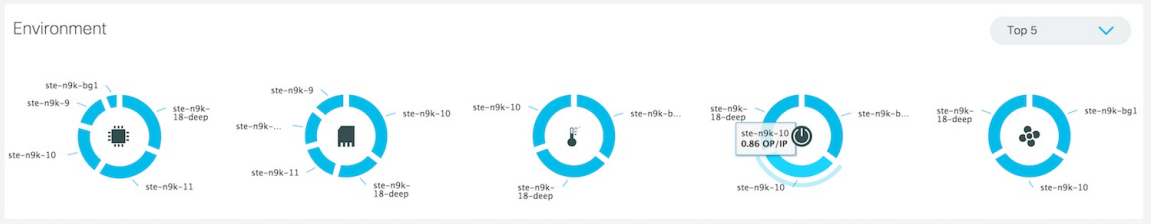
4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



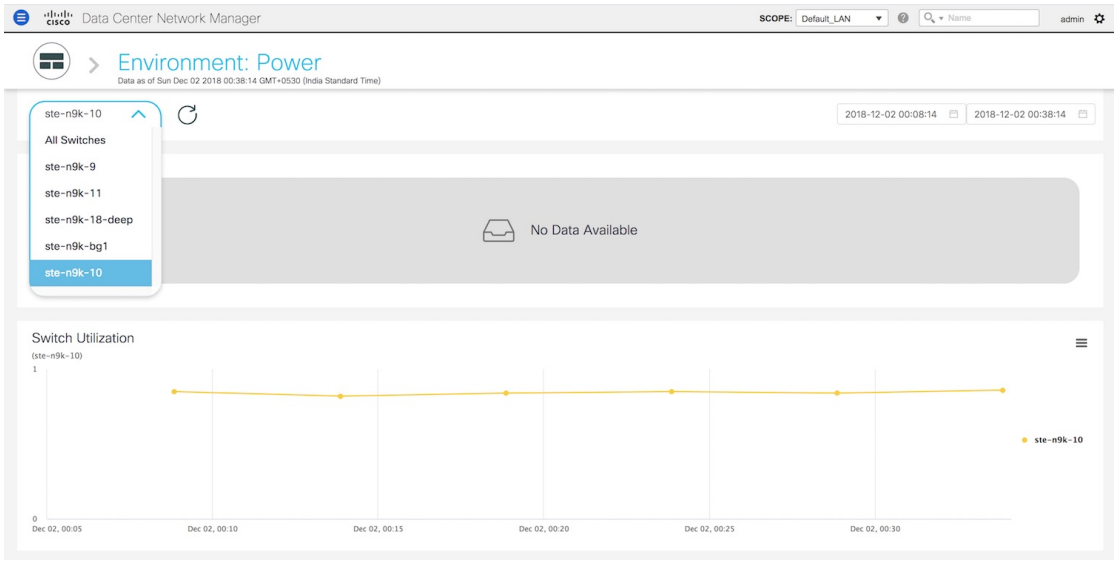
5. Click the icon next to **Environment: Temperature** at the top of the window to go back to the LAN Telemetry Summary window.

Environment - Power

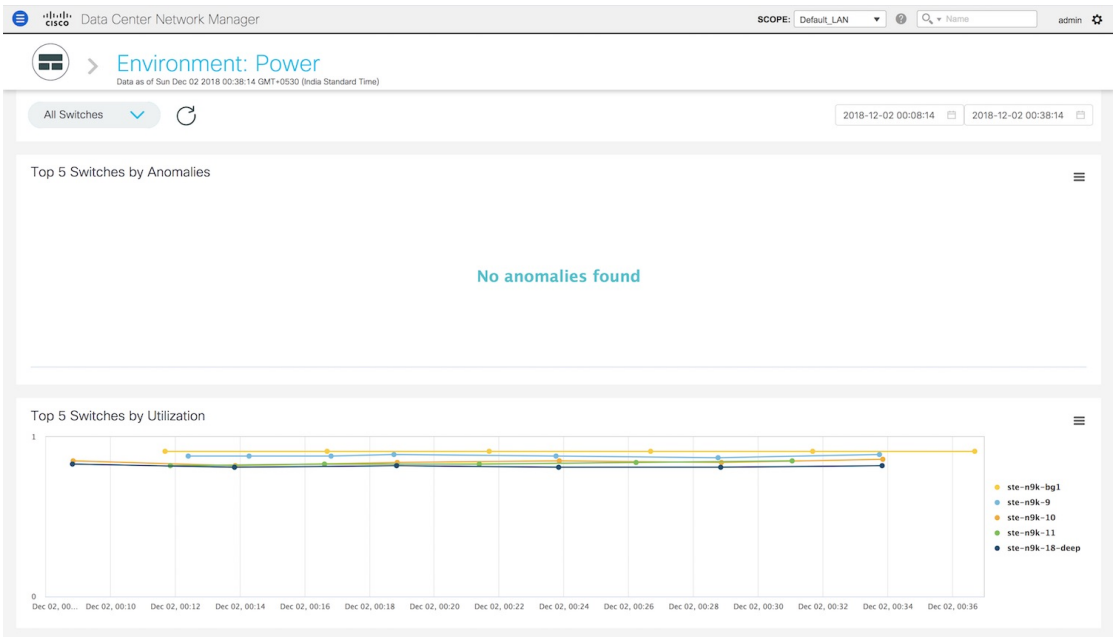
The fourth donut chart shows the proportion of top five or top ten switches based on the power usage or efficiency of the power supplies. When hovered, it shows the switch name and the corresponding metric value.



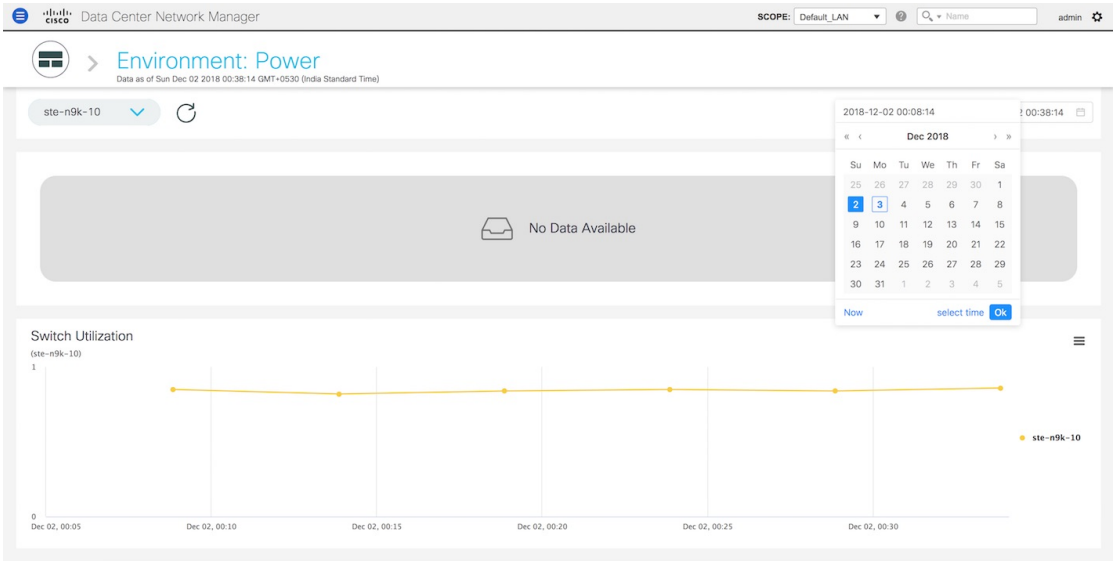
1. Click the Power donut to display more information about the power efficiency metrics for the switches in the fabric. On the **Environment: Power** window, you can select a specific switch from the drop-down list for which you want to display the metrics.



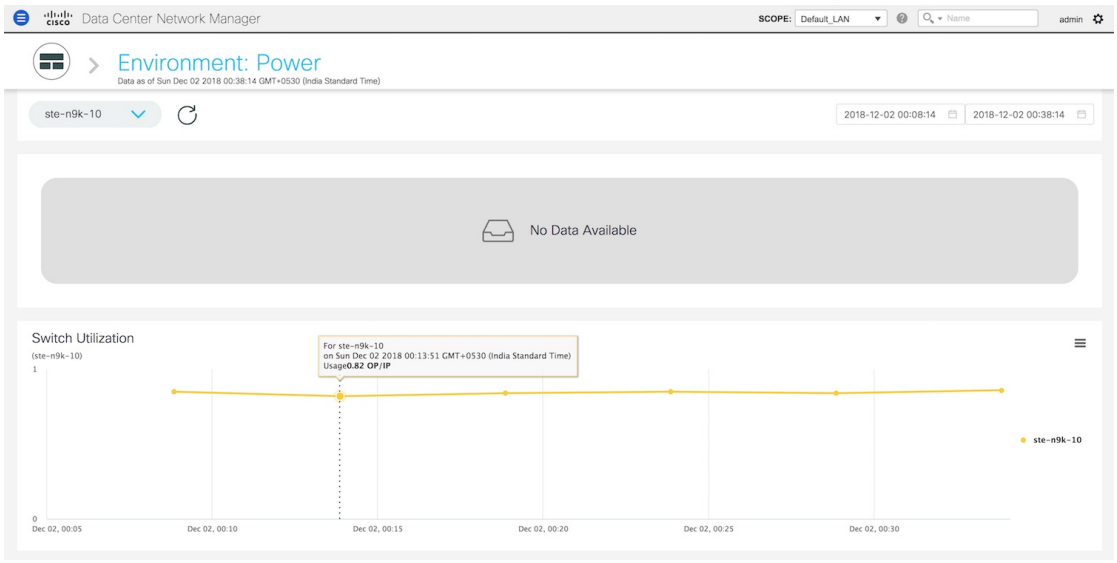
You can select **All Switches** to display metrics for the top five switches based on anomalies and the top five switches based on power usage or efficiency. By definition, efficiency is Output-Power/Input-Power, which therefore results in a maximum efficiency of 1.0. Each switch has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches on the right of the graph.



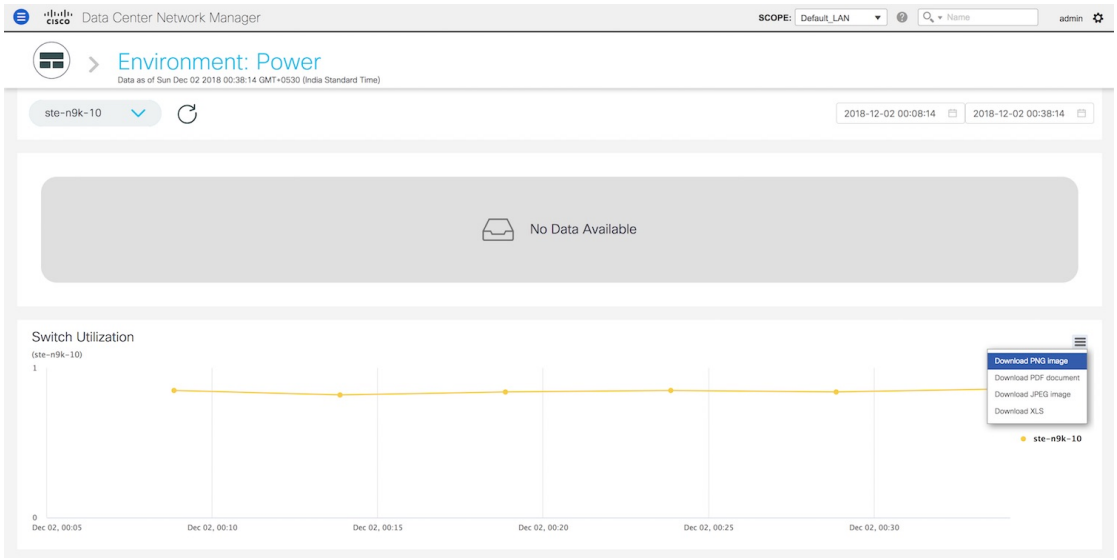
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the graph for more information on the power efficiency or usage at a specific time.



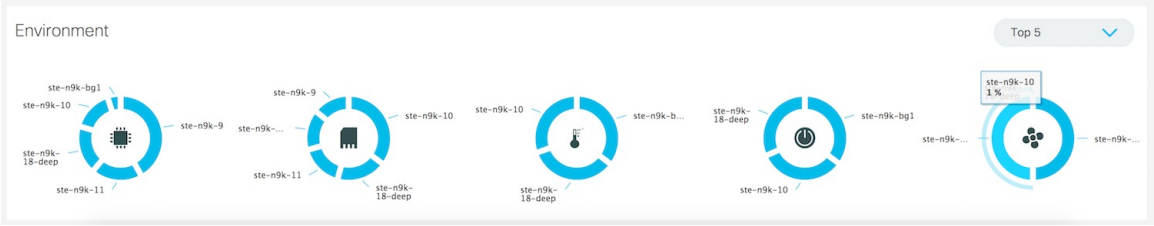
4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



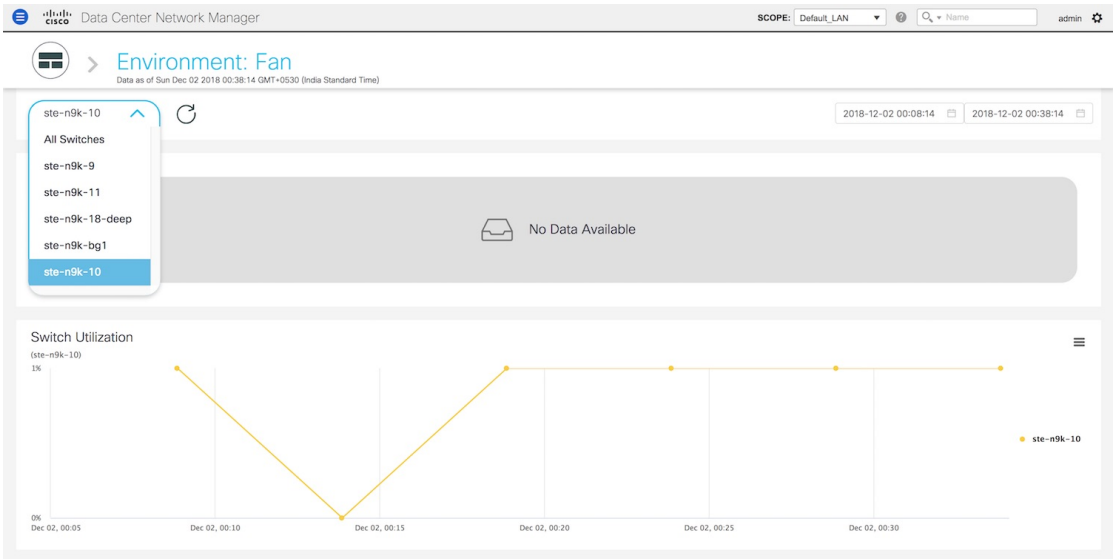
5. Click the icon next to **Environment: Power** at the top of the window to go back to the LAN Telemetry Summary window.

Environment - Fan

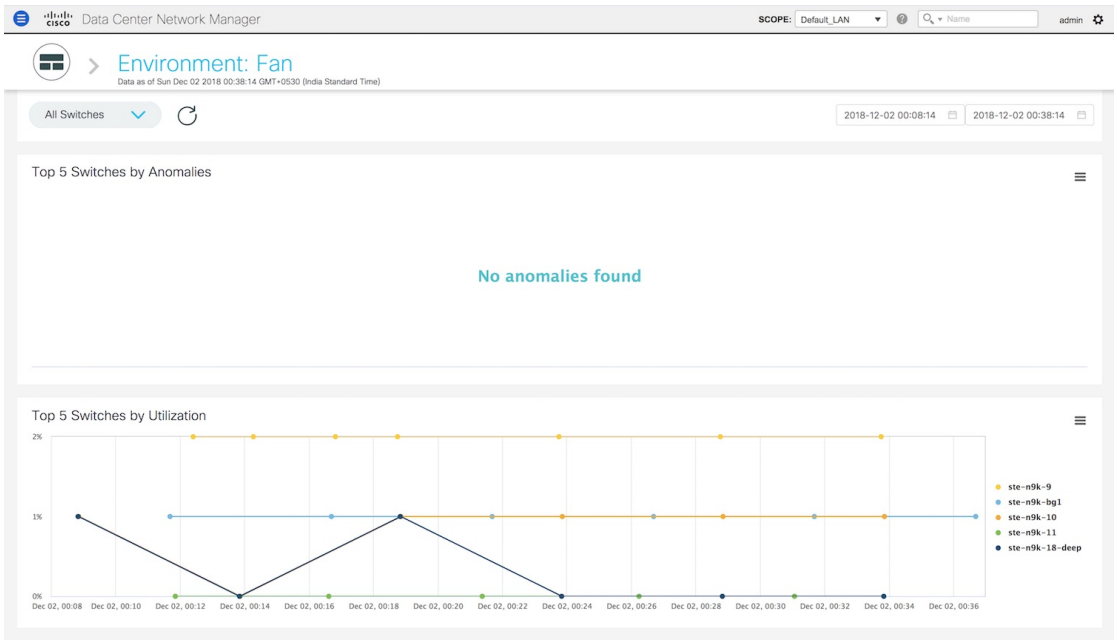
The fifth donut chart shows the proportion of top five or top ten switches based on fan utilization. When hovered, it shows the switch name and the corresponding metric value.



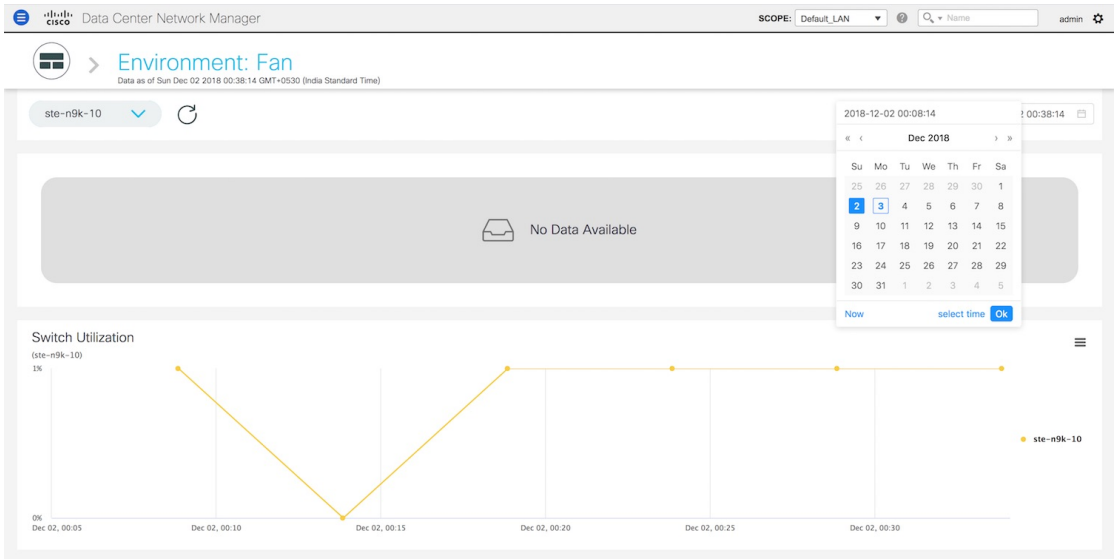
1. Click the Fan donut to display more information about the fan utilization. On the **Environment: Fan** window, you can select a specific switch from the drop-down list for which you want to display the metrics.



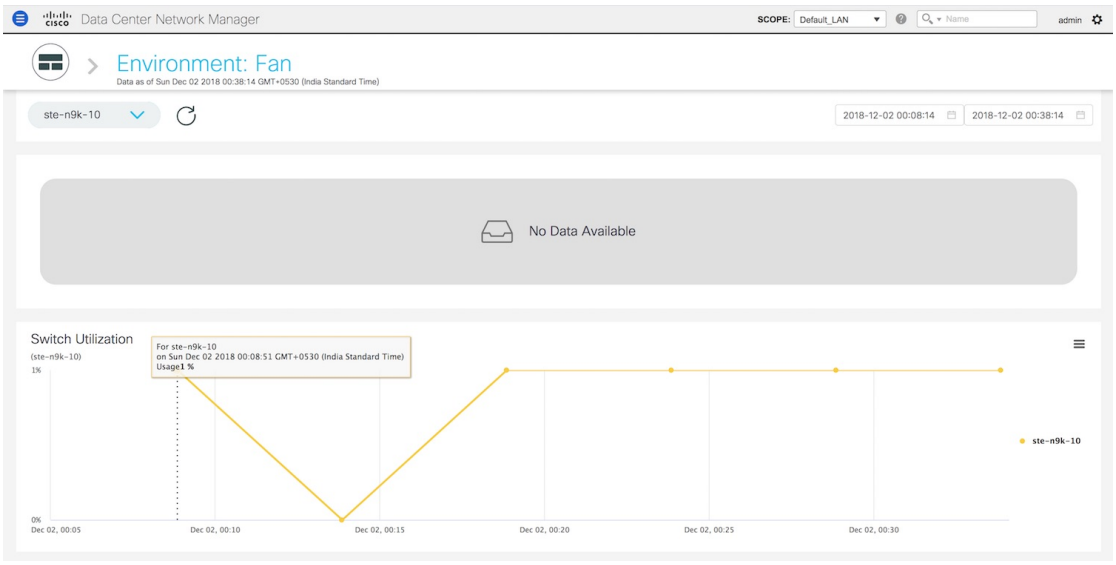
You can select **All Switches** to display metrics for the top five switches based on the number of anomalies and the top five switches based on fan utilization. Each switch has a specific color that is associated with it in the graph. You can see the colors that are associated with the switches on the right of the graph.



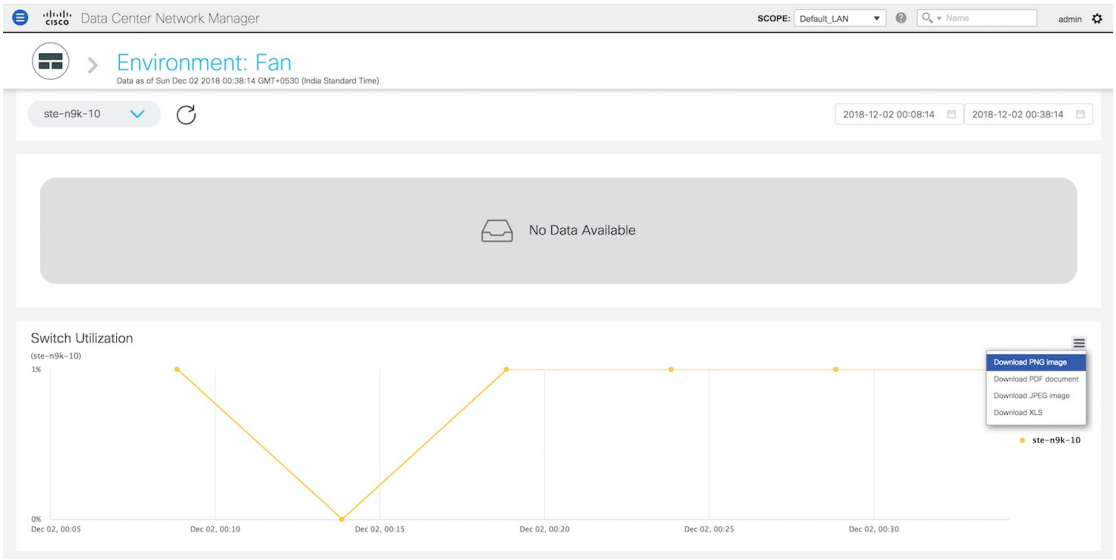
2. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. Click **Now** to display metrics for the current date and time. Click the **Refresh** icon next to the switch selection dropdown to display metrics for the last 30 minutes.



3. Hover over specific points on the respective graphs for more info on fan utilization at a specific time.



4. Click the icon at the top right of the graph to download the graph as a PNG image, PDF document, JPEG image or an XLS file.



5. Click the icon next to **Environment: Fan** at the top of the window to go back to the LAN Telemetry Summary window.

Alarms

The Alarms menu includes the following submenus:

Viewing Alarms and Events

You can view the alarms, cleared alarms, and events.

Procedure

Step 1 Choose **Monitor > Alarms > View**.

Step 2 Choose any of the following tabs.

- **Alarms**: This tab displays the alarms that are generated for various categories. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Last Updated (optional), Policy, and Message. You can specify the **Refresh Interval** in this tab. You can select one or more alarms and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them.
- **Cleared Alarms**: This tab displays the cleared alarms. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Cleared At (optional), Cleared By, Policy, and Message. You can select one or more alarms and then click the **Delete** button to delete them.
- **Events**: This tab displays the events that are generated for the switches. This tab displays information such as **Ack**, **Acknowledged user**, **Group**, **Switch**, **Severity**, **Facility**, **Type**, **Count**, **Last Seen**, and **Description**. You can select one or more events and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them. If you want to delete all events, click the **Delete All** button.

Monitoring and Adding Alarm Policies

You can add alarm policies for the following:

- **Device Health**: Device health policies enable you to create alarms when Device ICMP Unreachable, Device SNMP Unreachable, or Device SSH Unreachable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
- **Interface Health**: Interface health policies enable you to monitor Up or Down, Packet Discard, Error, Bandwidth details of the interfaces. By default all interfaces are selected for monitoring.
- **Syslog Alarm**: Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

Before you begin

If you have created a self-signed certificate or imported an SSL certificate to the keystore, you must copy the new fmserver.jks located at `/usr/local/cisco/dcm/wildfly-10.1.0.Final/standalone/configuration` to `/etc/elasticsearch`. If you do not copy the fmserver.jks file to the elasticsearch directory, you will not be able to get the Alarms and Policies. As the elasticsearch database will be stabilizing, you cannot configure any Alarm Policy on the Cisco DCNM Web UI **Monitor > Alarms > Alarm Policies**.

Procedure

Step 1 Choose **Monitor > Alarms > Alarm Policies**.

Step 2 Select the **Enable Alarms** check box to enable alarm policies.

Step 3 From the **Add** drop-down list, choose any of the following:

- Device Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, CPU Utilization parameters, Memory Utilization parameters, Environment Temperature parameters, device availability, and device features.
- Interface Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, link-state, Bandwidth (In/Out), Inbound errors, Outbound errors, Inbound Discards, and Outbound Discards.
- Syslog Alarm Policy: Select the devices for which you want to create policies and then specify the following parameters.
  - Devices: Define the scope of this policy. Select individual devices or all devices to apply this policy.
  - Policy Name: Specify the name for this policy. It must be unique.
  - Description: Specify a brief description for this policy.
  - Severity: Define the severity level for this syslog alarm policy. Choices are: Critical, Major, Minor, and Warning.
  - Identifier: Specify the identifier portions of the raise & clear messages.
  - Raise Regex: Define the format of a syslog raise message. The syntax is as follows: **Facility-Severity-Type: Message**
  - Clear Regex: Define the format of a syslog clear message. The syntax is as follows: **Facility-Severity-Type: Message**

Table 8: Example 1

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_ADMIN_UP: Interface Ethernet15/1 is admin up .
Clear Regex	ETHPORT-5-IF_DOWN_NONE: Interface Ethernet15/1 is down (Transceiver Absent)

In the above example, the regex expressions are part of the syslog messages that appear in the terminal monitor.

Table 9: Example 2

Identifier	ID1-ID2
Raise Regex	ETH_PORT_CHANNEL-5-PORT_DOWN: $(ID1): $(ID2) is down
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP: $(ID1): $(ID2) is up

Table 10: Example 3

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning cleared

Step 4 Click **OK** to add the policy.

Syslog Messages in Terminal Monitor and Console

The following examples show how the syslog messages appear in the terminal monitor and the console. The regex expression is matched with the part of the syslog messages after the % sign.

```
leaf-9516# terminal monitor
leaf-9516# conf t
leaf-9516(config)# int e15/1-32
leaf-9516(config-if-range)# no shut
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/1 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/1 is down (Transceiver Absent)
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/2 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/2 is down (Transceiver Absent)
2019 Aug 2 04:41:28 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/3 is admin up .
```

The syslog messages in the console have a similar format as they would appear in the terminal monitor, except for the additional port information enclosed in the %$ signs. However, the regex expression is matched with the part of the syslog messages after the last % sign.

```
SR-leaf1# 2019 Aug 26 23:55:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-
PFM_ALERT: FAN_BAD: fan6
2019 Aug 26 23:56:15 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:18 SR-leaf1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL:
System ready
2019 Aug 26 23:56:25 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:35 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED:
The guest shell has been enabled. The command 'guestshell' may be used
to access it, 'guestshell destroy' to remove it.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FAN_REMOVED: Fan
module 5 (Serial number ) Fan5(sys_fan5) removed
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 2 minutes 0 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

```
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 1 minutes 40 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK:
Fan module 5 (Fan5(sys_fan5) fan) ok
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

Activating Policies

After you create new alarm policies, activate them.

Procedure

Step 1 Choose **Monitor > Alarms > Policies**.

Step 2 Select the policies that you want to activate and then click the **Activate** button.

Deactivating Policies

You can deactivate the active alarm policies.

Procedure

Step 1 Choose **Monitor > Alarms > Policies**.

Step 2 Select the policies that you want to deactivate and then click the **Deactivate** button.

Importing Policies

You can create alarm policies using the import functionality.

Procedure

Step 1 Choose **Monitor > Alarms > Policies** and then click the **Import** button.

Step 2 Browse and select the policy file saved on your computer.

You can only import policies in text format.

Exporting Policies

You can export the alarm policies into a text file.

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Click the **Export** button and then select a location on your computer to store the exported file.

Editing Policies

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Select the policy that you want to edit.

Step 3 Click the **Edit** button and then make necessary changes.

Step 4 Click the **OK** button.

Deleting Policies

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Select the policy that you want to delete.

Step 3 Click the **Delete** button. The policy is deleted.