Monitoring Traffic

This chapter includes the following sections:

- Traffic Monitoring, page 1
- Guidelines and Recommendations for Traffic Monitoring, page 2
- Creating a Traffic Monitoring Session, page 3
- Adding Sources for Traffic Monitoring, page 4
- Activating a Traffic Monitoring Session, page 4
- Deleting a Traffic Monitoring Session, page 5

Traffic Monitoring

Traffic monitoring copies traffic from one or more sources and sends the copied traffic to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Type of Session

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port.

Traffic Sources

An Ethernet traffic monitoring session can monitor any of the following traffic sources:

- Uplink Ethernet port
- Ethernet port channel
- VLAN
- Service profile vNIC
- Service profile vHBA

- FCoE port
- Port channels
- Server port

A Fibre Channel traffic monitoring session can monitor any of the following traffic sources:

- Uplink Fibre Channel port
- SAN port channel
- VSAN
- Service profile vHBA
- Fibre Channel storage port

Guidelines and Recommendations for Traffic Monitoring

When configuring or activating traffic monitoring, consider the following guidelines:

- You can create and store up to 16 traffic monitoring sessions, but only two can be active at the same time.
- A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.
- To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.
- To monitor traffic from a VM, you must first determine the identity of the dynamic vNIC assigned to the VM. Follow the procedure in to find the vNIC and view its identity properties, then add the vNIC as a source for the monitoring session. If you later move the VM using VMotion, a new dynamic vNIC is assigned and you must reconfigure the monitoring source.

  Viewing Dynamic vNIC Properties in a VM
- You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored using an Ethernet traffic monitoring session, with an Ethernet destination port, the destination traffic will be FCoE.
- Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, you must create two sessions—one per fabric—and connect two analyzers. Add the vNIC as the traffic source for both sessions.
- All traffic sources must be located within the same switch as the destination port.
- A port configured as a destination port cannot also be configured as a source port.
- A member port of a port channel cannot be configured individually as a source. If the port channel is configured as a source, all member ports are source ports.
- A vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously.
- A server port can be a source only if it is a non-virtualized rack server adapter-facing port.

- Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.

Creating a Traffic Monitoring Session

Note This procedure describes how to create an Ethernet traffic monitoring session. To create a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** ➤ **Traffic Monitoring Sessions** ➤ ***Fabric_Interconnect_Name***.

Step 3 Right-click ***Fabric_Interconnect_Name*** and choose **Create Traffic Monitoring Session**.

Step 4 In the **Create Traffic Monitoring Session** dialog box, complete the following fields:

Name	Description
Name field	The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Admin State field	Whether traffic will be monitored for the physical port selected in the **Destination** field. This can be: • **enabled**—Cisco UCS begins monitoring the port activity as soon as some source components are added to the session. • **disabled**—Cisco UCS does not monitor the port activity.
Destination drop-down list	Select the physical port whose communication traffic you want to monitor from the navigation tree.

Step 5 Click **OK**.

What to Do Next

- Add traffic sources to the traffic monitoring session.
- Activate the traffic monitoring session.

Adding Sources for Traffic Monitoring

You can choose multiple sources from more than one source type to be monitored by a traffic monitoring session. The available sources depend on the components configured in the Cisco UCS instance.

Note This procedure describes how to add sources for Ethernet traffic monitoring sessions. To add sources for a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** ➤ **Traffic Monitoring Sessions** ➤ ***Fabric_Interconnect_Name***.

Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to configure.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Sources** area, expand the section for the type of traffic source that you want to add.

Step 6 To see the components that are available for monitoring, click the + button in the right-hand edge of the table to open the **Create Monitoring Session Source** dialog box.

Step 7 Select a source component and click **OK**.
You can repeat the preceding three steps as needed to add multiple sources from multiple source types.

Step 8 Click **Save Changes**.

What to Do Next

Activate the traffic monitoring session. If the session is already activated, traffic will be forwarded to the monitoring destination when you add a source.

Activating a Traffic Monitoring Session

Note This procedure describes how to activate an Ethernet traffic monitoring session. To activate a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN** ➤ **Traffic Monitoring Sessions** ➤ ***Fabric_Interconnect_Name***.
Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to activate.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Properties** area, click the **enabled** radio button for **Admin State**.
Step 6 Click **Save Changes**.

If a traffic monitoring source is configured, traffic begins to flow to the traffic monitoring destination port.

Deleting a Traffic Monitoring Session

Note This procedure describes how to delete an Ethernet traffic monitoring session. To delete a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN** ➤ **Traffic Monitoring Sessions** ➤ ***Fabric_Interconnect_Name***.
Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to delete.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click the **Delete** icon.
Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.