Traffic Monitoring

Traffic Monitoring

Traffic monitoring copies traffic from one or more source ports 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).

Types of Traffic Monitoring Sessions

There are two types of monitoring sessions:

- Ethernet
- Fibre channel

The type of destination port determines what kind of monitoring session you need. 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 except when you are using Cisco UCS 6300 Fabric Interconnects.

Note For Cisco UCS 6332 and 6332-16UP Fabric Interconnects, you cannot choose Fibre Channel destination ports. The destination port must be an unconfigured physical Ethernet port.

Traffic Monitoring Across Ethernet

An Ethernet traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• Uplink Ethernet port • Ethernet port channel • VLAN • Service profile vNIC • Service profile vHBA • FCoE port • Port channels • Unified uplink port • VSAN	Unconfigured Ethernet Port

Note 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 server port can be a source, only if it is a nonvirtualized rack server adapter-facing port.

Traffic Monitoring for Cisco UCS 6300 Interconnects

- Cisco UCS 6300 Fabric Interconnect supports port-based mirroring.
- Cisco UCS 6300 Fabric Interconnect supports VLAN SPAN only in the Rx or the receive direction.
- Ethernet SPAN is port based on the Cisco UCS 6300 Fabric Interconnect.

Traffic Monitoring for Cisco UCS 6200 Interconnects

- Cisco UCS 6200 and 6324 supports monitoring traffic in the ‘transmit’ direction for up to two sources per Fabric Interconnect.
- Cisco UCS 6200 SPAN traffic is rate-limited by the SPAN destination port speed. This can be either 1 or 10 Gbps.

Important (For 6200 and 6324 Fabric Interconnects) You can monitor or use SPAN on port channels only for ingress traffic.

Traffic Monitoring Across Fibre Channel

You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored with an Ethernet traffic monitoring session, at an Ethernet destination port, the destination traffic is FCoE. The Cisco UCS 6300 Fabric Interconnect supports FC SPAN

only on the ingress side. A Fibre Channel port on a Cisco UCS 6248 Fabric Interconnect cannot be configured as a source port.

A Fibre Channel traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• FC Port • FC Port Channel • Uplink Fibre Channel port • SAN port channel • VSAN • Service profile vHBA • Fibre Channel storage port	• Fibre Channel uplink port • Unconfigured Ethernet Port (Cisco UCS 6332 and Cisco UCS 6332-16UP Fabric Interconnects)

Guidelines and Recommendations for Traffic Monitoring

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

Traffic Monitoring Sessions

A traffic monitoring session is disabled by default when created. To begin monitoring traffic, first activate the session. A traffic monitoring session must be unique on any fabric interconnect within the Cisco UCS pod. Create each monitoring session with a unique name and unique VLAN source. To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.

Maximum Number of Supported Active Traffic Monitoring Sessions Per Fabric-Interconnect

You can create and store up to 16 traffic monitoring sessions, but only four can be active at the same time. For each Cisco UCS 6300 Fabric Interconnect, you can only monitor up to four traffic directions. The receive and transmit directions each count as one monitoring session, while the bi-direction monitoring session is counted as 2. For example:

- Four active sessions — If each session is configured to monitor traffic in only one direction
- Two active sessions — If each session is configured to monitor traffic bidirectionally.
- Three active sessions — If one session is unidirectional and the second session is bidirectional.

Note 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.

vNIC

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, create two sessions, one per fabric and connect two analyzers. Add the vNIC as the traffic source using the exact same name for both sessions. If you change the port profile of a virtual machine, any associated vNICs being used as source ports are removed from monitoring, and you must reconfigure the monitoring session. If a traffic monitoring session was configured on a dynamic vNIC under a release earlier than Cisco UCS Manager Release 2.0, you must reconfigure the traffic monitoring session after upgrading.

vHBA

A vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously. When a VHBA is set as the SPAN source, the SPAN destination only receives VN-Tagged frames. It does not receive direct FC frames.

Creating an Ethernet Traffic Monitoring Session

Procedure

Step 1 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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Admin State field	Indicates whether traffic will be monitored for the physical port selected in the **Destination** field. This can be one of the following: • **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.
Span Control Packets field	Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following: • **Enabled**—Cisco UCS monitors outgoing control packets on the port. • **Disabled**—Cisco UCS does not monitor outgoing control packets on the port.
Destination drop-down list	The physical port that is being monitored. Click the link in this field to view the port properties.

Name	Description
Admin Speed field	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. For Ethernet Traffic Monitoring sessions in 6332 and 6332-16UP FIs, you cannot use the 1Gbps speed configuration for the configured Ethernet Destination Port.

Step 2 Click **OK**.

What to do next

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

Setting the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

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

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

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Set Destination**.

Step 5 In the **Set Destination** dialog box, complete the following fields:

Example:

Name	Description
Destination drop-down list	The physical port where you want to monitor all the communication from the sources.
Admin Speed field	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. For Ethernet Traffic Monitoring sessions in 6332 and 6332-16UP FIs, you cannot use the 1Gbps speed configuration for the configured Ethernet Destination Port.

Step 6 Click **OK**.

Clearing the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

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

Step 2 Expand **LAN** > **Traffic Monitoring Sessions** > *Fabric_Interconnect_Name* > *Monitor_Session_Name*.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Clear Destination**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand**SAN** > **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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Admin State field	Indicates whether traffic will be monitored for the physical port selected in the **Destination** field. This can be one of the following: • **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.

Name	Description
Span Control Packets field	Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following: • **Enabled**—Cisco UCS monitors outgoing control packets on the port. • **Disabled**—Cisco UCS does not monitor outgoing control packets on the port.
Destination drop-down list	Select the physical port where you want to monitor all the communication from the sources.
Admin Speed drop-down list	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. This can be one of the following: • **1 Gbps** • **10 Gbps** • **25 Gbps** • **Auto**—Cisco UCS determines the data transfer rate.

Step 5 Click **OK**.

What to do next

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

Setting the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand**SAN** > **Traffic Monitoring Sessions** > *Fabric_Interconnect_Name* > *Monitor_Session_Name*

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Set Destination**.

Step 5 In the **Set Destination** dialog box, complete the following fields:

Name	Description
Destination drop-down list	Select the physical port where you want to monitor all the communication from the sources.
Admin Speed drop-down list	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain. This can be one of the following: • **1 Gbps** • **2 Gbps** • **4 Gbps** • **8 Gbps** • **Auto**—Cisco UCS determines the data transfer rate.

Step 6 Click **OK**.

Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **Traffic Monitoring Sessions** > **Fabric_Interconnect_Name** > **Monitor_Session_Name**

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Clear Destination**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Adding Traffic Sources to a Monitoring Session

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 domain.

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 **LAN**.

Step 2 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 **Add 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 **LAN**.

Step 2 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 **LAN**.

Step 2 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 a confirmation dialog box displays, click **Yes**.