Traffic Monitoring

Traffic Monitoring

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

Important

For FC port channels on Cisco UCS 6200 Fabric Interconnects, you can monitor only egress traffic.

For FC port channels on Cisco UCS 6300 Fabric Interconnects, you can monitor only ingress traffic.

Traffic Monitoring Session Types

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.

Note

For Cisco UCS 6300 Fabric Interconnects, the destination port must also be an unconfigured physical Ethernet port. For Cisco UCS 6332 and Cisco UCS 6332-16UP Fabric Interconnects, you cannot choose Fibre Channel destination ports, but can use unconfigured ethernet ports as a destination for FC traffic monitoring sessions.

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 • Unified storage port • Appliance storage port	• Unconfigured Ethernet Port

Traffic Monitoring for UCS 6300 Interconnects

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

Traffic Monitoring for UCS 6200 Interconnects

- Cisco UCS 6200 and 6324 supports monitoring traffic in the transmit (tx) 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 Gbps or 10 Gbps.

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, the destination traffic is FCoE. The Cisco UCS 6300 Fabric Interconnect supports FC SPAN only on the ingress side. You cannot configure a Fibre Channel port on a Cisco Cisco UCS 6248 Fabric Interconnect 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 • Ethernet Port (only for Cisco UCS 6300 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, you must activate the session.

- Create a unique traffic monitoring session on any fabric interconnect within the Cisco UCS pod.
- Create each monitoring session with a unique name and unique source.
- Add all vNICs from the service profile of a server to monitor traffic from a server.
- Locate all traffic sources within the same switch as the destination port.
- Do not add the same source in multiple traffic monitoring sessions.
- Do not configure a port as a destination port and a source port.
- Do not configure a member port, of a port channel, individually as a source. If you configure the port channel as a source, all member ports are source ports.

Maximum Supported Active Traffic Monitoring Sessions

You can only monitor up to four traffic directions for each Cisco UCS 6300 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 Fabric Interconnect. The receive and transmit directions each count separately as one active session, while the bidirectional is counted as two active sessions. 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, you must reconfigure the monitoring session. All associated vNICs used as source ports are removed from monitoring.

vHBA

You can use a vHBA as 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.

SPAN Ports Support Matrix

Note For Cisco UCS 6200 and 6324 FIs, you can only set the source mode to transmit for two sources per Cisco UCS domain.

Ethernet Span Port Sources

Source Ethernet SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Ethernet Port-Channel	Receive	Receive	Receive, Transmit, Both
FCoE Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Port-Channel	Receive	Receive	Receive, Transmit, Both
Appliance Port	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Storage	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Unified Ports	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
VLAN	Receive	Receive	Receive
Static vNIC	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
vHBA	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both

Ethernet Span Port Destinations

Destination Ethernet SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet SPAN Ports	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1Gbps, 10 Gbps, 40 Gbps

FC Span Port Sources

Source FC SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC Uplink	Transmit	Not Supported	Receive
FC Port-Channel	Transmit	Not Supported	Receive
FC Storage	Transmit	Not Supported	Receive
VSAN	Not Supported	Not Supported	Receive
vHBA	Receive, Transmit, Both	Not Supported	Receive, Transmit, Both

FC Span Port Destinations

Destination FC SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC SPAN Ports	FC Uplink at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Unconfigured at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto
FC SPAN Ports	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto

Creating a Traffic 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 existing components configured.

Before you begin

Before creating a traffic monitoring session in Cisco UCS Central, ensure that port configuration is set to **Global** on the **Policy Resolution Control** page for the Cisco UCS.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 On the **Fabric Interconnects** page, select the fabric interconnect to which you want to add a traffic monitoring session.

Step 3 On the **Fabric Interconnect** page, click the Tools icon and choose **Create Traffic Monitoring**.

Step 4 In the **Traffic Monitoring** dialog box, on the **Basic** tab, do the following:

a) Choose whether to create an **Ethernet** or **FC** traffic monitoring session.

You cannot modify the type after creation.

b) Enter the **Name** for your traffic monitoring session.

You cannot modify the name after creation.

c) Choose the **Admin State**:

- **Disabled**—Creates the session, but does not activate traffic monitoring.
- **Enabled**—Immediately activates the traffic monitoring session upon creation.

d) Select the **Destination Port** that you want to monitor.

Step 5 On the **Sources** tab, add the sources that you want to monitor.

For Ethernet traffic monitoring, you can monitor ports, port channels, VLANs, vNICs or vHBAs.

For FC traffic monitoring, you can monitor ports, port channels, VSANs, or vHBAs.

Step 6 Click **Create**.

Editing an Existing Traffic Monitoring Session

Modify the **Admin State** to activate or deactivate the traffic monitoring session.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 On the **Fabric Interconnects** page, select the fabric interconnect with the traffic monitoring session that you want to modify.

Step 3 On the **Fabric Interconnect** page, click the **Traffic Monitoring** tab.

Step 4 Select the traffic monitoring session that you want to modify, and click the **Edit** icon.

Note You cannot modify the name or the type of traffic monitoring.

Step 5 On the **Basic** tab, in Admin State, choose one of the following:

- **Disabled**—Deactivates traffic monitoring.
- **Enabled**—Activates the traffic monitoring session.

Step 6 Modify the **Destination Port**, if necessary.

Step 7 On the **Sources** tab, make any necessary changes to the sources that you want to monitor.

Step 8 Click **Save**.

Activating or Deactivating a Traffic Monitoring Session

Existing traffic monitoring sessions can be activated or deactivated.

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Choose the fabric interconnect where you want to update traffic monitoring.
Step 3 On the fabric interconnect page, click **Traffic Monitoring**.
Step 4 Click on the traffic monitoring session that you want to edit.
Step 5 Click the **Edit** icon.
Step 6 Modify the Admin State:

- **Enabled**—Immediately activates the traffic monitoring session.
- **Disabled**—Deactivates the active traffic monitoring session.

Step 7 Click **Save**.

Deleting a Traffic Monitoring Session

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.
Step 2 Choose the fabric interconnect where you want to update traffic monitoring.
Step 3 On the fabric interconnect page, click **Traffic Monitoring**.
Step 4 Click on the traffic monitoring session that you want to delete.
Step 5 Click the **Delete** icon.