



Traffic Monitoring

- [Traffic Monitoring, on page 1](#)
- [Guidelines and Recommendations for Traffic Monitoring, on page 3](#)
- [Creating an Ethernet Traffic Monitoring Session, on page 4](#)
- [Creating a Fibre Channel Traffic Monitoring Session, on page 5](#)
- [Adding Traffic Sources to a Monitoring Session, on page 6](#)
- [Activating a Traffic Monitoring Session, on page 11](#)
- [Deleting a Traffic Monitoring Session, on page 12](#)
- [SPAN Restrictions for the Cisco UCS Mini, on page 13](#)

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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • FC Port • FC Port Channel • Uplink Fibre Channel port • SAN port channel • VSAN • Service profile vHBA • Fibre Channel storage port 	<ul style="list-style-type: none"> • 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



- Note** This procedure describes creating an Ethernet traffic monitoring session. To create a Fibre Channel traffic monitoring session, the following changes are required:
- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
 - Enter the **create fc-mon-session** command instead of the **create eth-mon-session** command in Step 3.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope eth-traffic-mon	Enters Ethernet traffic monitoring command mode.
Step 2	UCS-A /eth-traffic-mon # scope fabric {a b}	Enters traffic monitoring command mode for the specified fabric.
Step 3	UCS-A /eth-traffic-mon/fabric # create eth-mon-session session-name	Creates a traffic monitoring session with the specified name.
Step 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session # create dest-interface slot-num port-num	Configures the interface at the specified slot and port number to be the destination for the traffic monitoring session. Enters the command mode for the interface.
Step 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # set speedadmin-speed	Sets the data transfer rate of the port channel to be monitored. This can be: <ul style="list-style-type: none"> • 1gbps—1 Gbps • 10gbps—10 Gbps • 20gbps—20 Gbps • 40gbps—40 Gbps

	Command or Action	Purpose
Step 6	UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # commit-buffer	Commits the transaction to the system configuration.

Example

The following example creates an Ethernet traffic monitoring session to copy and forward traffic to the destination port at slot 2, port 12, sets the admin speed to 20 Gbps, and commits the transaction:

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session EthMonitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create dest-interface 2 12
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # set speed 20gbps
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface #
```

What to do next

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

Creating a Fibre Channel Traffic Monitoring Session

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope fc-traffic-mon	Enters Fibre Channel traffic monitoring command mode.
Step 2	UCS-A /fc-traffic-mon # scope fabric {a b}	Enters Fibre Channel traffic monitoring command mode for the specified fabric.
Step 3	UCS-A /fc-traffic-mon/fabric # create fc-mon-session session-name	Creates a Fibre Channel traffic monitoring session with the specified name.
Step 4	UCS-A /fc-traffic-mon/fabric/fc-mon-session # create dest-interface slot-num port-num	Creates and enters the command mode of the destination slot and port for the Fibre Channel traffic monitoring session.
Step 5	UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # set speedadmin-speed	Sets the data transfer rate of the port channel to be monitored. This can be: <ul style="list-style-type: none"> • 1gbps—1 Gbps • 2gbps—2 Gbps • 4gbps—4 Gbps

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 8gbps—8 Gbps • auto—Cisco UCS determines the data transfer rate.
Step 6	UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # commit-buffer	Commits the transaction to the system configuration.

Example

The following example creates a Fibre channel traffic monitoring session to copy and forward traffic to the destination port at slot 1, port 10, sets the admin speed to 8 Gbps, and commits the transaction:

```
UCS-A# scope fc-traffic-mon
UCS-A /fc-traffic-mon # scope fabric a
UCS-A /fc-traffic-mon/fabric # create fc-mon-session FCMonitor
UCS-A /fc-traffic-mon/fabric/fc-mon-session* # create dest-interface 1 10
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # set speed 8gbps
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # commit-buffer
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface #
```

What to do next

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

Adding Traffic Sources to a Monitoring Session

Adding an Uplink Source Port to a Monitoring Session



Note This procedure describes adding an Ethernet uplink port as a source for a traffic monitoring session. To add a Fibre Channel uplink port as a source, enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.

Before you begin

A traffic monitoring session must be created.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope eth-uplink	Enters Ethernet uplink command mode.

	Command or Action	Purpose
Step 2	UCS-A /eth-uplink # scope fabric {a b}	Enters uplink fabric mode for the specified fabric.
Step 3	UCS-A /eth-uplink/fabric # scope interface <i>slot-num port-num</i>	Enters the interface command mode for the specified uplink port.
Step 4	UCS-A /eth-uplink/fabric/interface # create mon-src <i>session-name</i>	Adds the uplink port as a source to the specified monitoring session.
Step 5	(Optional) UCS-A /eth-uplink/fabric/interface/mon-src # set direction {both receive transmit}	Specifies the traffic direction to be monitored. Note If you do not select any direction, the default direction is Rx.
Step 6	UCS-A /eth-uplink/fabric/interface/mon-src # commit-buffer	Commits the transaction to the system configuration.

Example

The following example adds the ingress traffic on Ethernet uplink port 3 on slot 2 of fabric A as a source for a monitoring session and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 2 3
UCS-A /eth-uplink/fabric/interface # create mon-src Monitor23
UCS-A /eth-uplink/fabric/interface/mon-src* # set direction receive
UCS-A /eth-uplink/fabric/interface/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/interface/mon-src #
```

What to do next

You can add additional sources to the traffic monitoring session.

Adding a vNIC or vHBA Source to a Monitoring Session



Note This procedure describes adding a vNIC as a source for a traffic monitoring session. To add a vHBA as a source, enter the **scope vhba** command instead of the **scope vnic** command in Step 2.

Before you begin

A traffic monitoring session must be created.

Procedure

	Command or Action	Purpose
Step 1	Switch-A# scope system	Enters system mode.

	Command or Action	Purpose
Step 2	Switch-A /system # scope vm-mgmt	Enters VM management mode.
Step 3	(Optional) Switch-A /system/vm-mgmt # show virtual-machine	Displays the running virtual machines.
Step 4	Switch-A /system/vm-mgmt # scope virtual-machine uuid	Enters command mode for the virtual machine that contains the dynamic vNIC.
Step 5	(Optional) Switch-A /system/vm-mgmt/virtual-machine # show expand	Displays the virtual machine details, including the vNIC MAC address.
Step 6	Switch-A /system/vm-mgmt/virtual-machine # scope vnic mac-address	Enters the command mode for the vNIC at the specified MAC address.
Step 7	Switch-A /system/vm-mgmt/virtual-machine/vnic # create mon-src session-name	Adds the vNIC as a source to the specified monitoring session.
Step 8	(Optional) Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # set direction {both receive transmit}	Specifies the traffic direction to be monitored.
Step 9	Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # commit-buffer	Commits the transaction to the system configuration.

Example

The following example adds the ingress traffic on a dynamic vNIC as a source for a monitoring session and commits the transaction:

```
Switch-A# scope system
Switch-A /system # scope vm-mgmt
Switch-A /system/vm-mgmt # show virtual-machine
Virtual Machine:
  UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
  Service Profile: org-root/ls-dsw-bld1-esx
  Server: sys/chassis-1/blade-1
  Status: Online
.
.
.
Switch-A /system/vm-mgmt # scope virtual-machine 42327c42-e00c-886f-e3f7-e615906f51e9
Switch-A /system/vm-mgmt/virtual-machine # show expand
Virtual Machine:
  UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
  Service Profile: org-root/ls-dsw-bld1-esx
  Server: sys/chassis-1/blade-1
  Status: Online

vNIC:
  Name:
  Status: Online
  MAC Address: 00:50:56:B2:00:00
```



```

VIF:
  Vif Id: 32772
  Status: Online
  Phys Fabric ID: B
  Virtual Fabric:
Switch-A /system/vm-mgmt/virtual-machine # scope vnic 00:50:56:B2:00:00
Switch-A /system/vm-mgmt/virtual-machine/vnic # create mon-src Monitor23
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # set direction receive
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # commit-buffer

Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src #

```

What to do next

You can add additional sources to the traffic monitoring session.

Adding a VLAN or VSAN Source to a Monitoring Session



Note This procedure describes adding a VLAN as a source for a traffic monitoring session. To add a VSAN as a source, the following changes are required:

- Enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.
- Enter the **create vsan** command instead of the **create vlan** command in Step 3.

Before you begin

A traffic monitoring session must be created.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope eth-uplink	Enters Ethernet uplink command mode.
Step 2	UCS-A /eth-uplink # scope fabric {a b}	Enters uplink fabric mode for the specified fabric. Note This step is required when adding a local VLAN as a source. To add a global VLAN as a source, omit this step.
Step 3	UCS-A /eth-uplink/fabric # create vlan <i>vlan-name vlan-id</i>	Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters uplink VLAN mode.
Step 4	UCS-A /eth-uplink/fabric/vlan # create mon-src <i>session-name</i>	Adds the VLAN as a source to the specified monitoring session.
Step 5	UCS-A /eth-uplink/fabric/vlan/mon-src # commit-buffer	Commits the transaction to the system configuration.

Example

The following example adds a local VLAN as a source for an Ethernet monitoring session and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan vlan23 23
UCS-A /eth-uplink/fabric/vlan # create mon-src Monitor23
UCS-A /eth-uplink/fabric/vlan/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/vlan/mon-src #
```

What to do next

You can add additional sources to the traffic monitoring session.

Adding a Storage Port Source to a Monitoring Session



Note This procedure describes adding a Fibre Channel storage port as a source for a Fibre Channel traffic monitoring session. To add an FCoE storage port as a source for an Ethernet traffic monitoring session, enter the **create interface fcoe** command instead of the **create interface fc** command in Step 3.

Before you begin

A traffic monitoring session must be created.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope fc-storage	Enters Fibre Channel storage port command mode.
Step 2	UCS-A /fc-storage # scope fabric {a b}	Enters Fibre Channel storage port fabric mode for the specified fabric.
Step 3	UCS-A /fc-storage/fabric # create interface fc slot-num port-num	Creates a Fibre Channel storage port interface and enters the interface command mode.
Step 4	UCS-A /fc-storage/fabric/fc # create mon-src session-name	Adds the storage port as a source to the specified monitoring session.
Step 5	UCS-A /fc-storage/fabric/fc/mon-src # commit-buffer	Commits the transaction to the system configuration.

Example

The following example adds a Fibre Channel storage port on port 3 of slot 2 as a source for a Fibre Channel monitoring session and commits the transaction:

```

UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric # create interface fc 2 3
UCS-A /fc-storage/fabric/fc* # create mon-src Monitor23
UCS-A /fc-storage/fabric/fc/mon-src* # commit-buffer
UCS-A /fc-storage/fabric/fc/mon-src #

```

What to do next

You can add additional sources to the traffic monitoring session.

Activating a Traffic Monitoring Session



Note This procedure describes activating an Ethernet traffic monitoring session. To activate a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **scope fc-mon-session** command instead of the **scope eth-mon-session** command in Step 3.

Before you begin

Configure a traffic monitoring session.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope eth-traffic-mon	Enters Ethernet traffic monitoring command mode.
Step 2	UCS-A /eth-traffic-mon # scope fabric {a b}	Enters traffic monitoring command mode for the specified fabric.
Step 3	UCS-A /eth-traffic-mon/fabric # scope eth-mon-session session-name	Enters the command mode of the traffic monitoring session with the specified name.
Step 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session # disable enable	Disables or enables the traffic monitoring session.
Step 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session # commit-buffer	Commits the transaction to the system configuration.

When activated, the traffic monitoring session begins forwarding traffic to the destination when a traffic source is configured.

Example

The following example activates an Ethernet traffic monitoring session and commits the transaction:

```

UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # scope eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session # enable
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session # show

Ether Traffic Monitoring Session:
  Name          Admin State      Oper State      Oper State Reason
  -----
  Monitor33     Enabled           Up              Active

UCS-A /eth-traffic-mon/fabric/eth-mon-session #

```

Deleting a Traffic Monitoring Session



Note This procedure describes deleting an Ethernet traffic monitoring session. To delete a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **delete fc-mon-session** command instead of the **delete eth-mon-session** command in Step 3.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope eth-traffic-mon	Enters Ethernet traffic monitoring command mode.
Step 2	UCS-A /eth-traffic-mon # scope fabric {a b}	Enters traffic monitoring command mode for the specified fabric.
Step 3	UCS-A /eth-traffic-mon/fabric # delete eth-mon-session <i>session-name</i>	Deletes the traffic monitoring session with the specified name.
Step 4	UCS-A /eth-traffic-mon/fabric # commit-buffer	Commits the transaction to the system configuration.

Example

The following example deletes an Ethernet traffic monitoring session and commits the transaction:

```

UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # delete eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric* # commit-buffer
UCS-A /eth-traffic-mon/fabric #

```

SPAN Restrictions for the Cisco UCS Mini

Consider the following guidelines and restrictions when configuring the SPAN feature on Cisco UCS Mini

- FC port as SPAN destination is not supported.
- VSAN as SPAN source is not supported.
- FC uplink ports as SPAN source is not supported.

