Configuring SPAN

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) to analyze traffic between ports on Cisco NX-OS devices.

- Finding Feature Information, on page 1
- About SPAN, on page 1
- Prerequisites for SPAN, on page 7
- Guidelines and Limitations for SPAN, on page 7
- Default Settings for SPAN, on page 14
- Configuring SPAN, on page 14
- Verifying the SPAN Configuration, on page 42
- Configuration Examples for SPAN, on page 43
- Related Documents, on page 47
- Feature History for SPAN, on page 48

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

About SPAN

SPAN analyzes all traffic between source ports by directing the SPAN session traffic to a destination port with an external analyzer attached to it.

You can define the sources and destinations to monitor in a SPAN session on the local device.

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. SPAN sources include the following:

- Ethernet ports

- Port channels
- The inband interface to the control plane CPU
- VLANs (ingress only)—When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources.
- Remote SPAN (RSPAN) VLANs
- Fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender (FEX)
- Satellite ports and host interface port channels on the Cisco Nexus 2000 Series Fabric Extender— These interfaces are supported in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode.

Note Layer 3 subinterfaces are not supported.

Note A single SPAN session can include mixed sources in any combination of the above.

Characteristics of Source Ports

SPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- An RSPAN VLAN cannot be used as a SPAN source.
- If you use the supervisor inband interface as a SPAN source, the following packets are monitored:
  - All packets that arrive on the supervisor hardware (ingress)
  - All packets generated by the supervisor hardware (egress)

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources.

Characteristics of Destination Ports

SPAN destination ports have the following characteristics:

- Destinations for a SPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one SPAN session at a time.
- Destination ports do not participate in any spanning tree instance. SPAN output includes bridge protocol data unit (BPDU) Spanning-Tree Protocol hello packets.
- All SPAN destinations configured for a given session receive all spanned traffic.

- An RSPAN VLAN cannot be used as a SPAN destination.
- You can configure SPAN destinations to inject packets to disrupt a certain TCP packet stream in support of the Intrusion Detection System (IDS).
- You can configure SPAN destinations to enable a forwarding engine to learn the MAC address of the IDS.
- F Series module FabricPath core ports, Fabric Extender host interface (HIF) ports, HIF port channels, and fabric port-channel ports are not supported as SPAN destination ports.
- Shared interfaces cannot be used as SPAN destinations.
- VLAN ACL redirects to SPAN destination ports are not supported
- All SPAN destinations configured for a given session receive all spanned traffic.

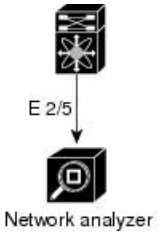
SPAN Sessions

You can create SPAN sessions to designate sources and destinations to monitor.

See the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide* for information on the number of supported SPAN sessions.

This figure shows a SPAN configuration. Packets on three Ethernet ports are copied to destination port Ethernet 2/5. Only traffic in the direction specified is copied.

Figure 1: SPAN Configuration



Source Port	Direction	Destination Ports
E 2/1	Rx	E 2/5
E 2/2	Rx, Tx	
E 2/3	Tx	

188383

Extended SPAN Sessions

Cisco NX-OS Release 6.2(2) and later releases support extended SPAN sessions in addition to the two traditional SPAN sessions supported in prior releases. Extended SPAN sessions can be traditional or unidirectional. The session direction is specified during session creation. A pool of 12 independent session resources are available. Unidirectional sessions use one resource, and traditional sessions use two resources. These 12 resources are shared between local and SPAN source sessions across all VDCs.

If you are configuring an extended SPAN session on a Cisco Nexus 7710 switch or a Cisco Nexus 7718 switch, the following applies:

- The **mode extended** command must be used with the third configuration session.
- You can configure 16 sessions as unidirectional or bidirectional, as required.
- You do not need to maintain two traditional sessions.
- You do not need to use the resource manager to reserve the two traditional sessions.

4K VLANs per SPAN Session

Cisco NX-OS Release 7.3(0)D1(1) and later releases support 4K VLANs per SPAN session. You can use the **source interface all** command to enable the monitor session on the switch to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The 4K VLANs per SPAN Session feature also enables monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in the monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.

The 4K VLANs per SPAN Session feature has the following characteristics:

- This is not supported on M3 series modules.
- You will not be able to capture any traffic on the M3 Series modules in spite of configuring the**source interface all** command.
- You can use the **source interface all** command for multiple sessions in the same VDC.
- Supports all session parameters such as MTU truncation, Sampling and Rate Limiting.
- Simple and Complex Rule-based SPAN is supported with the **source interface all** command. This enables traffic flow-based monitoring using a set of filter rules across the VDC.
- Traffic generated by Supervisors is not spanned.
- Supported only in Ethernet VDCs of Cisco Nexus 7000 Series switches.
- Supported only in extended SPAN sessions.

Rule-Based SPAN

Rule-based SPAN filters the ingress or egress SPAN traffic based on a set of rules. For Cisco NX-OS releases prior to 6.2(2), you can filter on VLANs, the destination index, and the source index. Beginning with Cisco NX-OS Release 6.2(2), you can filter the SPAN traffic based on a combination of fields in the Layer 2, Layer 3, or Layer 4 header packet.

Every SPAN session (traditional and extended) has an associated filter. Every SPAN session has one filter resource. A simple filter has only one rule, and you can add multiple fields or conditions to this rule. The packets are replicated only if all the conditions are met.

Table 1: Supported Filter Fields

Ethernet	IPv4	IPv6	ARP/RARP	FCoE

Frame Type	Frame Type	Frame Type	Frame Type	Frame Type
VLAN	VLAN	VLAN	VLAN	VLAN
TR	TR	TR	TR	TR
BPDU	BPDU	BPDU	BPDU	BPDU
Port Channel Lane	Port Channel Lane	Port Channel Lane	Port Channel Lane	Port Channel Lane
Flow Hash	Flow Hash	Flow Hash	Flow Hash	Flow Hash
L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA
L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA
EtherType	EtherType	EtherType	EtherType	EtherType
CoS/VL	CoS/VL	CoS/VL	CoS/VL	CoS/VL
	ToS	ToS	ARP	FCD_ID
	L4 Protocol	L4 Protocol	Request	FCS_ID
	IPv4 SA	IPv6 SA	Sender IP	SOF
	IPv4 DA	IPv6 DA	Target IP	R_CTL
				TYPE
				Cmd_Code

Exception SPAN

Exception SPAN enables you to span exception packets. Packets that have failed an intrusion detection system (IDS), Layer 3 IP verification, and FabricPath are treated as exception packets.

Note Beginning with Cisco NX-OS Release 6.2(10), you can remove the FabricPath and VLAN tag headers from SPAN packets. Use the **system default switchport monitor exclude header** and the **switchport monitor exclude header** commands. See the *Cisco Nexus 7000 Series NX-OS Security Command Reference* for more information on these commands.

An exception SPAN session is supported in either one of the two traditional bidirectional SPAN sessions or in one of the extended SPAN sessions. Rate limiters, MTU truncation, and sampling are supported in the exception SPAN session. Only the exception packets sent to the drop destination interface are supported as a SPAN source. Exception packets that are pushed to the supervisor, ACLQoS, or Layer 2 are not spanned. Each VDC supports one exception SPAN session.

Extended SPAN is supported in the egress direction only. In the case of an extended SPAN Rx session, the exception source configuration will be rejected.

Virtual SPAN Sessions

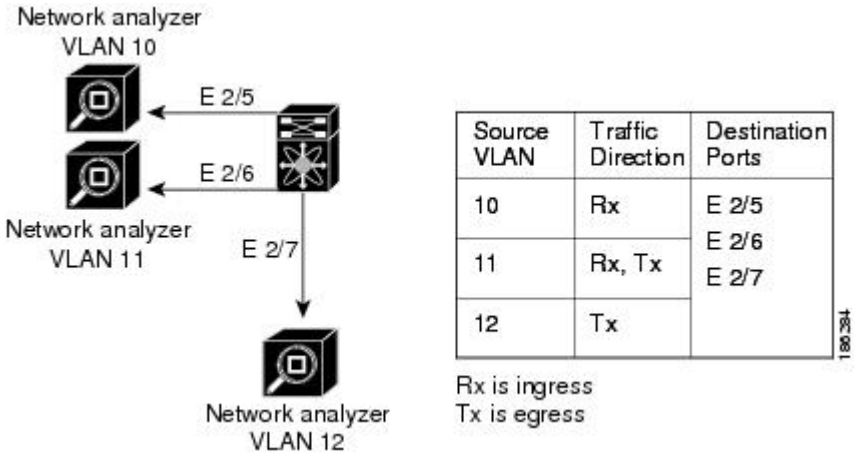
You can create a virtual SPAN session to monitor multiple VLAN sources and choose only VLANs of

interest to transmit on multiple destination ports. For example, you can configure SPAN on a trunk port and monitor traffic from different VLANs on different destination ports.

The figure below shows a virtual SPAN configuration. The virtual SPAN session copies traffic from the three VLANs to the three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it. In the figure below, the device transmits packets from one VLAN at each destination port.

Note Virtual SPAN sessions cause all source packets to be copied to all destinations, whether the packets are required at the destination or not. VLAN traffic filtering occurs at the egress destination port level.

Figure 2: Virtual SPAN Configuration



For information about configuring a virtual SPAN session see the *Configuring a Virtual SPAN Session* section.

Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor SPAN data sources for application performance, traffic analysis, and packet header analysis.

To use NAM for monitoring the Cisco Nexus 7000 SPAN data sources, see the *Cisco Nexus 7000 Series Network analysis Module (NAM-NX1) Quick Start Guide*.

High Availability

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied. For more information on high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. SPAN applies only to the VDC where the commands are entered.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for SPAN

SPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired SPAN configuration. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Guidelines and Limitations for SPAN

General SPAN Guidelines and Limitations

- For SPAN session limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.
- SPAN is not supported for management ports.
- All SPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Link Aggregation Control Protocol (LACP) Port Channel is not supported as a SPAN destination.

Note Monitor session allows LACP PO to be added as SPAN destination even though the same is not supported. This does not impact any functionality.

- A destination port can only be configured in one SPAN session at a time.
- You cannot configure a port as both a source and destination port.
- If a module is not in the VDC in which the inband interface is sourced, packets destined to the supervisor cannot be captured.
- For Cisco NX-OS releases prior to 6.1, you can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored. Beginning with Cisco NX-OS Release 6.1, the monitoring of the inband interface is no longer restricted to the default VDC:
  - Only users with the network admin privilege can add the inband interface as a SPAN source.
  - The inband interface can be added as a source from any VDC except the admin VDC, but at any time, only one VDC can have the inband interface as a source.
- Inband SPAN is treated as a shared resource. If a particular VDC does not have the resource allocated to it, inband port sourcing is rejected. Similarly, if a VDC that has the inband supervisor resource allocated to it removes the inband port from the source list of all monitor sessions, the inband resource is released from that VDC.
- For the supervisor inband interface, SPAN is supported only in the VDC in which the inband interface is sourced. If a module is part of a VDC in which the inband interface is not sourced, at least one interface

of the module must be in the VDC in which the inband interface is sourced in order to capture supervisor inband packets from this module.

- A single SPAN session can include mixed sources in any combination of the following:
  - Ethernet ports, but not subinterfaces
  - VLANs, that can be assigned to port channel subinterfaces
  - The inband interface to the control plane CPU
- When a SPAN session contains both source interfaces and source VLAN clauses, there is a possibility that other VLANs also will be spanned.
- Destination ports do not participate in any spanning tree instance. SPAN output includes bridge protocol data unit (BPDU) Spanning-Tree Protocol hello packets.
- When a SPAN session contains source ports or VLAN sources that are monitored in the transmit or transmit and receive direction, packets that these ports receive might be replicated to the SPAN destination port even though the packets are not actually transmitted on the source ports. Some examples of this behavior on source ports are as follows:
  - Traffic that results from flooding
  - Broadcast and multicast traffic
- You can enable SPAN for a source port before it becomes operationally active. Thus for Layer 2 ports, traffic flooded to the VLANs that contain these ports are captured even when the link is not connected for the ports.
- For VLAN SPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
- Beginning with Cisco NX-OS Release 6.2(2), the spanning of inband interfaces is as follows:
  - For Supervisor 1 systems, the two bidirectional traditional sessions can support an inband SPAN source.
  - For Supervisor 2 and Supervisor 2e systems, all the SPAN sessions can support an inband SPAN source.
  - Only one VDC can support inband SPAN at a time.
- You can configure an RSPAN VLAN for use only as a SPAN session source.
- You can configure a SPAN session on the local device only.
- If you span a fabricpath core interface when inter-VLAN routing is enabled across Layer 2 multi-path (L2MP), it is not possible to capture the traffic egressing out of the core interface.
- SPAN is supported on Fabric Extender interfaces in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode. Layer 3 subinterfaces are not supported.
- Cisco NX-OS does not span Link Layer Discovery Protocol (LLDP) or Link Aggregation Control Protocol (LACP) packets when the source interface is a Fabric Extender HIF (downlink) port or HIF port channel.
- SPAN sessions cannot capture packets with broadcast or multicast MAC addresses that reach the supervisor, such as ARP requests and Open Shortest Path First (OSPF) protocol hello packets, if the

source of the session is the supervisor Ethernet in-band interface. To capture these packets, you must use the physical interface as the source in the SPAN sessions.

- The rate limit percentage of a SPAN session is based on 10G, 40G, and 100G for the respective modules (that is, 1 percent corresponds to 0.1G, 0.4G, or 1G respectively), and the value is applied per every forwarding engine instance.
- Beginning with Cisco NX-OS Release 6.1, SPAN is supported for Supervisor 2.
- SPAN does not capture pause frames in a Fibre Channel over Ethernet (FCoE) network because pause frames sent from the virtual expansion (VE) port are generated and terminated by the outermost MAC layer. For more information on FCoE, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.
- On both Supervisor 1 and Supervisor 2, you cannot monitor the FCoE inband traffic.
- You can monitor both ingress and egress FCoE traffic can be monitored in a local SPAN session through Ethernet interfaces, including shared interfaces, or VLANs. For shared interfaces, you can monitor the FCoE traffic only in the storage VDC.
- The MAC in MAC (MiM) header in SPAN copies is preserved for the following SPAN destinations:
  - F2e modules with Release 6.2 or later releases.
  - F3 series modules with any Cisco NX-OS Release.
  - For F3 series modules with Release 6.2.(6a), 6.2.(6b), or 6.2(8), the Fabricpath (FP) header is preserved unconditionally. In Release 6.2.10, the FP header is preserved by default, but this behavior can changed by using the **switchport monitor exclude header** command to remove the FP or VLAN tag header for a specified SPAN destination in a VDC or the **system default switchport monitor exclude header** command to remove the FP or VLAN tag header for all destinations ports in the VDC. In Release 6.2.12, you can remove the FabricPath and VLAN tag headers using the **switchport monitor exclude header** command at the SPAN destination.
- The MiM header in SPAN copies is not preserved for the following SPAN destinations:
  - F1 and F2 series modules with any Cisco NX-OS Release.
  - F2e modules with Release 6.1(x).
  - For F3 series modules with Release 6.2.6, the FabricPath (FP) header is not preserved.

Guidelines and Limitations for F1 Series Module

- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.
- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.

- F1 Series modules are Layer 2 domain modules. Packets from Layer 3 sources can be spanned and directed to an F1 Series module SPAN destination. An F1 Series module interface cannot be configured as Layer 3, but it can receive Layer 3 traffic in a SPAN destination mode.
- When using SPAN sessions on F1 Series or F2 Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the SPAN destination interface or port channel for that session. If the SPAN source traffic exceeds the capacity of the SPAN destination, packet drops might occur on the SPAN source interfaces. This guideline does not apply to F2e, F3 or M3 Series modules.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2.

Note You cannot enable MTU truncation and the SPAN rate limit for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

- For F1 Series modules, MTU truncation on egress spanned FabricPath (core) packets has 16 fewer bytes than the configured value because the SPAN destination removes the core header. In addition, when trunk ports are used as the SPAN destination, the spanned ingress packets have 4 more bytes than the configured MTU truncation size.
- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- F1 Series modules have limited support for rule-based SPAN. They do not support IPv6 source IP and IPv6 destination IP filters. They support only IPv4 and IPv6 ToS filters with values from 0 to 3. Port channel member lane, FCoE source ID, and FCoE destination ID are not supported.

Guidelines and Limitations for F2/F2e Series Modules

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- When the supervisor inband interface is monitored in the transmit direction on F2 Series modules, a 12-byte SHIM header is inserted after SMAC in SPAN packets.

- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.

- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.
- SPAN source functionality on satellite ports and host interface port channels is not supported when the FEX is connected to F2 or F2e Series modules.
- When using SPAN sessions on F1 Series or F2 Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the SPAN destination interface or port channel for that session. If the SPAN source traffic exceeds the capacity of the SPAN destination, packet drops might occur on the SPAN source interfaces. This guideline does not apply to F2e, F3 or M3 Series modules.
- VLANs containing FEX interfaces can be a SPAN source, but the ingress traffic through the F2 Series module-based FEX ports cannot be captured.
- F2 Series modules support FEX, but they do not support FEX SPAN. Therefore, the FEX interfaces connected through the F2 Series modules cannot be made SPAN sources.
- You can span Fabric port channels on F2 Series modules.
- Layer 3 multicast egress packets cannot be spanned on F2 Series modules.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2. These features are not supported on M1 Series modules.
- For F2 Series modules, ingress FEX packets spanned through the Fabric port channel have 6 fewer bytes than the configured MTU size because the VNTag header is removed on the SPAN destination.
- For F2 Series modules, egress SPAN packets of all traffic that ingresses on Layer 2 ports (including edge-to-edge traffic) have 16 fewer bytes than the configured MTU size because a MAC-in-MAC header is added internally and removed at the SPAN destination.
- For F2, F2e, and F3 Series modules using SPAN destination port channels, SPAN traffic is distributed among the member ports. However, the distribution pattern can be different from that of regular (non-SPAN destination) port channels. For example, you can have even load distribution for regular port channels but uneven load distribution (or no load balancing) for SPAN destination port channels.
- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules. It is not supported on M Series modules.
- Beginning with Cisco NX-OS Release 6.1, FCoE SPAN on F2 Series modules is supported for storage VDCs.
- Hardware session 15 is used by NetFlow on F2 and F2e Series modules. Any extended session using this hardware ID will not span incoming traffic on the F2 and the F2e ports.

- F2 and F2e Series modules have limited support for rule-based SPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter. They do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

Guidelines and Limitations for F3 Series Module

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- SPAN sampling is supported only on F Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- Layer 3 multicast egress packets cannot be spanned on F3 Series modules.
- Prior to Cisco NX-OS Release 7.2(0)D1(1), multiple SPAN destinations are not supported when an F Series module is present in a VDC. If multiple SPAN destinations are configured in a SPAN session, the session is disabled until the F Series module is powered down or moved to another VDC or the multiple SPAN destinations are reduced to a single destination.

  Starting from Cisco NX-OS Release 7.2(0)D1(1), multiple destination SPAN sessions are supported. Only the primary destination is used to transmit SPAN packets originated from Fx modules. Traffic from M series module goes to every destination port.
- MTU truncation and the SPAN rate limit are supported on F Series and M2 Series modules and Supervisor 2.
- A FabricPath core port is not supported as a SPAN destination when an F Series module is present in a VDC. However, a FabricPath core port can be configured as a SPAN source interface.
- F3 Series modules do not support wildcards in the IPv6 source IP filters and the IPv6 destination IP filters.

Guidelines and Limitations for M1/M1XL Series Modules

- SPAN sampling is not supported on M Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels that are connected to the Cisco Nexus 2000 Series Fabric Extender as SPAN sources. However, you cannot configure them as SPAN destinations.

Note SPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. SPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender.

- If a port channel is the SPAN destination interface for SPAN traffic that is sourced from a Cisco Nexus 7000 M1 Series module, only a single member interface will receive copied source packets. The same limitation does not apply to SPAN traffic sourced from all other Cisco Nexus series modules, including the Cisco Nexus 7000 M1-XL Series modules.
- MTU truncation and the SPAN rate limit are not supported on M1 Series modules.
- Multicast best effort mode applies only to M1 Series modules.
- Extended SPAN sessions cannot source incoming traffic on M1 Series modules in either the ingress or egress direction.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- M1 Series modules and Supervisor 1 do not support rule-based SPAN. They support only VLAN filtering.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.

Guidelines and Limitations for M2/M2XL Series Modules

- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels that are connected to the Cisco Nexus 2000 Series Fabric Extender as SPAN sources. However, you cannot configure them as SPAN destinations.

Note SPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. SPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender.

- For certain rate limit and packet size values on F Series modules, M2 Series modules, and Supervisor 2, the SPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- Packets may get dropped when the ingress SPAN configured on M2 module and on any other next gen line card module such as F3, M3 having SPAN destination ports; and if the configured monitor sessions on M2 modules and its hardware session IDs (check the **show monitor resource session all** command output for hw_ssn_id) are more than 11. To overcome this issue, shut down all the SPAN sessions/unconfigure and re-configure the sessions.
- SPAN sampling is not supported on M Series modules.
- Traditional SPAN sessions support traffic from the F Series and M Series modules. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.
- For MTU truncation on M2 Series modules, the truncated length of SPAN packets is rounded down to the nearest multiplier of 16 bytes. For example, with an MTU configuration value of 65 to 79, packets are truncated to 64 bytes.

- Only eight sessions can support rate limiting on M2 Series modules. Any additional hardware sessions will not apply the configured rate limiter on M2 Series modules.
- M1 and M2 Series modules support exception SPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.

Guidelines and Limitations for M3 Series Modules

- Beginning with Cisco NX-OS Release 7.3(1)DX(1), SPAN is supported on M3 Series modules.
- SPAN sampling is supported on M Series modules and Supervisor 2.
- Extended SPAN sessions support traffic from M3 Series modules.
- If a monitor session has a source with both VLAN and a physical port, traffic may span on ports which may not be a part of the monitor session. This is applicable when M3-series I/O modules are used.

Default Settings for SPAN

The following table lists the default settings for SPAN parameters.

Parameters	Default
SPAN sessions	Created in the shut state
MTU truncation	Disabled
Multicast best effort mode	Disabled
SPAN rate limit for traditional SPAN sessions	Disabled
SPAN rate limit for extended SPAN sessions	Enabled
SPAN sampling	Disabled

Configuring SPAN

Note Cisco NX-OS commands for this feature may differ from those in Cisco IOS.

Configuring a SPAN Session

You can configure a SPAN session on the local device only. By default, SPAN sessions are created in the shut state.

For sources, you can specify Ethernet ports, port channels, the supervisor inband interface, and VLANs (ingress only).

A single SPAN session can include mixed sources in any combination of Ethernet ports, VLANs, or the inband interface to the control plane CPU. You cannot specify Ethernet port subinterfaces as sources for a SPAN session.

Note

- To use a Layer 3 port-channel subinterface as a SPAN source in the monitor session, you must specify the VLAN ID that you entered when configuring IEEE 802.1Q VLAN encapsulation for the subinterface as the filter VLAN. When you use the main interface and the SPAN VLAN filter to filter the 802.1Q VLANs on the subinterfaces, SPAN shows the traffic for all subinterfaces on the SPAN destination port.
- When VLANs containing trunk members are configured as SPAN sources, and another set of VLANs are configured as SPAN VLAN filters, then the unwanted traffic from those filter VLANs can be potentially captured.

When you specify the supervisor inband interface for a SPAN source, the device monitors all packets that arrive on the supervisor hardware (ingress).

For destination ports, you can specify Ethernet ports or port channels in either access or trunk mode. You must enable monitor mode on all destination ports.

For bidirectional traditional sessions, you can configure the sessions without specifying the direction of the traffic.

For extended SPAN sessions, you can configure the sessions in one of the following ways:

- Configure a bidirectional session by not specifying any direction when you create the session and changing the mode to extended by entering the **mode extended** command.
- Configure a unidirectional session by specifying the traffic direction when you create the session.

Before you begin

Make sure you are in the correct VDC. To switch VDCs, use the switchto vdc command.

You must have already configured the destination ports in access or trunk mode. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *interface slot*/*port*]
	Example:
	`switch(config)# interface ethernet 2/5`
	`switch(config-if)#`
		Enters interface configuration mode on the selected slot and port.

	Command or Action	Purpose

Step 3	**switchport**
	Example:
	`switch(config-if)# switchport`
	`switch(config-if)#`
		Configures switchport parameters for the selected slot and port or range of ports.

Step 4	**switchport mode** [**access** | **trunk** | **private-vlan**]
	Example:
	`switch(config-if)# switchport mode trunk`
	`switch(config-if)#`
		Configures switchport parameters for the selected slot and port or range of ports.
		• access
		• trunk
		• private-vlan

Step 5	**switchport monitor** [**ingress** [**learning**]] **Example:** `switch(config-if)# switchport monitor`	Configures the switchport interface as a SPAN destination: • **ingress**— Allows the SPAN destination port to inject packets that disrupt a certain TCP packet stream, for example, in networks with IDS. • **ingress learning**— Allows the SPAN destination port to inject packets, and allows the learning of MAC addresses, for example, the IDS MAC address.
Step 6	(Optional) Repeat Steps 2 and 3 to configure monitoring on additional SPAN destinations	—
Step 7	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

Step 8	**monitor session** *session-number* [**shut**]
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration. By default, the session is created in the shut state, and the session is a local SPAN session. The optional keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.

	Command or Action	Purpose
		• tx—Specifies an egress extended SPAN session. • shut—Specifies a shut state for the selected session.
Step 9	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session. **Note** You cannot use this command for a unidirectional SPAN session.
Step 10	**description***description* **Example:** `switch(config-monitor)# description my_span_session_3`	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.

Step 11	**source** {**interface** {**all** | *type*} | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	Example:
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	Example:
	`switch(config-monitor)# source interface port-channel 2`
	Example:
	`switch(config-monitor)# source interface sup-eth 0 both`
	Example:
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	Example:
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
	Example:
	`switch(config-monitor)# source interface all rx`
		Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender.
		You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1.
		You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both. For a unidirectional session, the direction of the source must match the direction specified in the session. Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can use the **all** keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The **all** keyword is supported only in Extended SPAN sessions.

Step 12	(Optional) Repeat Step 11 to configure all SPAN sources.	—
Step 13	(Optional) **filter vlan** {*number* | *range*} [**include-untagged**]	(Optional) Configures which VLANs to select from the configured sources. You can

	Command or Action	Purpose
	Example: `switch(config-monitor)# filter vlan 3-5, 7`	configure one or more VLANs, as either a series of comma-separated entries, or a range of numbers. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1. The include-untagged keyword applies a VLAN access map to one or more VLANs and includes untagged frames on a port with Layer 3 subinterfaces. You can enable monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in extended SPAN monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.
Step 14	(Optional) Repeat Step 13 to configure all source VLANs to filter.	—
Step 15	Required: **destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender cannot be configured as SPAN destinations.
Step 16	(Optional) Repeat Step 15 to configure all SPAN destination ports.	—
Step 17	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 18	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.

	Command or Action	Purpose
Step 19	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Multi-Destination SPAN on F2 Series Modules

If you are configuring a multiple destination port for a SPAN session on a Cisco Nexus 7000 switch, do the following:

- Remove the module type restriction when configuring multiple SPAN destination port to allow a SPAN session.
- Designate a primary destination port for VDCs with any Fx module or supervisor to activate a SPAN session.

Note The primary destination configuration does not impact transmission of SPAN packets originating from the M-series module; the primary destination has be active for the SPAN session to be activated.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

Before you begin

Multiple destination SPAN sessions were not supported in VDCs with F–series modules (F1/F2/F2E/F3), and hence even if the sessions were configured, they were not enabled in the VDCs. Starting from Cisco NX-OS Release 7.2, multiple destination SPAN sessions are supported. The primary destination is used to transmit SPAN packets originated from Fx modules.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switch to vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

	Command or Action	Purpose

Step 3	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 4 rx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration, which specifies the SPAN session for which the source rate limit is to be configured. By default, the session is created in the shut state, and the session is a local SPAN session.

Step 4	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] **Example:** `switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`	Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, or a range of VLANs. You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both. **Note** Source VLANs are supported only in the ingress (rx) direction.
Step 5	(Optional) Repeat Step 4 to configure all virtual SPAN VLAN sources.	—
Step 6	Required: **destination interface** *type* {*number* | *range*} [primary] **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. However, only one such primary port can be configured in a session. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.
Step 7	Required: **no rate-limit** **Example:** `switch(config-monitor)# no rate limit`	Sets the rate limit for the SPAN traffic.
Step 8	Required: **no destination interface** *type* {*number* | *range*} [primary] **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	Checks the configuration to ensure that the primary attribute is not configured on the destination port. Displays an error message if more than one port is configured. **Note** ERROR: Cannot configure more than one "Primary" destination port in a session.

	Command or Action	Purpose
Step 9	(Optional) Repeat Step 12 to configure all source VLANs to filter.	—
Step 10	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 11	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Multiple SPAN Sessions on a SPAN Destination Port

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switch to vdc** command).

Before you begin

With the introduction of multiple SPAN sessions, it is important to share the destination interface across multiple SPAN sessions, which not only reduce the N7K hardware cost of the SPAN sessions and the traffic monitoring equipment, it can also simplify the overall network connections.

- Rate limiter 'auto' mode is not allowed with span session(s) having shared span destination port(s).
- The 'manual' mode is recommended when the rate limit is required for individual SPAN session.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*[*session-type*]
	Example:
	`switch(config)# monitor session 3 span`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies a SPAN session.

	Command or Action	Purpose
Step 3	Required: **destination interface** {**ethernet x/y** | **port-channel z**} **Example:** `switch(config-monitor)# destination interface ethernet1/2`	(Optional) Specifies the option to add a destination port. **Note** Rate limit auto should be disabled for sharing SPAN destination ports across multiple sessions. However, if the rate limit auto is enabled for a destination port and the destination port is already used in any other SPAN session, there will be a request to disable the auto mode first.
Step 4	Required: **no rate-limit** {**auto** | **rate-value**} **Example:** `switch(config-monitor-local)# no rate-limit auto`	(Optional) Enables the rate limit. **Note** Auto rate limit should be disabled for sharing SPAN destination ports across multiple sessions. If a shared destination port is configured in the span session, the CLI gets rejected until you remove the shared destination port.

Configuring a Virtual SPAN Session

You can configure a virtual SPAN session to copy packets from source ports, VLANs, and RSPAN VLANs to destination ports on the local device. By default, SPAN sessions are created in the shut state.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

You have already configured the destination ports in trunk mode. For more information, see the Cisco

Nexus 7000 Series NX-OS Interfaces Configuration Guide.

You have already configured the destination ports to monitor a SPAN session with the **switchport monitor** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**no monitor session** *session-number* **Example:** `switch(config)# no monitor session 3`	Clears the configuration of the specified SPAN session. The new session configuration is added to the existing session configuration.

Step 3	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
	Example:
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration. By default, the session is created in the shut state, and the session is a local SPAN session. The optional keyword shut specifies a shut state for the selected session.

Step 4	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	Example:
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	Example:
	`switch(config-monitor)# source interface port-channel 2`
	Example:
	`switch(config-monitor)# source interface sup-eth 0 both`
	Example:
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	Example:
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
		Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, or a range of VLANs.
		You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces.
		You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both.
		Note Source VLANs are supported only in the ingress (rx) direction.
		For a unidirectional session, the direction of the source must match the direction specified in the session.

Step 5	(Optional) Repeat Step 4 to configure all virtual SPAN VLAN sources.	—
Step 6	Required: **destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.
Step 7	(Optional) Repeat Step 12 to configure all source VLANs to filter.	—

	Command or Action	Purpose
Step 8	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 9	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 10	Required: **interface ethernet** *slot/port [port]* **Example:** `switch(config)# interface ethernet 2/5 switch(config-if)#`	Enters interface configuration mode on the selected slot and port or range of ports.
Step 11	(Optional) **switchport trunk allowed vlan** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Configures the range of VLANs that are allowed on the interface. You can add to or remove from the existing VLANs, you can select all VLANs except those VLANs that you specify, or you can select all or none of the VLANs. By default, all VLANs are allowed on the interface. You can configure one or more VLANs as either a series of comma-separated entries or a range of numbers. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1.
Step 12	(Optional) Repeat Steps 10 and 11 to configure the allowed VLANs on each destination port.	
Step 13	(Optional) **show interface ethernet** **Example:** `switch(config)# interface ethernet 2/5 switch(config-if)#`	(Optional) Displays the interface trunking configuration for the selected slot and port or range of ports.
Step 14	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring an RSPAN VLAN

You can specify a remote SPAN (RSPAN) VLAN as a SPAN session source.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vlan** *vlan*
	Example:
	`switch(config)# vlan 901`
	`switch(config-vlan)#`
		Enters VLAN configuration mode for the VLAN specified.

Step 3	**remote-span** **Example:** `switch(config-vlan)# remote-span`	Configures the VLAN as an RSPAN VLAN.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits VLAN configuration mode.

Step 5	(Optional) **show vlan** **Example:** `switch(config)# show vlan`	(Optional) Displays the VLAN configuration. Remote SPAN VLANs are listed together.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Shutting Down or Resuming a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, SPAN sessions are created in the shut state.

You can resume (enable) SPAN sessions to resume the copying of packets from sources to destinations. In order to enable a SPAN session that is already enabled but operationally down, you must first shut it down and then enable it.

You can configure the shut and enabled SPAN session states with either a global or monitor configuration mode command.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **monitor session** {*session-range* | **all**} **shut** **Example:** `switch(config)# monitor session 3 shut`	Shuts down the specified SPAN sessions. By default, sessions are created in the shut state. The **no** form of the command resumes (enables) the specified SPAN sessions. By default, sessions are created in the shut state. **Note** If a monitor session is enabled but its operational status is down, to enable the session, you must first specify the **monitor session shut** command followed by the **no monitor session shut** command.

Step 3	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration.

Step 4	[**no**] **shut** **Example:** `switch(config-monitor)# shut`	Shuts down the SPAN session. By default, the session is created in the shut state. The **no** form of the command enables the SPAN session. By default, the session is created in the shut state.
Step 5	(Optional) **show monitor** **Example:** `switch(config-monitor)# show monitor`	Displays the status of SPAN sessions.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MTU Truncation for Each SPAN Session

To reduce the SPAN traffic bandwidth, you can configure the maximum bytes allowed for each replicated packet in a SPAN session. This value is called the maximum transmission unit (MTU) truncation size. Any SPAN packet larger than the configured size is truncated to the configured size.

Note MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

Note MTU truncation and SPAN sampling can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (size versus packet count).

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the MTU truncation size is to be configured.

Step 3	Required: **[no] mtu***mtu* **Example:** `switch(config-monitor)# mtu 64`	Configures the MTU truncation size for packets in the specified SPAN session. The range is from 64 to 1500 bytes.

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of MTU truncation, the maximum bytes allowed for each packet per session, and the modules on which MTU truncation is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a Source Rate Limit for Each SPAN Session

When a SPAN session is configured with multiple interfaces or VLANs as the sources in a high-traffic environment, the destination port can be overloaded, causing the normal data traffic to be disrupted at the source port. You can alleviate this problem as well as traffic overload on the source forwarding instance by configuring a source rate limit for each SPAN session.

Note MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session on F1 Series modules. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

Note SPAN sampling takes precedence over SPAN source rate limiting. Rate limiting takes effect after sampling is completed on SPAN source packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the source rate limit is to be configured.

Step 3	Required: **[no] rate-limit {auto** | *rate-limit*} **Example:** `switch(config-monitor)# rate-limit auto`	Configures the source rate limit for SPAN packets in the specified SPAN session in automatic or manual: • Auto mode—Automatically calculates the rate limit on a per-gigabyte basis as follows: destination bandwidth / aggregate source bandwidth. For example, if the rate limit per gigabyte is 0.5, for every 1G of source traffic, only 0.5G of packets are spanned. For ingress traffic, the per-gigabyte limit is applied to each forwarding engine of the F Series module based on how many ports

	Command or Action	Purpose
		are used as the SPAN source so that the source can be spanned at the maximum available bandwidth. For egress traffic, the per-gigabyte limit is applied to each forwarding engine of the F Series module without considering how many ports are used as the SPAN source. • Manual mode—Specifies the percentage of the maximum rate of SPAN packets that can be sent out from each forwarding engine on a module. The range is from 1 to 100. For example, if the rate limit is 10 percent, the maximum rate of SPAN packets that can be sent out from each of the forwarding engines on an F Series module is 1G (or 10 percent of the 10G line rate).

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Sampling for Each SPAN Session

Beginning with Cisco NX-OS Release 6.1, you can configure a sampling range for spanned traffic in order to reduce the SPAN traffic bandwidth and to monitor peer-to-peer traffic. Packet range-based sampling is used to provide an accurate count of the SPAN source packets.

Note Sampling and MTU truncation can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (packet count versus size). However, sampling takes precedence over SPAN source rate limiting. Rate limiting takes effect after sampling is completed on SPAN source packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`	

Step 3	**monitor session** *session-number* [*rt* | *tx*] [*shut*] **Example:** `switch(config-monitor)# sampling 100`	Configures the sampling range for SPAN source packets. The sampling value is the range in which one packet out of x packets will be spanned, where x is from 2 to 1023. In this example, 1 out of every 100 packets will be spanned.
Step 4	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the status of SPAN sessions, including the configuration status of SPAN sampling, the sampling value, and the modules on which sampling is and is not supported.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Complex Rule-based SPAN

Before you begin

Complex filter rules can be created with multiple filters and product table resources. A few keywords, **Match**, **Permit**, **Deny** and **Filter-list** have been introduced in this release. The "Match" keyword helps to match on the fields and values set by the user. "Permit" keyword followed by the filter names allow a SPAN copy to be generated if all filters are hit. "Deny" keyword followed by the filter names allow a SPAN copy to be generated if all the filters are missed. "Filter-list" is a keyword that specifies all the rules defined by the permit and deny keywords.

Note Each filter list can contain multiple 'permit-deny' rules.

Creating Filters

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor filter***filter-name*
	Example:
	`switch(config)# monitor filter test-filter`
	`switch(config-monitor-filter)#`
		Enters the monitor filter configuration mode.
		Note The length of the string should not exceed 32 characters.

Step 3	**match** [**eth-type** *eth-type* | **src-mac** *mac-address mac-mask* | **dest-mac** *mac-address mac-mask* | **frame-type** *[arp* | *eth* | *fcoe* |*ipv4* |*ipv6*]
	Example:
	`switch(config-monitor-filter)# match eth-type 0x0800`
	`switch(config-monitor-filter)# match src-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00 dest-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00`
		Match specific fields in the packet under monitor filter configuration mode.
		Note Specifying match criteria in the same line or in multiple lines will have the same result.

Creating Filter-Lists

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor filter-list***filter-list-name* **Example:**	Enters the monitor filter configuration mode. **Note** The length of the string should not exceed 32 characters.

	Command or Action	Purpose
	`switch(config)# monitor filter-list sample-filter-list` `switch(config-monitor-filter-list)#`	

Step 3	**permit filter** *filter-names* **deny filter***filter-names*
	Example:
	`switch(config-monitor-filter-list)# permit filter test-filter deny filter test-filter1`
	`switch(config-monitor-filter-list)#`
	
	`switch(config-monitor-filter-list)# permit filter test-filter2`
	`switch(config-monitor-filter-list)#`
	
	`switch(config-monitor-filter-list)# deny filter test-filter3`
	`switch(config-monitor-filter-list)#`
		Use this command to permit and/or deny filters within the filter-list.
		Note
		• When the command **permit filter** *filter-names* **deny filter***filter-names* is specified in the same line, the rule matches all permit and deny criteria, where packets matching filter x and filter y in permit filter X and deny filter Y are SPAN-ed—this is an AND condition.
		• When the command **permit filter** *filter-names* **deny filter***filter-names* is specified in separate lines, the rule matches either permit or deny criteria, where packets match filter x OR filter y in permit filter X and deny filter Y are SPAN-ed—it is an OR condition.

Associating a Filter List to a Monitor Session

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Note If you want to attach a complex filter to a SPAN session, ensure that there are no filters already attached to the SPAN session.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**monitor session** *session-number* [*rt* | *tx*]
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)# filter filter-list sample-filter-list`
		Enters the monitor configuration mode and specifies the SPAN session. The optional keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.
		• tx—Specifies an egress extended SPAN session.
		Note • If you are attaching a filter-list to a SPAN session on a Cisco Nexus 7000 series switch, then the **mode extended** command should be specified within the SPAN session.
		• The direction of the filter is derived from the SPAN session direction.

Step 3	**exit** **Example:** `switch(config-monitor)# exit`	Returns to the global configuration mode.

Configuring a Session with Rules Enabled

To create a local/erspan-source unidirectional/bidirectional session, configure the following:

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [*rt* | *tx*] [*shut*]
	Example:
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
		Enters the monitor configuration mode to configure a local SPAN/ERSPAN session. The optional keywords are as follows:
		• rx—Specifies an ingress extended SPAN session.
		• tx—Specifies an egress extended SPAN session.
		• shut—Specifies a shut state for the selected session.

	Command or Action	Purpose
Step 3	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Changes mode to extended mode for bidirectional sessions.
Step 4	**filter frame-type source-ip src-ip** **Example:** `switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.3/32 cos 3`	Associates the rule-based filters to the session.

Step 5	Required: **source interface ethernet x/y**
	Example:
	`switch(conf-monitor)# source interface Ethernet 4/7`
	`switch(conf-monitor)# destination interface Ethernet 4/7`
		Associates the source port and the destination port.

Step 6	Required: **no shut** **Example:** `switch(config-monitor)# no shut`	Brings up the session. **Note** Filter command can be split into separate lines and configured under the session mode. All the filters specified under a session will be under the AND rule.

Configuring the Multicast Best Effort Mode for a SPAN Session

You can configure the multicast best effort mode for any SPAN session. By default, SPAN replication occurs on both the ingress and egress modules. When you enable the multicast best effort mode, SPAN replication occurs only on the ingress module for multicast traffic or on the egress module for packets that egress out of Layer 3 interfaces (that is, on the egress module, packets that egress out of Layer 2 interfaces are not replicated for SPAN).

Note For Layer 3 multicast traffic, SPAN replication occurs on the egress module. If traffic is multicasted to multiple egress modules, you could capture multiple SPAN copies for each packet (that is, one copy from each egress module).

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session for which the source rate limit is to be configured.

Step 3	Required: **[no] multicast best-effort** **Example:** `switch(config-monitor)# multicast best-effort`	Configures the multicast best effort mode for the specified SPAN session.

Step 4	**show monitor session** *session-number*
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Rule-Based SPAN

You can configure filters for ingress or egress SPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [**shut**]
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode. The new session configuration is added to the existing session configuration. By default, the session is created in the shut state, and the session is a local SPAN session. The optional keywords are as follows:

	Command or Action	Purpose
		• **rx**—Specifies an ingress extended SPAN session. • **tx**—Specifies an egress extended SPAN session. • **shut**—Specifies a shut state for the selected session.
Step 3	**mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session.

Step 4	[**no**] **filter**[*vlan-range*] [**bpdu** [**true** | **false**]] [**cos** *cos-value*] [**dest-mac***dest-mac*] [**eth-type** *eth-value*] [**flow-hash** *flow-value*] [**frame-type** [**eth** | **arp** | **fcoe** | **ipv4** | **ipv6**]] [**pc-lane** *port-number*] [**src_mac** *mac-address*] [**trace-route** [**true** | **false**]]
	Example:
	`switch(config-monitor)# filter vlan 10,20`
	`switch(config-monitor)# filter frame-type arp trace-route true`
	`switch(config-monitor)# filter bpdu false`
		Configures the filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows:
		• **vlan**—Specifies a filter based on a VLAN range.
		• **bpdu**—Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
		• **cos**—Specifies a filter based on the class of service (CoS) in the dotlq header.
		• **dest-mac**—Specifies a filter based on a destination MAC address.
		• **eth-type**—Specifies a filter based on the Ethernet type.
		• **flow-hash**—Specifies a filter based on the result bundle hash (RBH) value.
		• **frame-type**—Specifies a filter based on a frame type.
		• **pc-lane**—Specifies a filter based on a member of the port channel.
		• **src-mac**—Specifies a filter based on a source MAC address.
		• **trace-route**—Specifies a filter based on the route bit in the header.

Step 5	(Optional) [**no**]**filter frame-type eth** **Example:**	(Optional) Configures the Ethernet frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command.

	Command or Action	Purpose
	`switch(config-monitor)# filter frame-type eth`	
Step 6	(Optional) [**no**]**filter frame-type arp** [[**arp-rarp** [**arp** | **rarp**]] [**req-resp** [**req** | **rsp**]] [**sender-ip** *ip-address*] [**target-ip** *ip-address*]] **Example:** `switch(config-monitor)# filter frame-type arp arp-rarp arp`	(Optional) Configures the ARP frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **arp-rarp**—Specifies an ARP or RARP frame type filter. • **req-resp**—Specifies a filter based on a request or response. • **sender-ip**—Specifies a filter based on a sender IP address. • **target-ip**—Specifies a filter based on a target IP address.
Step 7	(Optional) [**no**]**filter frame-type fcoe fcoe** [[**fc-sid** *FC-source-ID*] [**fc-did** *FC-dest-ID*] [**fcoe-type** *fcoe-value*] [**r-ctl** *r-ctl-value*] [**sof** *sof-value*] [**cmd-code** *cmd-value*]] **Example:** `switch(config-monitor)# filter frame-type fcoe`	(Optional) Configures the FCoE frame type filter for the SPAN session. To remove the filter from the session, enter the **no** form of the command. The optional keywords are as follows: • **fc-sid**—Specifies a filter based on an FC source ID. • **fc-did**—Specifies a filter based on an FC destination ID. • **fcoe-type**—Specifies a filter based on an FCoE type. • **r-ctl**—Specifies a filter based on the routing control flags (R CTL) value. • **sof**—Specifies a filter based on the start of frame (SOF) packets. • **cmd-code**—Specifies a filter based on a command code.
Step 8	(Optional) [**no**]**filter frame-type ipv4** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** tos-value] [**l4-protocol** *l4-value*]] **Example:** `switch(config-monitor)# filter frame-type ipv4 l4-protocol 3`	(Optional) Configures the IPv4 frame type filter for the SPAN session. To remove the filter from the session, enter the no form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv4 source IP address.

	Command or Action	Purpose
		• **dest-ip**—Specifies a filter based on an IPv4 destination IP address. • **tos**—Specifies a filter based on the type of service (TOS) in the IP header. • **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 9	(Optional) [**no**]**filter frame-type ipv6** [[**src-ip** *src-ip*] [**dest-ip** *dest-ip*] [**tos** tos-value] [**l4-protocol** *l4-value*]] **Example:** `switch(config-monitor)# filter frame-type ipv6 src-ip 10.0.0.1`	(Optional) Configures the IPv6 frame type filter for the SPAN session. To remove the filter from the session, enter the no form of the command. The optional keywords are as follows: • **src-ip**—Specifies a filter based on an IPv6 source IP address. • **dest-ip**—Specifies a filter based on an IPv4 destination IP address. • **tos**—Specifies a filter based on the type of service (TOS) in the IP header. • **l4-protocol**—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.
Step 10	(Optional) Repeat Steps 4 to 9 for all filters for the session.	
Step 11	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] **Example:** `switch# configure terminal switch(config)#`	(Optional) Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1. You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both.

	Command or Action	Purpose
		For a unidirectional session, the direction of the source must match the direction specified in the session.
Step 12	**destination interface** *type* {*number* | *range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports. **Note** The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as SPAN destinations.
Step 13	**no shut** **Example:** `switch(config-monitor)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 14	(Optional) **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **Example:** `switch(config-monitor)# show monitor session 3`	Displays the SPAN configuration.
Step 15	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Exception SPAN

You can configure the device to span exception packets.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session-number* [**rx**|**tx**| **both**]
	Example:
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		Enters the monitor configuration mode and specifies the SPAN session. The optional keywords are as follows:.
		• **rx**—Specifies an ingress extended SPAN session.
		• **tx**—Specifies an egress extended SPAN session.
		• **shut**—Specifies a shut state for the selected session.

Step 3	(Optional) **mode extended** **Example:** `switch(config-monitor)# mode extended`	(Optional) Configures the SPAN session as an extended bidirectional session form of the command.
Step 4	(Optional) [**source exception**{**layer3**|**fabricpath**|**other** | **all**} **Example:** `switch(config-monitor)# filter frame-type eth`	Configures the source as an exception SPAN session. These exception types are supported: • **layer3**—Specifies the Layer 3 exception type. • **fabricpath**—Specifies the FabricPath exception type. • **other**—Specifies other exceptions that are dropped through redirect registers programmed with a drop destination interface. • **all**—Includes all Layer 3, FabricPath, and other exceptions.
Step 5	**destination interface** *type [number |range*} **Example:** `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	Configures destinations for copied source packets. You can configure one or more destinations as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. **Note** SPAN destination ports must be either access or trunk ports.

	Command or Action	Purpose
		Note The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as SPAN destinations.
Step 6	**no shut** **Example:** `switch(config)# no shut`	Enables the SPAN session. By default, the session is created in the shut state.
Step 7	**show monitor session** *session-number* **Example:** `switch(config)# show monitor session 3`	(Optional) Displays the status of SPAN sessions, including the configuration status of the rate limit, the percentage of the maximum SPAN rate allowed per session, and the modules on which the rate limit is and is not supported.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Removing FabricPath and VNTAG Headers

If you are working with a device connected to a SPAN destination port that does not understand FabricPath or VNTAG headers, you may want those headers stripped from the packet.

You can do this at either the global or port level. If you want to strip the headers to all SPAN destination ports in the VDC, you can apply the global command. If you want to apply the command only to a certain port, you can use the port-level command. If the ports are not SPAN destination ports, the command is rejected.

When you enter both the global and port-level configurations for this feature, the port-level overrides the global configuration.

Note The port-level command overrides the global command. So you can configure the device to strip the headers globally and then issue the no form of the port-level command to exclude the specified ports from stripping the headers.

Removing Headers Globally

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system default switchport monitor exclude header**	Removes the FabricPath and VNTAG headers for all SPAN destination ports in the VDC. Use the **no** form of the command to preserve the headers on packets for SPAN destination ports.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Removing Headers per Port

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type* {*module* | *port*}	Enters the interface mode and specifies the port or ports from which you want to remove the FabricPath and VNTAG headers.
Step 3	(Optional) switch(config)# [**no**]**switchport monitor exclude header**	Removes the FabricPath and VNTAG headers for the specified SPAN destination ports in the VDC. Use the **no** form of the command to preserve the headers on packets for SPAN destination ports.
Step 4	(Optional) switch(config)# **exit**	Returns to global configuration mode.
Step 5	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Verifying the SPAN Configuration

To display the SPAN configuration, perform one of the following tasks:

Command	Purpose
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the SPAN session configuration.

Command	Purpose
show resource monitor-session	Displays the resources that are available for the traditional sessions.
show resource monitor-session-extended	Displays the resources that are available for the extended session.
show running-config	Displays configuration of the commands for removing the FabricPath and VNTAG headers for SPAN.

Configuration Examples for SPAN

Configuration Example for a SPAN Session

To configure a SPAN session, follow these steps:

Procedure

Step 1 Configure destination ports in access mode and enable SPAN monitoring.

Example:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

Step 2 Configure a SPAN session.

Example:

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

Configuration Example to Monitor All VLANs and Ports in an Extended SPAN Monitor Session

Example

This example shows how to monitor all VLANs and ports in an Extended SPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

This example shows how to monitor a higher number of specific VLAN sources than the VLAN source limits currently supported in the extended SPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# destination interface ethernet 4/1
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
switch(config)# copy running-config startup-config
```

Configuration Example for a Unidirectional SPAN Session

To configure a unidirectional SPAN session, follow these steps:

Procedure

Step 1 Configure destination ports in access mode and enable SPAN monitoring.

Example:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

Step 2 Configure a SPAN session.

Example:

```
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
```

```
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

Configuration Example for a Virtual SPAN Session

Procedure

Step 1 Configure destination ports in access or trunk mode, and enable SPAN monitoring.

Example:

```
switch# configure terminal
 switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 100-200
  switch(config-if)# switchport monitor
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config)# interface ethernet 3/2
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 201-300
  switch(config-if)# switchport monitor
  switch(config-if)# no shut
 switch(config-if)# exit
switch(config)#
```

Step 2 Configure a SPAN session.

Example:

```
switch(config)# no monitor session 4
switch(config)# monitor session 4tx
  switch(config-monitor)# source vlan 100-300
  switch(config-monitor)# destination interface ethernet 3/1-2
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# show monitor session 4
switch(config)# copy running-config startup-config
```

Configuration Example for a SPAN Session with a Private VLAN Source

To configure a SPAN session that includes a private VLAN source, follow these steps:

Procedure

Step 1 Configure source VLANs.

Example:

```
switch# configure terminal
  switch(config)# vlan 100
    switch(config-vlan)# private-vlan primary
    switch(config-vlan)# exit
    switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)# interface ethernet 3/2
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk native vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

Step 2 Configure destination ports in access or trunk mode, and enable SPAN monitoring.

Example:

```
switch# configure terminal
  switch(config)# interface ethernet 3/3
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk allowed vlan add 100-200
  switch(config-if)# switchport monitor
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

Step 3 Configure a SPAN session.

Example:

```
switch# no monitor session 3
switch(config)# monitor session 3
  switch(config-if)# source vlan 100
  switch(config-if)# destination interface ethernet 3/3
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config-if)# show monitor session 3
switch(config-if)# copy running-config startup-config
```

Configuration Example for SPAN with MTU Truncation and SPAN Sampling

Example

This example shows how to configure MTU truncation and SPAN sampling for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mtu 100
switch(config-monitor)# sampling 10
switch(config-monitor)# show monitor session 3
```

Configuration Example for Rule-Based SPAN

Example

This example shows how to configure a rule-based SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

Configuration Example for Exception SPAN

Example

This example shows how to configure a SPAN session to span exception packets:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# source exception all
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

Related Documents

Table 2: Related Documents

Related Topic	Document Title
Cisco Network Analysis Module (NAM)	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*

VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Fabric Extender	*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*
SPAN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*

Feature History for SPAN

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 3: Feature History for SPAN

Feature Name	Releases	Feature Information
SPAN	7.3(0)DX(1)	Added support for M3 Series modules.
SPAN	7.3(0)D1(1)	Added support for 4K VLANs per SPAN Session.
SPAN	6.2(10)	Added support to remove FabricPath and VLAN tag headers from SPAN packets.
SPAN	6.2(2)	Added NAM support for SPAN data sources.
SPAN	6.2(2)	Added support for FEX ports as a SPAN source in the Tx direction only on F2e Series modules
SPAN	6.2(2)	Added support for extended SPAN.
SPAN	6.2(2)	Added support for rule-based SPAN.
SPAN	6.2(2)	Added support for exception SPAN.
SPAN	6.1(1)	Added support for SPAN sampling.
SPAN	6.1(1)	Allowed the inband interface to be added as a source from any VDC except the admin VDC.
SPAN	6.1(1)	Added support for Supervisor 2.
SPAN	6.1(1)	Added support for M2 Series modules.

SPAN	6.1(1)	Added FCoE SPAN support on F2 Series modules for storage VDCs.
SPAN	6.0(1)	Added support for F2 Series modules.
SPAN	5.2(1)	Added SPAN source support for Cisco Nexus 2000 Series Fabric Extender interfaces.
SPAN	5.2(1)	Added the ability to configure MTU truncation, the source rate limit, and the multicast best effort mode for each SPAN session.
SPAN	5.1(1)	Added support for F1 Series modules and increased the number of supported SPAN sessions from 18 to 48.
SPAN	4.1(3)	Added a table of SPAN session limits.