Configuring SPAN

This chapter contains the following sections:

Information About SPAN

The Switched Port Analyzer (SPAN) feature (sometimes called port mirroring or port monitoring) selects network traffic for analysis by a network analyzer. The network analyzer can be a Cisco SwitchProbe, a Fibre Channel Analyzer, or other Remote Monitoring (RMON) probes.

SPAN Sources

SPAN sources refer to the interfaces from which traffic can be monitored. The Cisco Nexus device supports Ethernet, Fibre Channel, virtual Fibre Channel, port channels, SAN port channels, VSANs and VLANs as SPAN sources. With VLANs or VSANs, all supported interfaces in the specified VLAN or VSAN are included as SPAN sources. You can choose the SPAN traffic in the ingress direction, the egress direction, or both directions for Ethernet, Fibre Channel, and virtual Fibre Channel source interfaces:

- Ingress source (Rx)—Traffic entering the device through this source port is copied to the SPAN destination port.
- Egress source (Tx)—Traffic exiting the device through this source port is copied to the SPAN destination port.

Note Fibre Channel ports and VSAN ports cannot be configured as ingress source ports in a SPAN session.

Characteristics of Source Ports

A source port, also called a monitored port, is a switched interface that you monitor for network traffic analysis. The switch supports any number of ingress source ports (up to the maximum number of available ports on the switch) and any number of source VLANs or VSANs.

A source port has these characteristics:

- Can be of Ethernet, Fibre Channel, virtual Fibre Channel, port channel, SAN port channel, VSAN or VLAN port type.
- Cannot be a destination port.
- Can be configured with a direction (ingress, egress, or both) to monitor. For VLAN and VSAN sources, the monitored direction can only be ingress and applies to all physical ports in the group. The RX/TX option is not available for VLAN or VSAN SPAN sessions.
- There is no limit to the number of egress SPAN ports, but there is upper limit of 128 source ports in the monitor session.
- Port Channel and SAN Port Channel interfaces can be configured as ingress or egress source ports.
- Can be in the same or different VLANs or VSANs.
- For VLAN or VSAN SPAN sources, all active ports in the source VLAN or VSAN are included as source ports.

SPAN Destinations

SPAN destinations refer to the interfaces that monitors source ports. The Cisco Nexus Series device supports Ethernet and Fibre Channel interfaces as SPAN destinations.

Starting with Cisco NX-OS Release 7.2(0)N1(1), HIF and virtual ethernet (Veth) ports as SPAN destination is supported.

Source SPAN	Dest SPAN
Ethernet	Ethernet
Fibre Channel	Fibre Channel
Fibre Channel	Ethernet (FCoE)
Virtual Fibre Channel	Fibre Channel
Virtual Fibre Channel	Ethernet (FCoE)

Characteristics of Destination Ports

Each local SPAN session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports, VSANs, or VLANs. A destination port has these characteristics:

- Can be any physical port. Source Ethernet, FCoE, and Fibre Channel ports cannot be destination ports.
- Cannot be a source port.
- Cannot be a port channel or SAN port channel group.
- Does not participate in spanning tree while the SPAN session is active.
- Is excluded from the source list and is not monitored if it belongs to a source VLAN of any SPAN session.
- Receives copies of sent and received traffic for all monitored source ports.

SPAN with ACL

The SPAN with ACL filtering feature allows you to filter SPAN traffic so that you can reduce bandwidth congestion. To configure SPAN with ACL filtering, you use ACL's for the session to filter out traffic that you do not want to span. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in spanning only the traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter can apply to all sources in the session.

Guidelines and Limitations for SPAN

- The **switchport monitor rate-limit interface** command is not applicable on the Nexus 5500 device. The rate limit for SPAN traffic takes place at the SPAN source port on a Nexus 5500 device. Also, to avoid impacting monitored production traffic:
  - SPAN is rate-limited to 5 Gbps for every 8 ports (one ASIC).
  - RX-SPAN is rate-limited to 0.71 Gbps per port when the RX-traffic on the port exceeds 5 Gbps.
- The switch supports four active SPAN sessions. When you configure more than two SPAN sessions, the first two sessions are active. During startup, the order of active sessions is reversed; the last two sessions are active. For example, if you configured ten sessions 1 to 10 where 1 and 2 are active, after a reboot, sessions 9 and 10 will be active. To enable deterministic behavior, explicitly suspend sessions 3 to 10 with the **monitor session** *session-number* **shut** comma

The following limitations apply to SPAN (local SPAN) session Access Control Lists (ACL) configurations:

- Due to system limitations, the extent to which an ACL associated to SPAN session can scale depends on the how the SPAN source is configured. The following table shows different scenarios and the corresponding maximum ACL size supported.

Note These calculations assume that each ACE in the ACL results in one final TCAM entry.

Scenario	Maximum ACL Size
SPAN has single Switch Port as source with both Tx and Rx.	Current Available TCAM Entries/2
SPAN has multiple Switch Ports as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has Port Channel (with one or more member switch ports) as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has single HIF Ports as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has multiple HIF Ports as source with both Tx and Rx.	Current Available TCAM Entries/4
SPAN has HIF Port Channel (with one or more member HIF ports) as source with both Tx and Rx.	Current Available TCAM Entries/4

- The following scenarios are unaffected by any system limitations for ACL and SPAN session scaling:
  - SPAN has single Switch Port as source with Tx only.
  - SPAN has multiple Switch Ports as source with Tx only.

- SPAN has a Port Channel (with one or more member switch ports) as source with Tx only.
- SPAN has a single Host Interface (HIF) Port as source with Tx only.
- SPAN has multiple HIF Ports as source with Tx only.
- SPAN has a single Port HIF Channel (with one or more member HIF ports) as source with Tx only.
- SPAN has a single Switch Port as source with Rx only.
- SPAN has multiple Switch Ports as source with Rx only.
- SPAN has a Port Channel (with one or more member switch ports) as source with Rx only.
- SPAN has a single HIF Ports as source with with Rx only.
- SPAN has multiple HIF Ports as source with Rx only.
- SPAN has a HIF Port Channel (with one or more member HIF ports) as source with Rx only

- The following guidelines apply when configuring local SPAN sessions with ACLs:
  - When you associate an ACL with a SPAN session, you must ensure that its size is not greater than the calculations given in the table above. Otherwise the SPAN session fails and generate a "TCAM resource unavailable" error. If the ACL has Layer 4 Operations and TCAM resource expansion is enabled, you need to know the expected expanded size and you need to use the expanded size to calculate the maximum ACL size.
  - If you change the ACL that is attached to a SPAN session, the ACL size can exceed the maximum ACL size allowed. In this scenario, the SPAN session continues to work with the modified ACL. However, you should undo the ACEs added to the ACL to limit the size to maximum allowed ACL size.
  - If you add a SPAN session when one already exists, then to modify the first span session there should be free TCAM entries of size equal to number of ACEs in the associated ACL (Assuming that each ACE requires one TCAM entry. If it gets expanded, the expanded size should be considered). Therefore, TCAM entries consumed by the second SPAN session should be released.
  - To replace a large ACL with another large ACL (which could cause the SPAN session to enter a generic error state), you must first remove the existing filter access group (using the **no filter access-group** *current acl name* command), and then configure the new filter access group (using the **filter access-group** *new acl name* command).
- Local SPAN/SPAN on Drop/SPAN on Latency is not aware of VPC.
- The following is the limitation for HIF and Virtual Ethernet (Veth) as SPAN destination:
  - Multi-destination SPAN is not supported. If HIF/VETH port is a destination, the monitor session must have single destination.

Creating or Deleting a SPAN Session

You create a SPAN session by assigning a session number using the **monitor session** command. If the session already exists, any additional configuration information is added to the existing session.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number*	Enters the monitor configuration mode. New session configuration is added to the existing session configuration.

The following example shows how to configure a SPAN monitor session:

```
switch# configure terminal
switch(config) # monitor session 2
switch(config) #
```

Configuring an Ethernet Destination Port

You can configure an Ethernet interface as a SPAN destination port.

Note The SPAN destination port can only be a physical port on the switch.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot*/*port*	Enters interface configuration mode for the Ethernet interface with the specified slot and port. **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*. **Note** To enable the **switchport monitor** command on virtual ethernet ports, you can use the **interface vethernet** *slot*/*port* command.
Step 3	switch(config-if)# **switchport monitor**	Enters monitor mode for the specified Ethernet interface. Priority flow control is disabled when the port is configured as a SPAN destination.
Step 4	switch(config-if)# **exit**	Reverts to global configuration mode.
Step 5	switch(config)# **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 6	switch(config-monitor)# **destination interface ethernet** *slot*/*port*	Configures the Ethernet SPAN destination port. **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.

	Command or Action	Purpose
		Note To enable the virtual ethernet port as destination interface in the monitor configuration, you can use the **destination interface vethernet** *slot*/*port* command.

The following example shows how to configure an Ethernet SPAN destination port (HIF):

```
switch# configure terminal
switch(config)# interface ethernet100/1/24
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# destination interface ethernet100/1/24
switch(config-monitor)#
```

The following example shows how to configure a virtual ethernet (VETH) SPAN destination port:

```
switch# configure terminal
switch(config)# interface vethernet10
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface vethernet10
switch(config-monitor)#
```

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 is not supported for SPAN-on-Drop sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode and specifies the SPAN session for which the MTU truncation size is to be configured.
Step 3	switch(config-monitor) # [**no**] **mtu**	Configures the MTU truncation size for packets in the specified SPAN session. The range is from 64 to 1518 bytes.
Step 4	switch(config-monitor) # **show monitor session** *session-number*	(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

	Command or Action	Purpose
		modules on which MTU truncation is and is not supported.
Step 5	switch(config-monitor) # **copy running-config** startup-config	(Optional) Copies the running configuration to the startup configuration.

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

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # mtu
switch(config-monitor) # copy running-config startup-config
switch(config-monitor) #
```

Configuring Fibre Channel Destination Port

Note The SPAN destination port can only be a physical port on the switch.

You can configure a Fibre Channel port as a SPAN destination port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface fc** *slot*/*port*	Enters interface configuration mode for the specified Fibre Channel interface selected by the slot and port values. **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.
Step 3	switch(config-if)# **switchport mode SD**	Sets the interface to SPAN destination (SD) mode.
Step 4	switch(config-if)# **switchport speed 1000**	Sets the interface speed to 1000. The auto speed option is not allowed.
Step 5	switch(config-if)# **exit**	Reverts to global configuration mode.
Step 6	switch(config)# **monitor session** *session-number*	Enters the monitor configuration mode.
Step 7	switch(config-monitor)# **destination interface fc** *slot*/*port*	Configures the Fibre Channel destination port. **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.

	Command or Action	Purpose

The following example shows how to configure an Ethernet SPAN destination port:

```
switch# configure terminal
switch(config)# interface fc 2/4
switch(config-if)# switchport mode SD
switch(config-if)# switchport speed 1000
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface fc 2/4
```

Configuring Source Ports

A source port can be an Ethernet port, port channel, Fiber Channel ports, SAN port channel, VLAN, or a VSAN port. It cannot be a destination port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified monitoring session.
Step 3	switch(config-monitor) # **source interface** *type slot*/*port* [**rx** | **tx** | **both**]	Adds an Ethernet SPAN source port and specifies the traffic direction in which to duplicate packets. You can enter a range of Ethernet, Fibre Channel, or virtual Fibre Channel ports. You can specify the traffic direction to duplicate as ingress (Rx), egress (Tx), or both. By default, the direction is both. **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.

The following example shows how to configure an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
switch(config-monitor)#
```

The following example shows how to configure a Fibre Channel SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface fc 2/1
switch(config-monitor)#
```

The following example shows how to configure a virtual Fibre Channel SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface vfc 129
switch(config-monitor)#
```

Configuring Source Port Channels, VSANs, or VLANs

You can configure the source channels for a SPAN session. These ports can be port channels SAN port channels, VSANs and VLANs. The monitored direction can be ingress, egress, or both and applies to all physical ports in the group.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 3	switch(config-monitor) # **source** {**interface** {**port-channel** | **san-port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range* | **vsan** *vsan-range* }	Configures port channel, SAN port channel, VLAN, or VSAN sources. For VLAN or VSAN sources, the monitored direction is implicit.

The following example shows how to configure a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 1 rx
switch(config-monitor)# source interface port-channel 3 tx
switch(config-monitor)# source interface port-channel 5 both
switch(config-monitor)#
```

This example shows how to configure a SAN port channel SPAN source:

```
switch(config-monitor)#switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface san-port-channel 3 rx
switch(config-monitor)#
```

The following example shows how to configure a VLAN SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source vlan 1
switch(config-monitor)#
```

switch(config-monitor)#This example shows how to configure a VSAN SPAN source:

```
switch(config-monitor)#switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source vsan 1
switch(config-monitor)#
```

Configuring the Description of a SPAN Session

For ease of reference, you can provide a descriptive name for a SPAN session.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 3	switch(config-monitor) # **description** *description*	Creates a descriptive name for the SPAN session.

The following example shows how to configure a SPAN session description:

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # description monitoring ports eth2/2-eth2/4
switch(config-monitor) #
```

Configuring an ACL Filter for a SPAN Session

To selectively monitor traffic in a SPAN session, you can configure an access-control list (ACL) to filter packets. The SPAN session ignores any permit or deny actions specified in the access-list, and spans only the packets that match the access-list filter criteria.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode and specifies the SPAN session for which the ACL filter is to be configured.
Step 3	switch(config-monitor) # [**no**] **filter access-group** *acl_filter*	Configures the ACL filter for packets in the specified SPAN session. The ACL filter can be a MAC or an IP access-list.
Step 4	switch(config-monitor) # **show monitor session** *session-number*	(Optional) Displays the status of SPAN sessions, including the configuration status of ACL filter.
Step 5	switch(config-monitor) # **copy running-config** startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure an ACL filter for a SPAN session:

```
switch# configure terminal
switch(config) # monitor session 3
```

```
switch(config-monitor) # filter access-group acl_span_ses_3
switch(config) # copy running-config startup-config
switch(config) #
```

Activating a SPAN Session

The default is to keep the session state shut. You can open a session that duplicates packets from sources to destinations.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **no monitor session** {**all** | *session-number*} **shut**	Opens the specified SPAN session or all sessions.

The following example shows how to activate a SPAN session:

```
switch# configure terminal
switch(config) # no monitor session 3 shut
```

Suspending a SPAN Session

By default, the session state is **shut**.

Note The Cisco Nexus switch supports two active SPAN sessions. The Cisco Nexus 5548 Switch supports four active SPAN sessions. When you configure more than two SPAN sessions, the first two sessions are active. During startup, the order of active sessions is reversed; the last two sessions are active. For example, if you configured ten sessions 1 to 10 where 1 and 2 are active, after a reboot, sessions 9 and 10 will be active. To enable deterministic behavior, explicitly suspend the sessions 3 to 10 with the **monitor session** *session-number* **shut** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** {**all** | *session-number*} **shut**	Suspends the specified SPAN session or all sessions.

The following example shows how to suspend a SPAN session:

```
switch# configure terminal
switch(config) # monitor session 3 shut
switch(config) #
```

Displaying SPAN Information

Procedure

	Command or Action	Purpose
Step 1	switch# **show monitor** [**session** {**all** | *session-number* | **range** *session-range*} [**brief**]]	Displays the SPAN configuration.

The following example shows how to display SPAN session information:

```
switch# show monitor
SESSION  STATE        REASON                  DESCRIPTION
-------  -----------  ----------------------  --------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

The following example shows how to display SPAN session details:

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up
acl-name          : acl1
source intf       :
    rx            : fc3/1
    tx            : fc3/1
    both          : fc3/1
source VLANs      :
    rx            :
source VSANs      :
    rx            : 1
destination ports : Eth3/1
```

Configuration Example for a SPAN ACL

This example shows how to configure a SPAN ACL:

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# monitor session 1
switch(config-erspan-src)# filter access-group match_11_pkts
```