



CHAPTER 8

Configuring SPAN

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) on the device.

This chapter includes the following sections:

- [Information About SPAN, page 8-1](#)
- [Licensing Requirements for SPAN, page 8-4](#)
- [Prerequisites for SPAN, page 8-4](#)
- [Guidelines and Limitations, page 8-4](#)
- [Configuring SPAN, page 8-5](#)
- [Field Descriptions for SPAN, page 8-9](#)
- [Additional References, page 8-10](#)

Information About SPAN

You can configure an Ethernet SPAN to monitor traffic in and out of your device. These features allow you to copy packets from sources to destinations.

You create SPAN sessions to define the sources and destinations to use for the network traffic. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. Destination ports receive the copied traffic from all sources.

SPAN sessions apply to the local device.

This section includes the following topics:

- [SPAN Sessions, page 8-1](#)
- [Virtual SPAN Sessions, page 8-2](#)
- [Shutting Down a SPAN Session, page 8-3](#)
- [High Availability, page 8-3](#)
- [Virtualization Support, page 8-3](#)

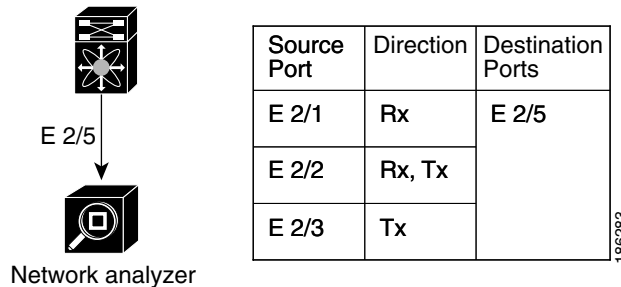
SPAN Sessions

You can create up to 18 SPAN sessions to define sources and destinations on the local device, although only two sessions can be running simultaneously.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 8-1 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 8-1 SPAN Configuration



Sources for a SPAN session include Ethernet ports, VLANs, and remote SPAN (RSPAN) VLANs.



Note

NX-OS does not support terminating an RSPAN session.

Destinations for a SPAN session include ports in either access or trunk mode.



Note

Only two SPAN sessions can be running simultaneously.

For information about configuring a SPAN session, see the “[Configuring a SPAN Session](#)” section on [page 8-5](#).

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.

Figure 8-2 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 Figure 8-2, the device transmits packets from one VLAN at each destination port.

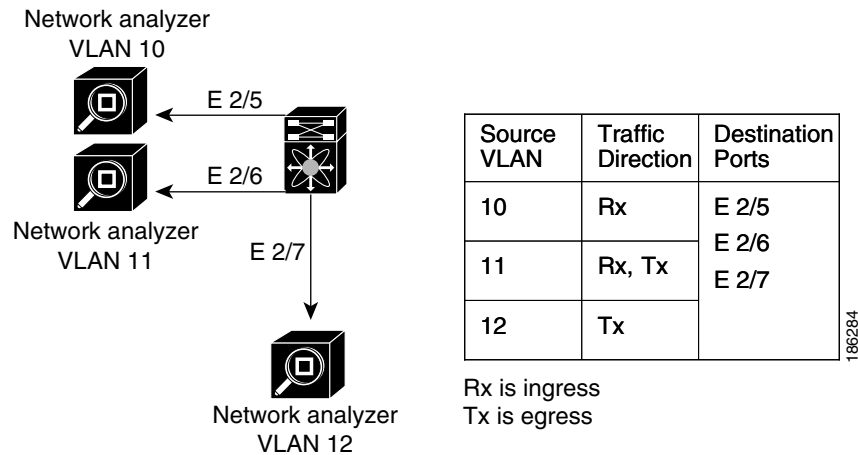


Note

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.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 8-2 Virtual SPAN Configuration



For information about configuring a virtual SPAN session, see the “[Configuring a Virtual SPAN Session](#)” section on page 8-7.

Shutting Down a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. Although you can define up to 18 SPAN sessions, only two SPAN sessions can be running simultaneously.

For information about shutting down SPAN sessions, see the “[Shutting Down or Resuming a SPAN Session](#)” section on page 8-9.

High Availability

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

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 DCNM Virtual Device Context Configuration Guide, Release 4.0* at the following URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/dcnm/virtual_device_context/configuration/guide/vdc_dcnm_book.html

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for SPAN

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	SPAN requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide, Release 4.0</i> .
NX-OS	SPAN requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/licensing/configuration/guide/nx-os_licensing.html

Prerequisites for SPAN

SPAN has the following prerequisites:

- You configure the ports on each device to support the desired SPAN configuration. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.0* at the following URL:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/dcnm/interfaces/configuration/guide/if_dcnm_book.html

Guidelines and Limitations

SPAN has the following configuration guidelines and limitations:

- A maximum of 18 SPAN sessions can be configured on a device.
- A maximum of two SPAN sessions can be running simultaneously on a device.
- You can configure a particular destination port in only one SPAN session.
- You cannot configure a port as both a source and destination port.
- 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 multiple egress source ports, packets that these ports receive may be replicated even though they are not transmitted on the ports. Some examples of this behavior on source ports are as follows:
 - Traffic that results from flooding
 - Broadcast and multicast traffic
- 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.
- VLAN SPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
- You can configure an RSPAN VLAN for use only as a SPAN session source.

Send document comments to nexus7k-docfeedback@cisco.com

- If you configure a SPAN session to monitor a routed interface, only the received traffic is captured, even if the session is configured for both directions. This limitation is only for traffic that enters a Layer 2 interface (with SVI as a Layer 3 interface) and then exits a routed (physical Layer 3) interface, which is the source of the monitor session. If traffic enters a routed (physical Layer 3) interface and exits another routed (physical Layer 3) interface, which is the source of the monitor session, then the destination port of the monitor session captures traffic in both directions. A SPAN session captures traffic in both directions if traffic entering the routed port is destined to an IP address (SVI) on the switch.

Configuring SPAN

You can configure a SPAN session to copy packets from sources to destinations on the local device only.

You can configure a virtual SPAN session by choosing multiple VLAN sources and then choosing which VLANs to allow on each destination port to limit the traffic that the device transmits on it.

This section includes the following topics:

- [Configuring a SPAN Session, page 8-5](#)
- [Configuring a Virtual SPAN Session, page 8-7](#)
- [Configuring an RSPAN VLAN, page 8-8](#)
- [Shutting Down or Resuming a SPAN Session, page 8-9](#)

Configuring a SPAN Session

You can configure a SPAN session to copy packets from sources to destinations on the local device only. By default, SPAN sessions are created in the shut state.

For sources, you can specify Ethernet ports, port channels, VLANs, and RSPAN VLANs. You can specify private VLANs (primary, isolated, and community) in SPAN sources.

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

BEFORE YOU BEGIN

- Configure the destination ports in access or trunk mode. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.0* at the following URL:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/dcnm/interfaces/configuration/guide/if_dcnm_book.html

DETAILED STEPS

To configure a SPAN session, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**. The available devices appear in the Summary pane.
 - Step 2** From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.

Send document comments to nexus7k-docfeedback@cisco.com

- Step 3** (Optional) To delete a SPAN session that you are no longer using, right-click the SPAN session and choose **Delete**.
- Step 4** (Optional) To configure a new SPAN session, from the menu bar choose **File > New > Local SPAN Session**. By default, SPAN sessions are created in the shut state.
- a. (Only the first time you create a SPAN session) From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.
 - b. (Optional) To modify the session number, from the Summary pane, double-click the Session Id field and enter a session number from 1 to 18.



Note You can only modify the session number immediately after you create the session.

- Step 5** From the Summary pane, choose the SPAN session to configure.
- Step 6** From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.
- Step 7** (Optional) To add a description of the SPAN session, specify it in the Description field.
- Step 8** (Optional) To add VLANs to filter (include) in the SPAN session, in the Filtered VLANs field, down arrow to displays the configured VLANs that you can choose.
- Step 9** Add source Ethernet ports to the SPAN session as follows:
- a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - b. Choose the port, right-click on the port row, and choose **Add to SPAN Source** to add this port to the SPAN session sources.
- Step 10** Add source VLANs or RSPAN VLANs to the SPAN session as follows:
- a. From the VLANs association panel, double-click the device to display the configured VLANs.
 - b. Choose the VLAN, right-click on the VLAN row, and choose **Add to SPAN Source** to add this VLAN to the SPAN session sources.
- Step 11** Add destination Ethernet ports to the SPAN session as follows:
- a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - b. Choose an access or trunk port.
 - c. In the Monitor column check the check box to enable monitoring on this port.
 - d. Right-click on the port row and choose **Add to SPAN Destination** to add this port to the SPAN session destinations.
- Step 12** (Optional) To modify SPAN session source settings, follow these steps:
- a. From the **Details** pane, click the **Configuration** tab and expand the **Source and Destination** section, if necessary.
 - b. To modify the ingress or egress choice for a source, check or uncheck the **Ingress** or **Egress** check box to activate the desired direction to monitor. By default, both ingress and egress are monitored.
 - c. To delete a SPAN source or destination, choose the source or destination entry, right-click on it, and choose **Delete**.
- Step 13** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com

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.

For destination ports, you can specify Ethernet ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it.

BEFORE YOU BEGIN

- Configure the destination ports in trunk mode. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.0* at the following URL:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/dcnm/interfaces/configuration/guide/if_dcnm_book.html

DETAILED STEPS

To configure a virtual SPAN session, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**. The available devices appear in the Summary pane.
 - Step 2** From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.
 - Step 3** (Optional) To delete a SPAN session that you are no longer using, right-click the SPAN session and choose **Delete**.
 - Step 4** (Optional) To configure a new SPAN session, from the menu bar choose **File > New > Local SPAN Session**. By default, SPAN sessions are created in the shut state.
 - a. (Only the first time you create a SPAN session) From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.
 - b. (Optional) To modify the session number, from the Summary pane, double-click the Session Id field and enter a session number from 1 to 18.



Note You can only modify the session number immediately after you create the session.

- Step 5** From the Summary pane, choose the SPAN session to configure.
- Step 6** From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.
- Step 7** (Optional) To add a description of the SPAN session, specify it in the **Description** field.
- Step 8** (Optional) To add VLANs to filter (include) in the SPAN session, in the Filtered VLANs field, down array to displays the configured VLANs that you can choose.
- Step 9** Add source Ethernet ports to the SPAN session as follows:
 - a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - b. Choose the port, right-click on the port row, and choose **Add to SPAN Source** to add this port to the SPAN session sources.

Send document comments to nexus7k-docfeedback@cisco.com

- Step 10** Add source VLANs or RSPAN VLANs to the SPAN session as follows:
- From the VLANs association panel, double-click the device to display the configured VLANs.
 - Choose the VLAN, right-click on the VLAN row, and choose **Add to SPAN Source** to add this VLAN to the SPAN session sources.
- Step 11** Add destination Ethernet ports to the SPAN session as follows:
- From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - Choose an access or trunk port.
 - In the Monitor column check the check box to enable monitoring on this port.
 - Right-click on the port row and choose **Add to SPAN Destination** to add this port to the SPAN session destinations.
- Step 12** Limit the VLANs allowed on a trunk port by following these steps:
- From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**. The available devices appear in the Summary pane.
 - From the Summary pane, double-click the device and then double-click the slot that you want to configure.
 - Choose the trunk port to configure.
 - From the Details pane, click the **Port Details** tab and expand the **Port Mode Settings** section, if necessary.
 - Limit the VLANs on the trunk by clicking the Allowed VLANs field. The field displays configured VLANs that you can choose.
- Step 13** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring an RSPAN VLAN

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

DETAILED STEPS

To configure an RSPAN VLAN, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Switching > VLAN**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that you want to configure.
- Step 3** Choose the VLAN to configure.
- Step 4** From the Details pane, click the **VLAN Details** tab and expand the **Advanced Settings** section, if necessary.
- Step 5** Check the **RSPAN VLAN** check box.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Shutting Down or Resuming a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. Because only two SPAN sessions can be running simultaneously, 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.

DETAILED STEPS

To shut down or resume (enable) a SPAN session, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**.
The available devices appear in the Summary pane.
 - Step 2** From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.
 - Step 3** From the Summary pane, choose the SPAN session to configure.
 - Step 4** From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.
 - Step 5** Resume (enable) the SPAN session by choosing **Up** in the Admin Status field.
 - Step 6** Shut down the SPAN session by choosing **Down** in the Admin Status field.



Note If a monitor session is enabled but its operational status is down, then to enable the session you must first shut down the session followed by resuming the session.

Field Descriptions for SPAN

This section includes the following field descriptions for SPAN:

- [Local SPAN Session: Configuration: Session Settings Section, page 8-9](#)
- [Local SPAN Session: Configuration: Source and Destination Section, page 8-10](#)

Local SPAN Session: Configuration: Session Settings Section

Table 8-1 Local SPAN Session: Configuration: Session Settings Section

Element	Description
Session Id	Local SPAN session number. Can only be specified when the session is first created. The value ranges from 1 to 18.
Description	Description for this session.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Table 8-1 Local SPAN Session: Configuration: Session Settings Section (continued)

Element	Description
Filtered VLANs	When clicked, list of configured VLANs.
Admin Status	Administrative status of the session.
Operational Status	<i>Display only.</i> Whether the session is shut (down) or enabled (up).
Status Description	<i>Display only.</i> Status description.

Local SPAN Session: Configuration: Source and Destination Section

Table 8-2 Local SPAN Session: Configuration: Source and Destination Section

Element	Description
Source	
Interface/VLAN	<i>Display only.</i> Port or VLAN number.
Description	<i>Display only.</i> Port or VLAN description.
Ingress	Status of whether to monitor ingress packets.
Egress	Status of whether to monitor egress packets.
Destination	
Interface	<i>Display only.</i> Port number.
Description	<i>Display only.</i> Port description.

Additional References

For additional information related to implementing SPAN, see the following sections:

- [Related Documents, page 8-11](#)
- [Standards, page 8-11](#)

Send document comments to nexus7k-docfeedback@cisco.com

Related Documents

Related Topic	Document Title
VDCs	<i>Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/dcnm/virtual_device_context/configuration/guide/vdc_dcnm_book.html

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Send document comments to nexus7k-docfeedback@cisco.com