



CHAPTER 9

Configuring Local SPAN and ERSPAN

This chapter describes how to configure the local and encapsulated remote (ER) switched port analyzer (SPAN) feature to monitor traffic and includes the following topics:

- [Information About SPAN and ERSPAN, page 9-1](#)
- [SPAN Guidelines and Limitations, page 9-5](#)
- [Default Settings, page 9-6](#)
- [Configuring SPAN, page 9-6](#)
- [Verifying the SPAN Configuration, page 9-20](#)
- [Example Configurations, page 9-20](#)
- [Additional References, page 9-22](#)
- [Feature History for SPAN and ERSPAN, page 9-23](#)

Information About SPAN and ERSPAN

The Switched Port Analyzer (SPAN) feature (sometimes called port mirroring or port monitoring) allows network traffic to be analyzed by a network analyzer such as a Cisco SwitchProbe or other Remote Monitoring (RMON) probe.

SPAN lets you monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports where the network analyzer is attached.

This section includes the following topics:

- [SPAN Sources, page 9-1](#)
- [SPAN Destinations, page 9-2](#)
- [SPAN Sessions, page 9-5](#)

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. These include Ethernet, virtual Ethernet, port-channel, port profile, and VLAN. When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources. When a port profile is specified as a SPAN source, all ports which inherit the port profile are SPAN sources. Traffic can be monitored in the receive direction, the transmit direction, or both directions for Ethernet and virtual Ethernet source interfaces.

Send document comments to nexus1k-docfeedback@cisco.com.

- Receive source (Rx)—Traffic that enters the switch through this source port is copied to the SPAN destination port.
- Transmit source (Tx)—Traffic that exits the switch through this source port is copied to the SPAN destination port.

Characteristics of SPAN Sources

A Local SPAN source has these characteristics:

- Can be port type Ethernet, virtual Ethernet, port channel, port profile, or VLAN.
- Cannot be a destination port or port profile.
- Can be configured to monitor the direction of traffic —receive, transmit, or both.
- Source ports can be in the same or different VLANs.
- For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.
- Local SPAN sources must be on the same host (VEM) as the destination port.
- For port profile sources, all active interfaces attached to the port profile are included as source ports.

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. This section includes the following topics:

- [Characteristics of Local SPAN Destinations, page 9-2](#)
- [Characteristics of ERSPAN Destinations, page 9-3](#)

Characteristics of Local SPAN Destinations

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

- Can be any physical or virtual Ethernet port, a port channel, or a port profile.
- Cannot be a source port or port profile.
- Is excluded from the source list and is not monitored if it belongs to a source VLAN of any SPAN session or a source port profile.
- Receives copies of transmitted and received traffic for all monitored source ports in the same VEM module. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.
- Must not be private VLAN mode.
- A destination port can only monitor sources on the same host (VEM). See [Figure 9-1, Local SPAN](#).
- Destination ports in access mode receive monitored traffic on all the VLANs.
- Destination ports in trunk mode receive monitored traffic only on the allowed VLANs in the trunk configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

Characteristics of ERSPAN Destinations

- An ERSPAN destination is specified by an IP address.
- In ERSPAN, the source SPAN interface and destination SPAN interface may be on different devices interconnected by an IP network. ERSPAN traffic is GRE-encapsulated. See [Figure 9-2, ERSPAN](#).

Local SPAN

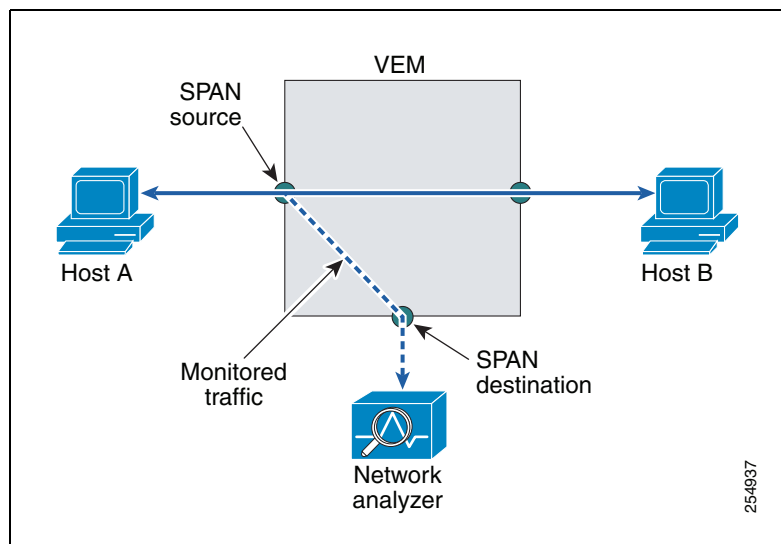
In Local SPAN, the source interface and destination interface are on the same VEM. The network analyzer is attached directly to the SPAN destination port. The SPAN source can be a port, a VLAN interface or port profile. The destination can be a port or port profile.

[Figure 9-1](#) shows that traffic transmitted by host A is received on the SPAN source interface. Traffic (ACLs, QoS, and so forth) is processed as usual. Traffic is then replicated. The original packet is forwarded on toward host B. The replicated packet is then sent to the destination SPAN interface where the monitor is attached.

Local SPAN can replicate to one or more destination ports. Traffic can be filtered so that only traffic of interest is sent out the destination SPAN interface.

Local SPAN can monitor all traffic received on the source interface including BPDUs.

Figure 9-1 Local SPAN



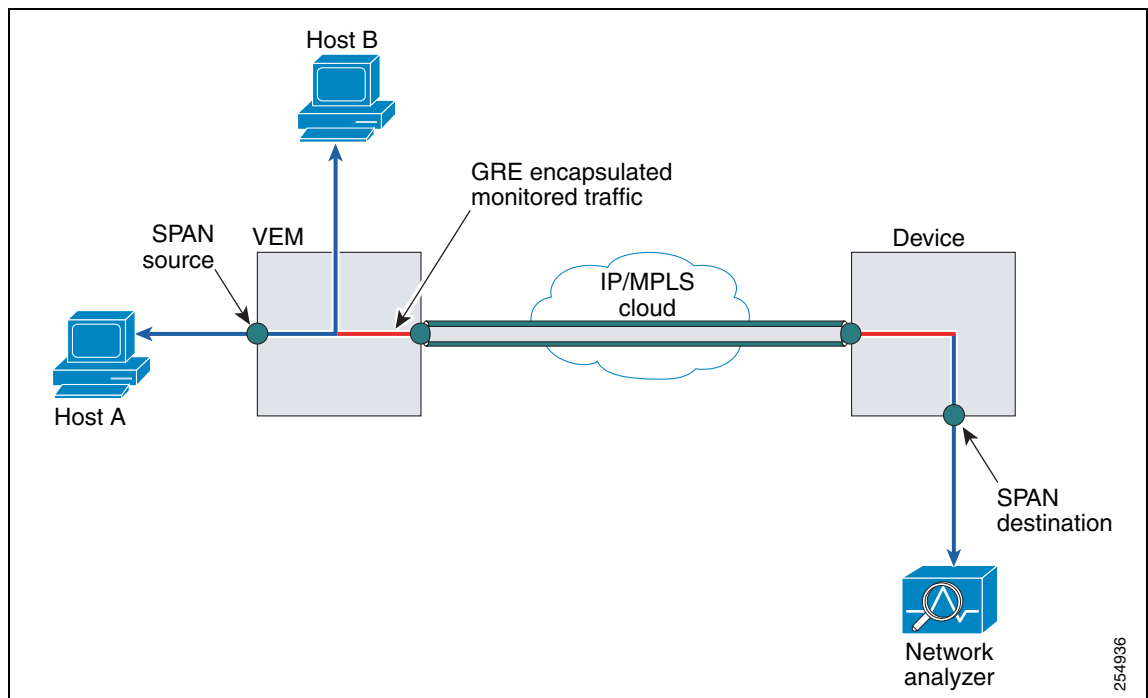
Send document comments to nexus1k-docfeedback@cisco.com.

Encapsulated Remote SPAN

Encapsulated remote (ER) SPAN monitors traffic in multiple network devices across an IP network and sends that traffic in an encapsulated envelope to destination analyzers. In contrast, Local SPAN cannot forward traffic through the IP network. ERSPAN can be used to monitor traffic remotely. ERSPAN sources can be ports, VLANs, or port profiles.

In [Figure 9-2](#), the ingress and egress traffic for host A are monitored using ERSPAN. Encapsulated ERSPAN packets are routed from host A through the routed network to the destination device where they are de-encapsulated and forwarded to the attached network analyzer. The destination may also be on the same L2 network as the source.

Figure 9-2 ERSPAN



Network Analysis Module

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

To use NAM for monitoring the Cisco Nexus 1000V ERSPAN data sources see the *Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note*, 4.2.

Send document comments to nexus1k-docfeedback@cisco.com.

SPAN Sessions

You can create up to 64 total SPAN sessions (Local SPAN plus ERSPAN) on the VEM.

You must configure an ERSPAN session ID that is added to the ERSPAN header of the encapsulated frame to differentiate between ERSPAN streams of traffic at the termination box. You can also configure the range of flow ID numbers. For more information, see [Configuring the Allowable ERSPAN Flow IDs](#), page 9-19.

When trunk ports are configured as SPAN sources and destinations, you can filter VLANs to send to the destination ports from among those allowed. Both sources and destinations must be configured to allow the VLANs.

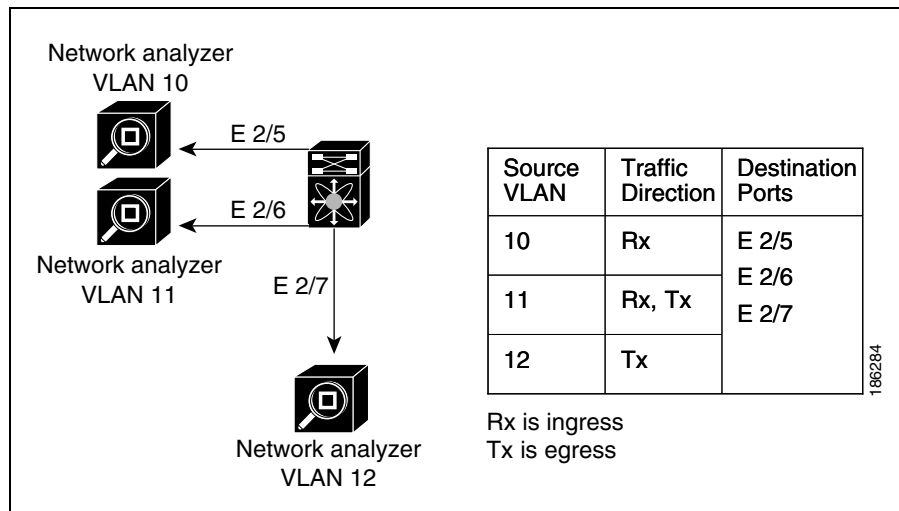
Figure 9-3 shows one example of a VLAN-based SPAN configuration in which traffic is copied from three VLANs to three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic transmitted. In Figure 9-3, the device transmits packets from one VLAN at each destination port. The destinations in this example are trunks on which allowed VLANs are configured.



Note

VLAN-based 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 transmit destination ports.

Figure 9-3 VLAN-based SPAN Configuration Example



SPAN Guidelines and Limitations

SPAN has the following configuration guidelines and limitations:

- A maximum of 64 SPAN sessions (Local SPAN plus ERSPAN) can be configured on the VSM.
- A maximum of 32 source VLANs are allowed in a session.
- A maximum of 32 destinations are allowed for a Local SPAN session.
- A maximum of 128 source interfaces are allowed in a session.

Send document comments to nexus1k-docfeedback@cisco.com.

**Caution****Overload Potential**

To avoid an overload on uplink ports, use caution when configuring ERSPAN, especially when sourcing VLANs.

- A port can be configured in a maximum of 4 SPAN sessions.
- The destination port used in one SPAN session cannot also be used as the destination port for another SPAN session.
- You cannot configure a port as both a source and destination port.
- In a SPAN session, packets that source ports receive may be replicated even though they are not transmitted on the ports. The following are examples of this behavior:
 - Traffic that results from flooding
 - Broadcast and multicast traffic
- For VLAN SPAN sessions switched on the same VLAN with both receive and transmit configured, two packets (one from receive and one from transmit) are forwarded from the destination port.

Default Settings

Table 9-1 lists the SPAN default settings.

Table 9-1 SPAN Defaults

Parameters	Default
State	SPAN sessions are created in the shut state.
Description	blank
Traffic direction for source interface or port profile	both
Traffic direction for source VLAN	receive (ingress or RX)

Configuring SPAN

This section describes how to configure SPAN and includes the following procedures.

- [Configuring a Local SPAN Session, page 9-7](#)
- [Configuring an ERSPAN Port Profile, page 9-9](#)
- [Configuring an ERSPAN Session, page 9-13](#)
- [Shutting Down a SPAN Session, page 9-16](#)
- [Resuming a SPAN Session, page 9-17](#)
- [Verifying the SPAN Configuration, page 9-20](#)

Send document comments to nexus1k-docfeedback@cisco.com.

Configuring a Local SPAN Session

Use this procedure to configure a SPAN session.

**Note**

If you are configuring ERSPAN, see the [“Configuring an ERSPAN Session” procedure on page 9-13](#).

BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You know the number of the SPAN session you are going to configure.
- The source and destination ports are already configured in either access or trunk mode. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*.
- SPAN sessions are created in the shut state by default.
- When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first (see [Step 2, no monitor session](#)).
- This procedure involves creating the SPAN session in Monitor Configuration mode; and then, optionally, configuring allowed VLANs in Interface Configuration mode.

SUMMARY STEPS

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number*
4. **description** *description*
5. **source** {**interface** {*type*} {*id* | *range*} | **vlan** {*id* | *range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]
6. (Optional) Repeat [Step 5](#) to configure additional SPAN sources.
7. (Optional) **filter vlan** {*number* | *range*}
8. (Optional) Repeat [Step 7](#) to configure all source VLANs to filter.
9. **destination** {**interface** {*type*} {*id*} | **port-profile** {*name*}}
10. (Optional) Repeat [Step 9](#) to configure all SPAN destination ports.
11. **no shut**
12. (Optional) **exit**
13. (Optional) **show monitor session** *session-number*
14. (Optional) **show interface** {*type*} {*id*} **switchport**
15. (Optional) **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	no monitor session session-number Example: n1000v(config)# no monitor session 3	Clears the specified session.
Step 3	monitor session session-number Example: n1000v(config)# monitor session 3 n1000v(config-monitor)#	Creates a session with the given session number and places you in the CLI Monitor Configuration mode to further configure the session.
Step 4	description description Example: n1000v(config-monitor)# description my_span_session_3	For the specified SPAN session, adds a description. <ul style="list-style-type: none"> description: up to 32 alphanumeric characters default = blank (no description)
Step 5	source {interface {type} {id} vlan {id range} port-profile {name}} [rx tx both] Example 1: n1000v(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx Example 2: n1000v(config-monitor)# source interface port-channel 2 Example 3: n1000v(config-monitor)# source interface vethernet 12 both Example 4: n1000v(config-monitor)# source vlan 3, 6-8 tx Example 5: n1000v(config-monitor)# source port-profile my_port_profile	For the specified session, configures the sources and the direction of traffic to monitor. <ul style="list-style-type: none"> type: Specify the interface type—Ethernet or vEthernet. ID: Specify the vEthernet number, the Ethernet slot/port, or the VLAN ID to monitor. range: Specify the VLAN range to monitor name: Specify the name of the existing port profile. This port profile is different from the port profile created to carry ERSPAN packets through the IP network as defined in the “Configuring an ERSPAN Port Profile” section on page 9-9. traffic direction: Specify direction of traffic monitoring: <ul style="list-style-type: none"> receive (rx) (the VLAN default) transmit (tx) both (the default)
Step 6	(Optional) Repeat Step 5 to configure additional SPAN sources.	
Step 7	filter vlan {id range} Example: n1000v(config-monitor)# filter vlan 3-5, 7	(Optional) For the specified SPAN session, configures the filter from among the source VLANs.
Step 8	(Optional) Repeat Step 7 to configure all source VLANs to filter.	

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 9	destination {interface {type} {id range} port-profile {name}} Example: n1000v(config-monitor)# destination interface ethernet 2/5, ethernet 3/7	For the specified SPAN session, configures the destination(s) for copied source packets. <ul style="list-style-type: none"> • type: Specify the interface type—Ethernet or vEthernet. • ID: Specify the vEthernet number or the Ethernet slot/port to monitor. • name: Specify the name of the port profile to monitor. Note SPAN destination ports must already be configured as either access or trunk ports.
Step 10	(Optional) Repeat Step 9 to configure all SPAN destination ports.	
Step 11	no shut Example: n1000v(config-monitor)# no shut	Enables the SPAN session. By default, the session is created in the shut state.
Step 12	exit Example: n1000v(config-monitor)# exit n1000v(config)#	(Optional) Exits Monitor Configuration mode and places you in CLI Configuration mode.
Step 13	show monitor session session-number Example: n1000v(config-if)# show monitor session 3	(Optional) Displays the configured monitor session.
Step 14	show interface {type} {id} switchport Example: n1000v(config-if)# show interface ethernet 2/5 switchport	(Optional) Displays the configured port including allowed VLANs.
Step 15	copy running-config startup-config Example: n1000v(config-if)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring an ERSPAN Port Profile

Use this procedure to configure a port profile on the VSM to carry ERSPAN packets through the IP network to a remote destination analyzer.

BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- This configuration must be completed for all hosts in the vCenter Server.
- You know the name to be used for this port profile.

Send document comments to nexus1k-docfeedback@cisco.com.



Note The port profile name is used to configure the VMKNIC. A VMKNIC is required on each ESX host to send ERSPAN encapsulated IP packets, and must have IP connectivity to the ERSPAN destination IP address.

- You know the name of the VMware port group to which this profile maps.
- You have the VMware documentation for adding a new virtual adapter.
- You have already created the system VLAN that sends IP traffic to the ERSPAN destination; and you know its VLAN ID which will be used in this configuration.

For more information about system port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

- The port profile used for ERSPAN must be configured for Layer 3 control. This procedure includes a step for making this configuration.



Note In order to ensure that VSM-VEM control communication messages are not dropped, it is recommended that you configure the QoS queuing feature on the uplink interface to which the VMKNIC with “capability L3 control” is mapped. For more information, see the *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1) SV1(4)*.

- Only one VM kernel NIC can be assigned to this Layer 3 control port profile per host.
- The port profile must be an access port profile. It cannot be a trunk port profile. This procedure includes steps to configure the port profile as an access port profile.
- For more information about creating a Layer 3 control port profile, see the [“Creating a Port Profile for Layer 3 Control” procedure on page 3-9](#).

SUMMARY STEPS

1. **config t**
2. **port-profile** *name*
3. **capability l3control**
4. **vmware port-group** *name*
5. **switchport mode access**
6. **switchport access vlan** *id*
7. **no shutdown**
8. **system vlan** *id*
9. **state enabled**
10. (Optional) **show port-profile name** *name*
11. (Optional) **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	port-profile port_profile_name Example: n1000v(config)# port-profile erspan_profile n1000v(config-port-prof)#	<p>Creates the port profile and places you into CLI Global Configuration mode for the specified port profile. Saves the port profile in the running configuration.</p> <p>The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.</p>
Step 3	capability l3control Example: n1000v(config-port-prof)# capability l3control n1000v(config-port-prof)#	Configures the port profile to carry ERSPAN traffic and saves this in the running configuration.
Step 4	vmware port-group name Example: n1000v(config-port-prof)#vmware port-group erspan n1000v(config-port-prof)#	<p>Designates the port profile as a VMware port group and adds the name of the VMware port group to which this profile maps. Saves the settings in the running configuration.</p> <p>The port profile is mapped to a VMware port group of the same name. When a vCenter Server connection is established, the port group created in Cisco Nexus 1000V is then distributed to the virtual switch on the vCenter Server.</p> <ul style="list-style-type: none"> • name: Port group name. If you do not specify a name, then the port group name will be the same as the port profile name. If you want to map the port profile to a different port group name, use the name option followed by the alternate name.
Step 5	switchport mode access Example: n1000v(config-port-prof)# switchport mode access n1000v(config-port-prof)#	Designates the interfaces as switch access ports (the default).
Step 6	switchport access vlan id Example 1: n1000v(config-port-prof)# switchport access vlan 2 n1000v(config-port-prof)#	<p>Assigns a VLAN ID to the access port for this port profile and saves the setting in the running configuration.</p> <p>This VLAN is used to send IP traffic to the ERSPAN destination.</p>
Step 7	no shutdown Example: n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#	Enables the interface in the running configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 8	<p>system vlan id</p> <p>Example: n1000v(config-port-prof)# system vlan 2 n1000v(config-port-prof)#</p>	<p>Associates the system VLAN ID with the port profile and saves it in the running configuration.</p> <p>Must match the VLAN ID assigned to the access port. If it does not match, then the following error message is generated:</p> <p>ERROR: System vlan being set does not match the switchport access vlan 2</p>
Step 9	<p>state enabled</p> <p>Example: n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#</p>	<p>Enables the port profile in the running configuration.</p> <p>This port profile is now ready to send out ERSPAN packets on all ESX Hosts with ERSPAN sources</p>
Step 10	<p>show port-profile name port_profile_name</p> <p>Example: n1000v(config-port-prof)# show port-profile name erspan port-profile erspan description: status: enabled capability uplink: no capability l3control: yes system vlans: 2 port-group: access max-ports: 32 inherit: config attributes: switchport access vlan 2 no shutdown evaluated config attributes: switchport access vlan 2 no shutdown assigned interfaces: n1000v(config-port-prof)#</p>	<p>(Optional) Displays the configuration for the specified port profile as it exists in the running configuration.</p>
Step 11	<p>copy running-config startup-config</p> <p>Example: n1000v(config-port-prof)# copy running-config startup-config [#####] 100% n1000v(config-port-prof)#</p>	<p>(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p>
Step 12	<p>Using the VMware documentation, go to vSphere Client and configure a VMKNIC on each ESX Host for sending ERSPAN encapsulated packets. Make sure the VMKNIC points to this port profile as a new virtual adapter. This VMKNIC must have IP connectivity to the ERSPAN destination IP address.</p>	

Send document comments to nexus1k-docfeedback@cisco.com.

Configuring an ERSPAN Session

Use this procedure to configure an ERSPAN session.



Note

If you are configuring Local SPAN, see the [“Configuring a Local SPAN Session” procedure on page 9-7](#).

BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You know the number of the SPAN session you are going to configure.
- You have already configured an ERSPAN-capable port profile on the VSM using the [“Configuring an ERSPAN Port Profile” procedure on page 9-9](#).
- Using the VMware documentation for adding a new virtual adapter, you have already configured the required VMKNIC on each of the ESX hosts. The VMKNIC must have IP connectivity to the ERSPAN destination IP address for sending ERSPAN encapsulated packets.
- SPAN sessions are created in the shut state by default.
- When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first (see [Step 2, no monitor session](#)).
- This procedure involves creating the SPAN session in ERSPAN source configuration mode (config-erspan-source).

SUMMARY STEPS

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number* **type erspan-source**
4. **description** *description*
5. **source** {**interface** *type* {*number* | *range*} | **vlan** {*number* | *range*} | **port-profile** *name*} } [**rx** | **tx** | **both**]
6. (Optional) Repeat [Step 5](#) to configure additional ERSPAN sources.
7. (Optional) **filter vlan** {*number* | *range*}
8. (Optional) Repeat [Step 7](#) to configure all source VLANs to filter.
9. **destination ip** *ip_address*
10. (Optional) **ip ttl** *ttl_value*
11. (Optional) **ip prec** *ipp_value*
12. (Optional) **ip dscp** *dscp_value*
13. (Optional) **mtu** *mtu_value*
14. (Optional) **header-type** *value*
15. **erspan-id** *flow_id*
16. **no shut**
17. (Optional) **show monitor session** *session_id*

Send document comments to nexus1k-docfeedback@cisco.com.

18. (Optional) **exit**
19. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	no monitor session session-number Example: n1000v(config)# no monitor session 3	Clears the specified session.
Step 3	monitor session session-number type erspan-source Example: n1000v(config)# monitor session 3 type erspan n1000v(config-erspan-source)#	Creates a session with the given session number and places you in the CLI ERSPAN Source Configuration mode. This configuration is saved in the running configuration.
Step 4	description description Example: n1000v(config-erspan-src)# description my_erspan_session_3 n1000v(config-erspan-src)#	For the specified ERSPAN session, adds a description and saves it in the running configuration. <ul style="list-style-type: none"> • description: up to 32 alphanumeric characters default = blank (no description)
Step 5	source {interface type {number range} vlan {number range} port-profile name} [rx tx both] Example 1: n1000v(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx Example 2: n1000v(config-erspan-src)# source interface port-channel 2 Example 3: n1000v(config-erspan-src)# source interface vethernet 12 both Example 4: n1000v(config-erspan-src)# source vlan 3, 6-8 tx Example 5: n1000v(config-erspan-src)# source port-profile my_port_profile	For the specified session, configures the source(s) and the direction of traffic to monitor, and saves them in the running configuration. <ul style="list-style-type: none"> • type: Specify the interface type—ethernet, port-channel, vethernet. • number: Specify the interface slot/port or range; or the VLAN number or range to monitor. • name: name of an existing port profile. • traffic direction: Specify traffic monitoring to be in one of the following directions: <ul style="list-style-type: none"> – receive (rx) (the VLAN default) – transmit (tx) – both (the interface and port profile default value)
Step 6	(Optional) Repeat Step 5 to configure additional ERSPAN sources.	

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 7	filter vlan {number range} Example: n1000v(config-erspan-src)# filter vlan 3-5, 7	(Optional) For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored; and saves this in the running configuration. On the monitor port, only the traffic from the VLANs which match the VLAN filter list are replicated to the destination.
Step 8	(Optional) Repeat Step 7 to configure all source VLANs to filter.	
Step 9	destination ip ip_address Example: n1000v(config-erspan-src)# destination ip 10.54.54.1 n1000v(config-erspan-src)#	Configures the IP address of the host to which the encapsulated traffic is sent in this monitor session and saves it in the running configuration.
Step 10	ip ttl ttl_value Example: n1000v(config-erspan-src)# ip ttl 64 n1000v(config-erspan-src)#	(Optional) Specifies the IP time-to-live value, from 1-255, for ERSPAN packets in this monitor session, and saves it in the running configuration. The default is 64.
Step 11	ip prec precedence_value Example: n1000v(config-erspan-src)# ip prec 1 n1000v(config-erspan-src)#	(Optional) Specifies the IP precedence value, from 0-7, for the ERSPAN packets in this monitor session, and saves it in the running configuration. The default value is 0.
Step 12	ip dscp dscp_value Example: n1000v(config-erspan-src)# ip dscp 24 n1000v(config-erspan-src)#	(Optional) Specifies the IP DSCP value, from 0-63, for the ERSPAN packets in this monitor session, and saves it in the running configuration. The default is 0.
Step 13	mtu mtu_value Example: n1000v(config-erspan-src)# mtu 1000 n1000v(config-erspan-src)#	(Optional) Specifies an MTU size (50 - 1500) for ERSPANed packets in this monitor session, and saves it in the running configuration. The 1500 MTU size limit includes a 50-byte overhead added to monitored packets by ERSPAN. Packets larger than this size are truncated. The default is 1500.
Step 14	header-type value Example: n1000v(config-erspan-src)# header-type 2 n1000v(config-erspan-src)#	(Optional) Specifies the ERSPAN header type (2 or 3) used for ERSPAN encapsulation for this monitor session. <ul style="list-style-type: none"> • 2 = ERSPANv2 header type (the default) • 3 = ERSPANv3 header type (Used with NAM setups. Any other type of destination works only with the default v2 headers.)

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 15	erspan-id <i>flow_id</i> Example: n1000v(config-erspan-src)# erspan-id 51	Adds an ERSPAN ID (1-1023) to the session configuration and saves it in the running configuration. The session ERSPAN ID is added to the ERSPAN header of the encapsulated frame and can be used at the termination box to differentiate between various ERSPAN streams of traffic.
Step 16	no shut Example: n1000v(config-erspan-src)# no shut	Enables the ERSPAN session and saves it in the running configuration. By default, the session is created in the shut state.
Step 17	show monitor session <i>session_id</i> Example: n1000v(config-erspan-src)# show monitor session 3	(Optional) Displays the ERSPAN session configuration as it exists in the running configuration.
Step 18	copy running-config startup-config Example: n1000v(config-erspan-src)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Shutting Down a SPAN Session

Use this procedure to discontinue the copying of packets for a SPAN session. You can discontinue copying packets from one source and destination; and then resume for another source and destination.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know which SPAN session that you want to shut down.
- You can shut down a SPAN session from either Global Configuration mode or Monitor Configuration mode.

SUMMARY STEPS

From Global Configuration mode:

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} **shut**
3. **show monitor**
4. **copy running-config startup-config**

From Monitor Configuration mode:

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} [**type erspan-source**]

Send document comments to nexus1k-docfeedback@cisco.com.

3. **shut**
4. **show monitor**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	monitor session {session-number session-range all} shut Example: n1000v(config)# monitor session 3 shut n1000v(config)# Example: n1000v(config)# monitor session 3 n1000v(config-monitor)# shut	Shuts down the specified SPAN monitor session(s) from either Global Configuration mode or Monitor-Configuration mode. <ul style="list-style-type: none"> • session-number: Specifies a particular SPAN session number. • session range: Specifies a range of SPAN sessions (allowable = from 1 to 64). • all: Specifies all SPAN monitor sessions.
Step 3	show monitor Example: n1000v(config-monitor)# show monitor	(Optional) Displays the status of the SPAN sessions.
Step 4	copy running-config startup-config Example: n1000v(config-monitor)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Resuming a SPAN Session

Use this procedure to resume the copying of packets for a SPAN session. You can discontinue copying packets from one source and destination; and then resume for another source and destination.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know which SPAN session that you want to configure.
- You can resume the SPAN session from either Global Configuration mode or Monitor Configuration mode.

Send document comments to nexus1k-docfeedback@cisco.com.

SUMMARY STEPS

From Global Configuration mode:

1. `config t`
2. `no monitor session {session-number | session-range | all} shut`
3. `show monitor`
4. `copy running-config startup-config`

From Monitor Configuration mode:

1. `config t`
2. `monitor session {session-number | session-range | all} [type erspan-source]`
3. `no shut`
4. `show monitor`
5. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	<code>[no] monitor session {session-number session-range all} shut</code> Example: n1000v(config)# no monitor session 3 shut n1000v(config)# Example: n1000v(config)# monitor session 3 n1000v(config-monitor)# no shut	Starts the specified SPAN monitor session(s) from either Global Configuration mode or Monitor-Configuration mode. <ul style="list-style-type: none"> • session-number: Specifies a particular SPAN session number. • session range: Specifies a range of SPAN sessions (allowable = from 1 to 64). • all: Specifies all SPAN monitor sessions.
Step 3	<code>show monitor</code> Example: n1000v(config-monitor)# show monitor	(Optional) Displays the status of all configured SPAN sessions for verification.
Step 4	<code>show monitor session session-id</code> Example: n1000v(config-monitor)# show monitor session 3	(Optional) Displays detailed configuration and status of a specific SPAN session for verification.
Step 5	<code>copy running-config startup-config</code> Example: n1000v(config-monitor)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

Configuring the Allowable ERSPAN Flow IDs

Use this procedure to restrict the allowable range of flow IDs that can be assigned to ERSPAN sessions.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know the restricted range of ERSPAN flow IDs that you want to designate.
- The available ERSPAN flow IDs are 1-1023. You can restrict the range of available IDs using this procedure.

SUMMARY STEPS

1. **config t**
2. **[no] limit-resource erspan-flow-id minimum *min_val* maximum *max_val***
3. **show running monitor**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	[no] limit-resource erspan-flow-id minimum <i>min_val</i> maximum <i>max_val</i> Example: n1000v(config)# limit-resource erspan-flow-id minimum 20 maximum 40 n1000v(config)# Example: n1000v(config)# no limit-resource erspan-flow-id n1000v(config)#	Restricts the allowable range of ERSPAN flow IDs that can be assigned. <ul style="list-style-type: none"> • Allowable range = 1 to 1023 • Defaults: <ul style="list-style-type: none"> – <i>min_val</i> = 1 – <i>max_val</i> = 1023 <p>The no version of this command removes any configured values and restores default values.</p>
Step 3	show running monitor Example: n1000v(config-monitor)# show monitor session 3	(Optional) Displays changes to the default limit-resource erspan-flow-id values for verification.
Step 4	copy running-config startup-config Example: n1000v(config-monitor)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

Verifying the SPAN Configuration

To verify the SPAN configuration, use the following commands:

Command	Purpose
show monitor session {all <i>session-number</i> <i>range session-range</i> } [brief]	Displays the SPAN session configuration.
show monitor	Displays Ethernet SPAN information.
module vem <i>module-number</i> execute vemcmd show span	Displays the configured SPAN sessions on a VEM module.
show port-profile name <i>port_profile_name</i>	Displays a port profile.

Example Configurations

This section includes the following example configurations:

- [Example Configuration for a SPAN Session, page 9-20](#)
- [Example Configuration for an ERSPAN Session, page 9-21](#)

Example Configuration for a SPAN Session

To configure a SPAN session, follow these steps:

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

```
n1000v# config t
n1000v(config)# interface ethernet 2/5
n1000v(config-if)# switchport
n1000v(config-if)# switchport mode trunk
n1000v(config-if)# no shut
n1000v(config-if)# exit
n1000v(config)#
```

Step 2 Configure a SPAN session.

```
n1000v(config)# no monitor session 1
n1000v(config)# monitor session 1
n1000v(config-monitor)# source interface ethernet 2/1-3
n1000v(config-monitor)# source interface port-channel 2
n1000v(config-monitor)# source port-profile my_profile_src
n1000v(config-monitor)# source vlan 3, 6-8 tx
n1000v(config-monitor)# filter vlan 3-5, 7
n1000v(config-monitor)# destination interface ethernet 2/5
n1000v(config-monitor)# destination port-profile my_profile_dst
n1000v(config-monitor)# no shut
n1000v(config-monitor)# exit
n1000v(config)# show monitor session 1
n1000v(config)# copy running-config startup-config

n1000v(config)# show monitor session 1
session 1
-----
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

type           : local
state          : up
source intf    :
  rx           : Eth2/1 Eth2/2 Eth2/3
  tx           : Eth2/1 Eth2/2 Eth2/3
  both        : Eth2/1 Eth2/2 Eth2/3
source VLANs   :
  rx           :
  tx           : 3,6,7,8
  both        :
source port-profile :
  rx           : my_profile_src
  tx           : my_profile_src
  both        : my_profile_src
filter VLANs   : 3,4,5,7
destination ports : Eth2/5
destination port-profile : my_profile_dst

n1000v# module vem 3 execute vemcmd show span

VEM SOURCE IP NOT CONFIGURED.

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
      1             local    49,51,52,55,56

```

Example Configuration for an ERSPAN Session

The following example shows how to create an ERSPAN session for a source Ethernet interface and destination IP address on the Cisco Nexus 1000V. Packets arriving at the destination IP are identified by the ID 999 in their header.

```

monitor session 2 type erspan-source
source interface ethernet 3/3
source port-profile my_profile_src
destination ip 10.54.54.1
erspan-id 999
mtu 1000
no shut

show monitor session 2
  session 2
  -----
type           : erspan-source
state          : up
source intf    :
  rx           : Eth3/3
  tx           : Eth3/3
  both        : Eth3/3
source VLANs   :
  rx           :
  tx           :
  both        :
source port-profile :
  rx           : my_profile_src
  tx           : my_profile_src
  both        : my_profile_src
filter VLANs   : filter not specified
destination IP : 10.54.54.1
ERSPAN ID     : 999

```

Send document comments to nexus1k-docfeedback@cisco.com.

```

ERSPAN TTL           : 64
ERSPAN IP Prec.     : 0
ERSPAN DSCP         : 0
ERSPAN MTU          : 1000
ERSPAN Header Type: 2

module vem 3 execute vemcmd show span

VEM SOURCE IP: 10.54.54.10

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
    1             local   49,51,52,55,56
    2             999       2       10.54.54.1

```

Additional References

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

- [Related Documents, page 9-22](#)
- [Standards, page 9-22](#)

Related Documents

Related Topic	Document Title
Port profile configuration	<i>Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)</i>
Interface configuration	<i>Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)</i>
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)</i>

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 nexus1k-docfeedback@cisco.com.

Feature History for SPAN and ERSPAN

This section provides the SPAN and ERSPAN feature release history.

Feature Name	Releases	Feature Information
Port profile as Local SPAN and ERSPAN source	4.2(1)SV1(4)	You can specify a port profile as a source for local SPAN and ERSPAN monitor traffic.
NAM support for ERSPAN data sources	4.0(4)SV1(3)	NAM support was introduced.
ERSPAN Type III header	4.0(4)SV1(3)	ERSPAN Type III header format was introduced.
SPAN and ERSPAN	4.0(4)SV1(1)	SPAN and ERSPAN were introduced.

Send document comments to nexus1k-docfeedback@cisco.com.