Configuring Local SPAN and ERSPAN

This chapter contains the following sections:

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) probes.

SPAN allows you to 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.

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. These sources 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 that 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 as described by the following:

- 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.

  For a port profile source, either a dynamic vEthernet or an auto-generated Ethernet port profile should be used.

- Cannot be a destination port or port profile

- Can be configured to monitor the direction of traffic —receive, transmit, or both.

- Can be in the same or different VLANs.

- For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.

- Must be on the same host Virtual Ethernet Module (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.

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.

  For a port profile destination, either a dynamic vEthernet or an auto-generated Ethernet port profile should be used.

- 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. 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.

- Can only monitor sources on the same host (VEM)

- In access mode, can receive monitored traffic on all the VLANs.

- In trunk mode, can receive monitored traffic only on the allowed VLANs in the trunk configuration.

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 Generic Routing Encapsulation (GRE-encapsulated).
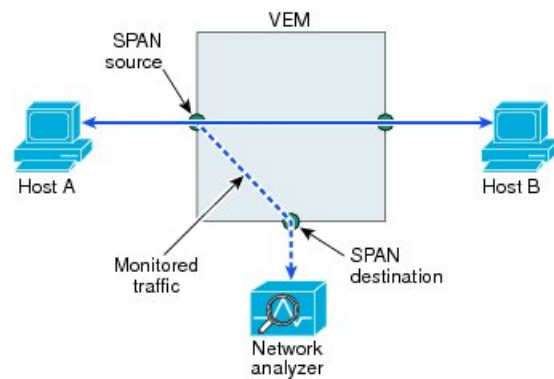
Local SPAN

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 a port profile.The destination can be a port or port profile.

The diagram 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 Bridge Protocol Data Unit (BPDU).

Figure 1: Local SPAN

Encapsulated Remote SPAN

Encapsulated remote SPAN (ERSPAN) 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 the following figure, 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 decapsulated and forwarded to the attached network analyzer. The destination may also be on the same Layer 2 network as the source.

Figure 2: ERSPAN Example
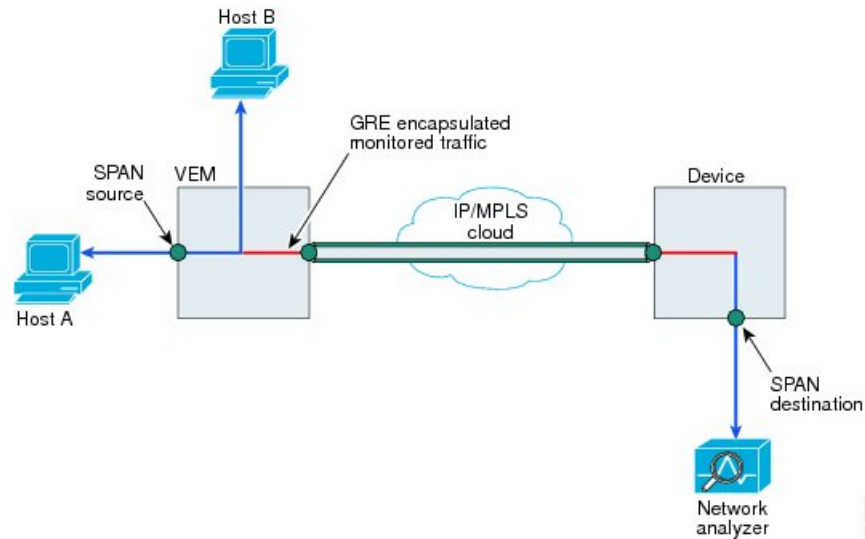
Network Analysis Module

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.*

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.

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.

The following figure 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 the figure, 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 3: VLAN-based SPAN Configuration Example
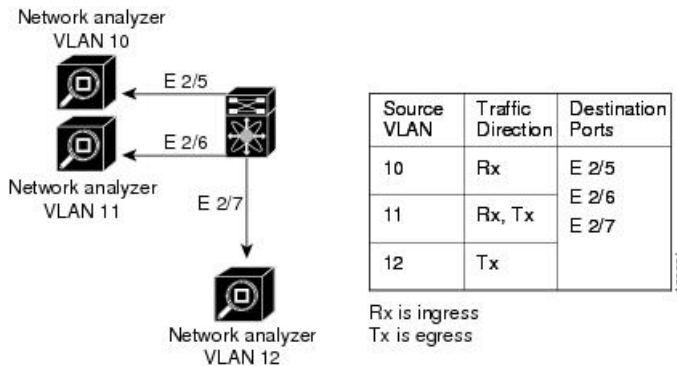
Guidelines and Limitations for SPAN

- A maximum of 64 SPAN sessions (Local SPAN plus ERSPAN) can be configured on the Virtual Supervisor Module (VSM).

- A maximum of 32 source VLANs are allowed in a session.

- A maximum of 32 destination interfaces are allowed for a Local SPAN session.

- A maximum of 8 destination port-profiles are allowed for a Local SPAN session.

- A maximum of 16 source port-profiles are allowed in a session.

- A maximum of 128 source interfaces are allowed in a session.

⚠

Caution   Overload Potential

To avoid an overload on uplink ports, use caution when configuring ERSPAN, especially when sourcing VLANs. The uplink that the VM kernel uses might get overloaded due to ERSPAN traffic. VSM-VEM communication might also be impacted. For example, when the Nexus 1000V is configured for Layer 3 connectivity, both AIPC traffic and ERSPAN traffic use the same VM kernel NIC.

- A port can be configured in a maximum of four SPAN sessions.

- A port can be a source in a maximum of four 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 for SPAN

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

Configuring a Local SPAN Session

This procedure involves creating the SPAN session in monitor configuration mode, and then, optionally, configuring allowed VLANs in interface configuration mode.

It is important to know the following information about SPAN:

• 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. This procedure includes how to do this.

• 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*.

Before you begin

• Log into the CLI in EXEC mode.

• Determine the number of the SPAN session you are going to configure.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no monitor session** *session-number*	Clears the specified session.

	Command or Action	**Purpose**
Step 3	switch(config)# **monitor session** *session-number*	Creates a session with the given session number and places you in monitor configuration mode to further configure the session.
Step 4	switch(config-monitor)# **description** *description*	Adds a description for the specified SPAN session. The *description* can be up to 32 alphanumeric characters. The default is blank (no description)

Step 5	switch(config-monitor)# **source** {**interface** {*type*} {*id*} | **vlan** {*id* | *range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]	For the specified session, configures the sources and the direction of traffic to monitor.
		
		• For the *type* argument, specify the interface type—Ethernet or vEthernet.
		
		• For the *id* argument, specify the vEthernet number, the Ethernet slot/port, or the VLAN ID to monitor.
		
		• For the *range* argument, specify the VLAN range to monitor.
		
		• For the *name* argument, 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
		
		• For the **traffic direction** keywords, specify as follows:
		
		    • **rx** which is the VLAN default indicates receive.
		
		    • **tx** indicates transmit.
		
		    • **both** is the default keyword

Step 6	(Optional) Repeat Step 5 to configure additional SPAN sources.	
Step 7	(Optional) switch(config-monitor)# **filter vlan** {*id* | *range*}	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.	

	Command or Action	Purpose
Step 9	switch(config-monitor)# **destination** {**interface** {*type*} {*id* | *range*} | **port-profile** {*name*}}	For the specified SPAN session, configures the destination(s) for copied source packets. • For the *type* argument, specify the interface type—Ethernet or vEthernet. • For the *id* argument, specify the vEthernet number or the Ethernet slot/port to monitor. • For the *name* argument specify the name of the port profile to monitor.
Step 10	(Optional) Repeat Step 9 to configure all SPAN destination ports.	
Step 11	switch(config-monitor)# **no shut**	Enables the SPAN session. By default, the session is created in the shut state.
Step 12	(Optional) switch(config-monitor)# **exit**	Exits monitor configuration mode and places you in interface configuration mode.
Step 13	(Optional) switch(config-if)# **show monitor session** *session-number*	Displays the configured monitor session.
Step 14	switch(config-if)# **show interface** {*type*} {*id*} **switchport**	Displays the configured port including allowed VLANs. • For the *type* argument, specify the interface type—Ethernet or vEthernet. • For the *id* argument, specify the vEthernet number or the Ethernet slot/port to monitor.
Step 15	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# description my_span_session_3
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, ethernet 3/7
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config-if)# show monitor session 3
switch(config-if)# show interface ethernet 2/5 switchport
switch(config-if)# copy running-config startup-config
```

Configuring an ERSPAN Session

This procedure involves creating the SPAN session in ERSPAN source configuration mode (config-erspan-source).

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. The step to do this is included in the procedure.

Before you begin

Before beginning this procedure, be sure you have done the following:

- Logged in to the CLI in EXEC mode

- Obtained the number of the SPAN session that you are going to configure

- The Hyper-V host must have IP connectivity to the ERSPAN destination IP address for sending ERSPAN-encapsulated packets.

- ERSPAN traffic uses GRE encapsulation. If there are firewalls between the ERSPAN source and destinations, we recommend that you set a rule to allow GRE traffic. This traffic could be identified by IP protocol number 47.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no monitor session** *session-number*	Clears the specified session.
Step 3	switch(config)# **monitor session** *session-number* **type erspan-source**	Creates a session with the given session number and places you in ERSPAN source configuration mode. This configuration is saved in the running configuration.
Step 4	switch(config-erspan-src)# **description** *description*	For the specified ERSPAN session, adds a description and saves it in the running configuration. The *description* can be up to 32 alphanumeric characters The default is blank (no description)
Step 5	switch(config-erspan-src)#**source** {**interface** *type* {*number*|*range*} | **vlan** {*number*|*range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]	For the specified session, configures the sources and the direction of traffic to monitor and saves them in the running configuration. • For the *type* argument, specify the interface type—ethernet, port-channel, vethernet.

	Command or Action	Purpose
		• For the *number* argument, specify the interface slot/port or range; or the VLAN number or range to monitor.
		• For the *name* argument, specify the name of the existing port profile.
		• For the traffic direction keywords, specify as follows:
		• **rx** which is the VLAN default indicates receive.
		• **tx** indicates transmit.
		• **both**is the default keyword
Step 6	(Optional) Repeat Step 5 to configure additional ERSPAN sources.	
Step 7	(Optional) switch(config-erspan-src)# **filter vlan** {*number* | *range*}	For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored; and saves the VLAN arguments to the running configuration. On the monitor port, only the traffic from the VLANs that 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	switch(config-erspan-src)# **destination ip** *ip_address*	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	(Optional) switch(config-erspan-src)# **ip ttl** *ttl_value*	Specifies the IP time-to-live value, from 1 to 255, for ERSPAN packets in this monitor session and saves it in the running configuration.
Step 11	(Optional) switch(config-erspan-src)# **ip prec** *precedence_value*	Specifies the IP precedence value, from 0 to 7, for the ERSPAN packets in this monitor session and saves it in the running configuration. The default value is 0.
Step 12	(Optional) switch(config-erspan-src)# **ip dscp** *dscp_value*	Specifies the IP DSCP value, from 0 to 63. for the ERSPAN packets in this monitor session and saves it in the running configuration. The default is 0.

	Command or Action	**Purpose**
Step 13	(Optional) switch(config-erspan-src)# **mtu** *mtu_value*	Specifies an MTU size (from 50 to 1500) for ERSPAN 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.
		Note If the ERSPAN destination is a Cisco 6500 switch, truncated ERSPAN packets are dropped unless the **no mls verify ip length consistent** command is configured on the Cisco 6500.
Step 14	switch(config-erspan-src)# **header-type** *value*	Specifies the ERSPAN header type (2 or 3) used for ERSPAN encapsulation for this monitor session as follows:
		• 2 is the ERPSPANv2 header type (the default)
		• 3 is the ERSPANv3 header type (Used with NAM setups. Any other type of destination works only with the default v2 headers.)
Step 15	switch(config-erspan-src)# **erspan-id** *flow_id*	Adds an ERSPAN ID (from 1 to 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	switch(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	(Optional) switch(config-erspan-src)# **show monitor session** *session_id*	Displays the ERSPAN session configuration as it exists in the running configuration
Step 18	(Optional) switch(config-erspan-src)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan
switch(config-erspan-src)# description my_erspan_session_3
switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-erspan-src)# filter vlan 3-5, 7
switch(config-erspan-src)# destination ip 10.54.54.1
switch(config-erspan-src)# ip ttl 64
switch(config-erspan-src)# ip prec 1
switch(config-erspan-src)# ip dscp 24
switch(config-erspan-src)# mtu 1000
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# erspan-id 51
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 3
switch(config-erspan-src)# copy running-config startup-config
```

Shutting Down a SPAN Session from Global Configuration Mode

Before you begin

- Log in to the CLI in EXEC mode.

- Determine which session you want to shutdown

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from global configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config)# **show monitor**	Displays the status of the SPAN sessions.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

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

Shutting Down a SPAN Session from Monitor Configuration Mode

Before you begin

- Log in to the CLI in EXEC mode.

- Determine which session you want to shutdown

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** {*session-number* | *session-range* | **all**} **[type erspan-source]**	Specifies the SPAN monitor session(s)) you want to shut down from monitor-configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	switch(config)# **shut**	Shuts down the specified SPAN monitor session(s) from monitor configuration mode.
Step 4	(Optional) switch(config-monitor)# **show monitor**	Displays the status of the SPAN sessions.
Step 5	(Optional) switch(config-monitor)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

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

Resuming a SPAN Session from Global Configuration Mode

You can discontinue copying packets from one source and destination and then resume from another source and destination in global configuration mode.

Before you begin

- Log in to the CLI in EXEC mode.

- Determine which SPAN session that you want to configure.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**]**monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from global configuration mode.
		- The *session-number* argument specifies a particular SPAN session number.
		- The *session-range* argument specifies a range of SPAN sessions from 1 to 64.
		- The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config)# **show monitor**	Displays the status of the SPAN sessions.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no monitor session 3 shut
switch(config)# show monitor
switch(config)# copy running-config startup-config
```

Resuming a SPAN Session from Monitor Configuration Mode

You can discontinue copying packets from one source and destination and then resume from another source and destination in monitor configuration mode.

Before you begin

- Log in to the CLI in EXEC mode.

- Determine which SPAN session that you want to configure.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **monitor session** {*session-number* | *session-range* | **all**} **shut**	Shuts down the specified SPAN monitor session(s) from monitor configuration mode. • The *session-number* argument specifies a particular SPAN session number. • The *session-range* argument specifies a range of SPAN sessions from 1 to 64. • The **all** keyword specifies all SPAN monitor sessions.
Step 3	(Optional) switch(config-monitor)# **show monitor**	Displays the status of the SPAN sessions.
Step 4	(Optional) switch(config-monitor)# **show monitor session** *session-id*	Displays detailed configuration and status of a specific SPAN session for verification.
Step 5	(Optional) switch(config-monitor)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# no shut
switch(config-monitor)# show monitor
switch(config-monitor)# show monitor session 3
switch(config-monitor)# copy running-config startup-config
```

Configuring the Allowable ERSPAN Flow IDs

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

Before you begin

• Log in to the CLI in EXEC mode.

• Determine the restricted range of ERSPAN flow IDs that you want to designate.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# [**no**] **limit-resource erspan-flow-id minimum** *min_val* **maximum** *max_va*l	Restricts the allowable range of ERSPAN flow IDs that can be assigned. The allowable range is from 1 to 1023. The defaults are as follows: • The minimum value = 1 • The maximum value = 1023 The **no** form of this command removes any configured values and restores default values.
Step 3	(Optional) switch(config)# **show running monitor**	Displays changes to the default limit-resource erspan-flow-id values for verification
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# limit-resource erspan-flow-id minimum 20 maximum 40
switch(config)# show monitor
switch(config)# show running monitor
switch(config)# copy running-config startup-config
```

Verifying the SPAN Configuration

Use one of the following commands to verify the configuration:

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

Configuration Examples

This section provides examples for creating a SPAN or an ERSPAN session with different configurations such as, with source Ethernet or vEthernet interface, with source dynamic or auto-generated port profile, or with destination IP address or vEthernet interface.

Note   To configure a SPAN or an ERPSAN session with source or destination as port profile, you must either use a dynamic vEthernet or an auto-generated Ethernet port profile.

The following port profiles are used in examples in this section.

```
switch# show port-profile brief

  ----------------------------------------------------------------------
Port                           Profile   Profile  Conf   Eval   Assigned  Child
Profile                        Type      State    Items  Items  Intfs     Profs
----------------------------------------------------------------
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
                               Vethernet  1        2      3      1         0
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_fef09dbe-d020-4a5f-80ee-157fe765f37c
                               Vethernet  1        2      3      1         0
NSM_template_segmentation      Vethernet  1        1      1      0         0
NSM_template_vlan              Vethernet  1        1      1      0         0
uplink-vpc                     Ethernet   1        3      5      11        0
uplink_network_default_policy  Ethernet   1        2      2      0         0
veth-nopolicy                  Vethernet  1        1      1      0         2
vpc                            Ethernet   1        2      2      0         1
------------------------------------------------------------------------------
Profile     Assigned  Total  Sys    Parent Child  UsedBy
Type        Intfs     Prfls  Prfls  Prfls  Prfls  Prfls
------------------------------------------------------------------------------
Vethernet   2         5      0      4      2      2
Ethernet    11        3      0      2      1      1
```

Examples for Configuring an ERSPAN Session

Example 1: ERSPAN Session with Source Ethernet Interface, Source Dynamic vEthernet Port Profile, and Destination IP Address

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

```
switch#  monitor session 2 type erspan-source
switch(config-erspan-src)# source interface ethernet 3/3
switch(config-erspan-src)# source port-profile
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
switch(config-erspan-src)# destination ip 10.54.54.1
switch(config-erspan-src)# erspan-id 999
switch(config-erspan-src)# mtu 1000
switch(config-erspan-src)# no shut

switch(config-erspan-src)# 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   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    tx   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    both : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf

filter VLANs      : filter not specified
destination IP    : 10.54.54.1
ERSPAN ID         : 999
ERSPAN TTL        : 64
ERSPAN IP Prec.   : 0
ERSPAN DSCP       : 0
ERSPAN MTU        : 1000
ERSPAN Header Type: 2

switch(config-erspan-src)# module vem 3 execute vemcmd show span

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

Example 2: ERSPAN Session with Source Ethernet Interface, Source Auto-Generated Ethernet Port Profile, and Destination IP Address

The following example shows how to create an ERSPAN session with a source Ethernet interface, a source auto-generated Ethernet port profile (Uplink Network + Ethernet Profile Policy), and a destination IP address on Cisco Nexus 1000V. Packets arriving at the destination IP are identified by the ID 999 in their header.

```
switch#  monitor session 3 type erspan-source
switch(config-erspan-src)# source interface ethernet 3/3
switch(config-erspan-src)# source  port-profile uplink-vpc
switch(config-erspan-src)# destination ip 10.54.54.1
switch(config-erspan-src)# erspan-id 999
switch(config-erspan-src)# mtu 1000
switch(config-erspan-src)# no shut

switch(config-erspan-src)# show monitor session 3
    session 3
--------------
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          : uplink-vpc
    tx          : uplink-vpc
```

```
   both          : uplink-vpc
filter VLANs     : filter not specified
destination IP   : 10.54.54.1
ERSPAN ID        : 999
ERSPAN TTL       : 64
ERSPAN IP Prec.  : 0
ERSPAN DSCP      : 0
ERSPAN MTU       : 1000
ERSPAN Header Type: 2
```

Examples for Configuring a SPAN Session

Example 1: SPAN Session with Source vEthernet Interface, Source Dynamic vEthernet Port Profile, Destination Ethernet Interface, and Destination Dynamic vEthernet Port Profile

The following example shows how to create a local SPAN session with a source vEthernet interface, a source dynamic vEthernet port profile, a destination Ethernet interface, and a destination dynamic vEthernet port-profile on Cisco Nexus 1000V.

```
switch(config)# show monitor session 1
   session 1
---------------
type     : local
state    : up
source intf:
    rx   :      Veth1
    tx   :      Veth1
    both :      Veth1
source VLANs :
    rx   :
    tx   :
    both :
source port-profile :
    rx   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    tx   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    both : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf

filter VLANs  : filter not specified
destination ports : Veth2
destination port-profile :

switch(config)# no monitor session 1
switch(config)# monitor session 1
  switch(config-monitor)# source interface vethernet 1
  switch(config-monitor)# source interface port-channel 2
  switch(config-monitor)# source port-profile
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
  switch(config-monitor)# source vlan 3, 6-8 tx
  switch(config-monitor)# filter vlan 3-5, 7
  switch(config-monitor)# destination interface ethernet 2/5
  switch(config-monitor)# destination port-profile destination port-profile
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_fef09dbe-d020-4a5f-80ee-157fe765f37c
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# copy running-config startup-config

switch(config)# show monitor session 1
   session 1
---------------
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   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    tx   : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf
    both : dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_7331e3fc-1abd-4631-addf-886d566697bf

filter VLANs      : 3,4,5,7
destination ports : Eth2/5
destination port-profile :
dynpp_6a521e29-f3d9-4019-8a24-d051f678af63_fef09dbe-d020-4a5f-80ee-157fe765f37c

switch# module vem 3 execute vemcmd show span

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

Example 2: SPAN Session with Source Auto-Generated Ethernet Port Profile and Destination vEthernet Interface

The following example shows how to create a local SPAN session with a source auto-generated Ethernet port profile (Uplink Network + Ethernet Profile Policy) and a destination vEthernet interface on Cisco Nexus 1000V.

```
switch(config)# monitor session 3
  switch(config-monitor)# source port-profile uplink-vpc
  switch(config-monitor)# destination interface ethernet 2
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# copy running-config startup-config

switch(config)# show monitor session 3
session 3
---------------
type            : local
state           : up
source intf     :
    rx          :
    tx          :
    both        :
source VLANs    :
    rx          :
    tx          :
    both        :
source port-profile :
    rx          : uplink-vpc
    tx          : uplink-vpc
    both        : uplink-vpc
filter VLANs      : filter not specified
destination ports : Veth2
destination port-profile :
```

Example for Enabling SPAN Monitoring

This example shows how to configure destination ports in access or trunk mode, and enable SPAN monitoring.

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

Feature History for SPAN and ERSPAN

Feature Name	Releases	Feature Information
SPAN and ERSPAN	5.2(1)SM1(5.1)	SPAN and ERSPAN were introduced.