Configuring ERSPAN

- Prerequisites for Configuring ERSPAN, on page 1
- Restrictions for Configuring ERSPAN, on page 1
- Information about Configuring ERSPAN, on page 2
- How to Configure ERSPAN, on page 5
- Configuration examples for ERSPAN, on page 15
- Verifying ERSPAN, on page 16
- Additional References, on page 18
- Feature History for ERSPAN, on page 19

Prerequisites for Configuring ERSPAN

- Apply the Access control list (ACL) filter before sending the monitored traffic on to the tunnel.

Restrictions for Configuring ERSPAN

The following restrictions apply for this feature:

- Truncation is supported only on IPv4 and IPv6 spanned packets and not on Layer 2 packets without an IP header.
- You can configure either a list of ports or a list of VLANs as a source, but cannot configure both for a given session.
- When a session is configured through the ERSPAN CLI, the session ID and the session type cannot be changed. To change them, you must use the **no** form of the commands to remove the session and then reconfigure it.
- ERSPAN source sessions do not copy locally-sourced ERSPAN Generic routing encapsulation (GRE)-encapsulated traffic from source ports.
- Disabling the **ip routing** command for IPv4 connections and **ipv6 unicast-routing** command for IPv6 connections stops ERSPAN traffic flow to the destination port.
- ERSPAN over MPLS VPN is supported on Layer 3 VPNs, Segment Routing and Seamless MPLS.
- ERSPAN over MPLS VPN is not supported for L2VPN, 6PE, 6VPE, MPLS over GRE and InterAS.

- You cannot configure an MPLS core switch as an ERSPAN destination. ERSPAN traffic can be transported from one Provider Edge (PE) to another Provide Edge (PE). It cannot be transported to the core switch between the two Provider Edges.
- ERSPAN sessions do not capture DHCP-inject packets. DHCP-inject packets refer to DHCP packets (DISCOVER, OFFER, REQUEST, and ACK packets) which are modified by the CPU and inserted back into the network.
- If a backup configuration having ERSPAN session enabled is restored to the running configuration, ERSPAN sessions are created automatically in disabled state. You must manually enable these ERSPAN sessions.
- ERSPAN does not support QoS shaping and policing.

Apart from the restrictions listed above, the following additional restrictions apply to Cisco Catalyst 9500X Series Switches:

- ERSPAN destination type/session is not supported.
- Filter-based ERSPAN is not supported.
- RSPAN is not supported.
- ERSPAN session do not capture CPU-originated traffic.
- ERSPAN source session in TX/egress direction is not supported.
- MTU size can be set up as 344 and 9000 bytes only. Any values between 344 and 9000 are not allowed.
- IPv4 Time to Live (TTL) and IPv4 Differentiated Services Code Point (DSCP) options are not supported.
- IPv6 TTL, IPv6 DSCP, and IPv6 flow label options are not supported.
- A source cannot be a part of more than one ERSPAN session.

Information about Configuring ERSPAN

The following sections provide information about configuring ERSPAN.

ERSPAN Overview

The Cisco ERSPAN feature allows you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports. ERSPAN sends traffic to a network analyzer, such as a Switch Probe device or a Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different devices, which help remote monitoring of multiple devices across a network.

ERSPAN supports encapsulated packets of up to 9180 bytes. ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session.

You can configure an ERSPAN source session, an ERSPAN destination session, or both on a device. A device on which only an ERSPAN source session is configured is called an ERSPAN source device. A device on which only an ERSPAN destination session is configured is called an ERSPAN termination device. A device can act as both; an ERSPAN source device and a termination device. To avoid over-subscription of traffic,

which can lead to drop in management traffic on the destination device, ensure that the destination session is configured and is working on the destination device, before configuring a source session on the source device.

For a source port or a source VLAN, the ERSPAN can monitor the ingress, egress, or both ingress and egress traffic. By default, ERSPAN monitors all traffic, including multicast, and Bridge Protocol Data Unit (BPDU) frames.

Note ERSPAN does not support monitoring multicast traffic on Cisco Catalyst 9500X Series Switches.

A device supports up to 66 sessions. A maximum of eight source sessions can be configured and the remaining sessions can be configured as RSPAN destinations sessions. A source session can be a local SPAN source session or an RSPAN source session or an ERSPAN source session. The number of source sessions decreases by the number of configured ERSPAN destination sessions.

A device can support a maximum of 50 Security Group Tag (SGT) filter per session.

An ERSPAN source session is defined by the following parameters:

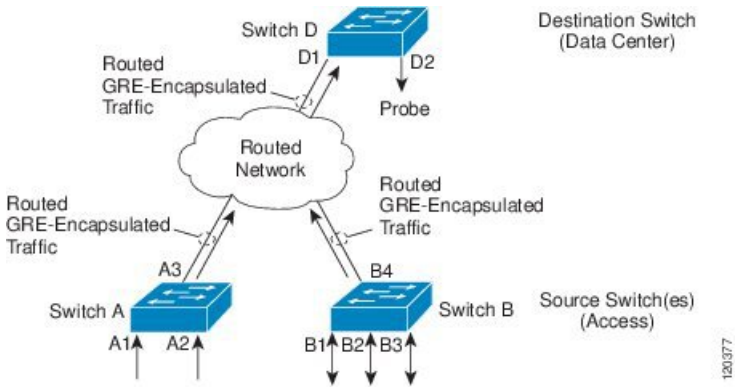
- A session ID.
- ERSPAN flow ID.
- List of source ports or source VLANs that are monitored by the session.
- Optional attributes, such as, IP type of service (ToS) and IP Time to Live (TTL), related to the Generic Routing Encapsulation (GRE) envelope.
- The destination and origin IP addresses. These are used as the destination and source IP addresses of the GRE envelope for the captured traffic, respectively.

Note

- ERSPAN source sessions do not copy ERSPAN GRE-encapsulated traffic from source ports. Each ERSPAN source session can have either ports or VLANs as sources, but not both.
- Because encapsulation and decapsulation are performed in the hardware, the CPU performance is not impacted.
- IPv4 and IPv6 delivery and transport headers are supported; including Type-II and Type-III headers.

  Cisco Catalyst 9500X Series Switches do not support Type-III headers.

Figure 1: ERSPAN Configuration



ERSPAN Sources

The Cisco ERSPAN feature supports the following sources:

- Source ports—A source port that is monitored for traffic analysis. Source ports in any VLAN can be configured and trunk ports can be configured as source ports along with nontrunk source ports.
- Source VLANs—A VLAN that is monitored for traffic analysis.

ERSPAN Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which ERSPAN source sends traffic for analysis.

When you configure a port as a destination port, it can no longer receive any traffic. The port is dedicated for use only by the ERSPAN feature. An ERSPAN destination port does not forward any traffic except that required for the ERSPAN session. You can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic.

SGT Based ERSPAN

A Security Group Tag (SGT) is a 16-bit value that the Cisco Identity Services Engine (ISE) assigns to the user or endpoint session upon login. The network infrastructure views the SGT as another attribute to assign to the session and inserts the Layer 2 tag to all traffic from that session. A platform can support a maximum of 50 SGT policies per session.

On an existing flow-based SPAN (FSPAN) or VLAN filter session, SGT filtering configurations are not allowed.

Note SGT filtering configuration is not supported on Cisco Catalyst 9500 Series Switches.

ERSPAN Timestamp

ERSPAN Timestamp is automatically enabled when the ERSPAN header is set to type III. The timestamp field is used to calculate packet latency in devices. The ERSPAN source session fills in the timestamp field with local time information when a packet is received. The destination session can hand over this timestamp to the application. ERSPAN supports all timestamps in 32-bit format. It supports 100 nanosecond (ns) granularity and the timestamp field wraparound time is around 7 minutes.

ERSPAN over MPLS VPN

Starting with the Cisco IOS XE Bengaluru 17.5.x release, you can transport ERSPAN traffic over a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). To enable ERSPAN over MPLS VPN you will have to enable Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP), and Cisco Express Forwarding in your network.

You can configure the ERSPAN destination to select the source VRF for the ERSPAN traffic over MPLS VPN. You can use the **vrf** keyword in the ERSPAN destination session source command to configure the source VRF.

How to Configure ERSPAN

The following sections provide information about how to configure ERSPAN.

Configuring an ERSPAN Source Session (IPv4)

The ERSPAN source session defines the session configuration parameters and the ports or VLANs to be monitored. To define an IPv4 ERSPAN source session, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *span-session-number* **type erspan-source** **Example:** `Device(config)# monitor session 1 type erspan-source`	Defines an ERSPAN source session using the session ID and the session type, and enters ERSPAN monitor source session configuration mode. • The *span-session-number* argument range is from 1 to 66. The same session number cannot be used more than once.

	Command or Action	Purpose
		• The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types. • The session ID (configured by the *span-session-number* argument) and the session type (configured by the **erspan-source** keyword) cannot be changed once entered. Use the **no** form of this command to remove the session and then re-create the session, with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-src)# description source1`	(Optional) Describes the ERSPAN source session. • The *string* argument can be up to 240 characters and cannot contain special characters or spaces.
Step 5	[**no**] **header-type 3** **Example:** `Device(config-mon-erspan-src)# header-type 3`	(Optional) Configures a switch to Type-III ERSPAN header. The default type is Type-II ERSPAN header. **Note** Type-III headers are not supported on Cisco Catalyst 9500X Series Switches.
Step 6	**source** {**interface** *interface-type interface-number* | **vlan** *vlan-id*} [**,** | **-** | **both** | **rx** | **tx**] **Example:** `Device(config-mon-erspan-src)# source interface fastethernet 0/1 rx`	Configures the source interface or the VLAN, and the traffic direction to be monitored. **Note** The **both** and **tx** options are not supported on Cisco Catalyst 9500X Series Switches.
Step 7	**filter** {**ip access-group** {*standard-access-list* | *expanded-access-list* | *acl-name* } | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **sgt** *sgt-ID* [**,** | **-**] | **vlan** *vlan-ID* [**,** | **-**]} **Example:** `Switch(config-mon-erspan-src)# filter vlan 3`	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port. The **filter sgt** *sgt-ID* command configures SGT filtering in the ERSPAN source session. **Note** • You cannot include source VLANs and filter VLANs in the same session. • Flow-based SPAN (FSPAN) session and SGT filtering configuration are not supported on Cisco Catalyst 9500X Series Switches

	Command or Action	Purpose
Step 8	**destination** **Example:** `Device(config-mon-erspan-src)# destination`	Enters ERSPAN source session destination configuration mode.
Step 9	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-src-dst)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN destination session configuration.
Step 10	**ip address** *ip-address* **Example:** `Device(config-mon-erspan-src-dst)# ip address 10.1.0.2`	Configures the IP address that is used as the destination of the ERSPAN traffic.
Step 11	**ip dscp** *dscp-value* **Example:** `Device(config-mon-erspan-src-dst)# ip dscp 10`	(Optional) Enables the use of IP differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel. **Note** The **ip dscp** command is not supported on Cisco Catalyst 9500X Series Switches.
Step 12	**ip ttl** *ttl-value* **Example:** `Device(config-mon-erspan-src-dst)# ip ttl 32`	(Optional) Configures the IP TTL value of packets in the ERSPAN traffic. **Note** The **ip ttl** command is not supported on Cisco Catalyst 9500X Series Switches.
Step 13	**mtu** *mtu-size* **Example:** `Device(config-mon-erspan-src-dst)# mtu 512`	Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 176 to 9000 bytes. The default value is 9000 bytes. On Cisco Catalyst 9500X Series Switches, MTU size can be set up as 344 and 9000 bytes only.
Step 14	**origin ip-address** *ip-address* **Example:** `Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1`	Configures the IP address used as the source of the ERSPAN traffic.
Step 15	**vrf** *vrf-id* **Example:**	(Optional) Configures the VRF name to use instead of the global routing table.

	Command or Action	Purpose
	`Device(config-mon-erspan-src-dst)# vrf 1`	
Step 16	**exit** **Example:** `Device(config-mon-erspan-src-dst)# exit`	Exits ERSPAN source session destination configuration mode, and returns to ERSPAN source session configuration mode.
Step 17	**no shutdown** **Example:** `Device(config-mon-erspan-src)# no shutdown`	Enables the configured sessions on an interface.
Step 18	**end** **Example:** `Device(config-mon-erspan-src)# end`	Exits ERSPAN source session configuration mode, and returns to privileged EXEC mode.

Configuring an ERSPAN Destination Session (IPv4)

The ERSPAN destination session defines the session configuration parameters and the ports that receive the monitored traffic.

Note C9500X-28C8D model of Cisco Catalyst 9500 Series Switches do not support IPv4 ERSPAN destination type/session.

To define an IPv4 ERSPAN destination session, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *session-number* **type erspan-destination** **Example:** `Device(config)# monitor session 1 type erspan-destination`	Defines an ERSPAN destination session using the session ID and the session type, and enters ERSPAN monitor destination session configuration mode. • The *session-number* argument range is from 1 – 66. The session number must be

	Command or Action	Purpose
		unique and cannot be used more than once. • The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types. • The session ID (configured by the *session-number* argument) and the session type (configured by the **erspan-destination**) cannot be changed once entered. Use the **no** form of this command to remove the session, and then recreate the session with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-dst)# description source1`	(Optional) Describes the ERSPAN destination session. • The *string* argument can be up to 240 characters in length and cannot contain special characters or spaces.
Step 5	**destination interface** *interface-type interface-number* **Example:** `Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1`	Associates the ERSPAN destination session number with source ports, and selects the traffic direction to be monitored.
Step 6	**source** **Example:** `Device(config-mon-erspan-dst)# source`	Enters ERSPAN destination session source configuration mode.
Step 7	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-dst-src)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN source session configuration.
Step 8	**ip address** *ip-address* [**force**] **Example:** `Device(config-mon-erspan-dst-src)# ip address 10.1.0.2`	Configures the IP address that is used as the destination of the ERSPAN traffic. • This IP address must be an address on a local interface or loopback interface, and match the address on the destination switch. • The **ip address** *ip-address* **force** command changes the destination IP

	Command or Action	Purpose
		address for all ERSPAN destination sessions.
Step 9	**vrf** *vrf-id* **Example:** `Device(config-mon-erspan-dst-src)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.
Step 10	**no shutdown** **Example:** `Device(config-mon-erspan-dst-src)# no shutdown`	Enables the configured sessions on an interface.
Step 11	**end** **Example:** `Device(config-mon-erspan-dst-src)# end`	Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode.

Configuring an ERSPAN Source Session (IPv6)

The ERSPAN source session defines the session configuration parameters and the ports or VLANs to be monitored. To define an IPv6 ERSPAN source session, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 3	**monitor session** *session-number* **type erspan-source** **Example:** `Device(config)# monitor session 1 type erspan-source`	Defines an ERSPAN source session using the session ID and the session type, and enters ERSPAN monitor source session configuration mode. • The *span-session-number* range is from 1 to 66. The same session number cannot be used more than once. • The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types.

	Command or Action	Purpose
		• The session ID (configured by the *span-session-number* argument) and the session type (configured by the **erspan-source** keyword) cannot be changed once entered. Use the **no** form of this command to remove the session and then re-create the session, with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-src)# description source1`	(Optional) Describes the ERSPAN source session. • The *string* argument can be up to 240 characters and cannot contain special characters or spaces.
Step 5	[**no**] **header-type 3** **Example:** `Device(config-mon-erspan-src)# header-type 3`	(Optional) Configures a switch to Type-III ERSPAN header. The default type is Type-II ERSPAN header. **Note** Type-III headers are not supported on Cisco Catalyst 9500X Series Switches.
Step 6	**source** {**interface** *interface-type interface-number* | **vlan** *vlan-id*} [**,** | **-** | **both** | **rx** | **tx**] **Example:** `Device(config-mon-erspan-src)# source interface fortygigabitethernet 1/0/3`	Configures the source interface or the VLAN, and the traffic direction to be monitored. **Note** The **both** and **tx** options are not supported on Cisco Catalyst 9500X Series Switches.
Step 7	**filter** {**ip access-group** {*standard-access-list* | *expanded-access-list* | *acl-name* } | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **sgt** *sgt-ID* [**,** | **-**] | **vlan** *vlan-ID* [**,** | **-**]} **Example:** `Switch(config-mon-erspan-src)# filter ipv6 access-group exampleacl`	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port. The **filter sgt** *sgt-ID* command configures SGT filtering in the ERSPAN source session. **Note** • You cannot include source VLANs and filter VLANs in the same session. • Flow-based SPAN (FSPAN) session and SGT filtering configuration are not supported on Cisco Catalyst 9500X Series Switches
Step 8	**destination** **Example:** `Device(config-mon-erspan-src)# destination`	Enters ERSPAN source session destination configuration mode.

	Command or Action	Purpose
Step 9	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-src-dst)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN destination session configuration.
Step 10	**ipv6 address** *ipv6-address* **Example:** `Device(config-mon-erspan-src-dst)# ipv6 address 2001:DB8::1`	Configures the IPv6 address that is used as the destination of the ERSPAN traffic.
Step 11	**ipv6 dscp** *dscp-value* **Example:** `Device(config-mon-erspan-src-dst)# ipv6 dscp 2`	(Optional) Enables the use of IPv6 differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel. **Note** The **ipv6 dscp** command is not supported on Cisco Catalyst 9500X Series Switches.
Step 12	**ipv6 ttl** *ttl-value* **Example:** `Device(config-mon-erspan-src-dst)# ipv6 ttl 4`	(Optional) Configures the IPv6 TTL value of packets in the ERSPAN traffic. **Note** The **ipv6 ttl** command is not supported on Cisco Catalyst 9500X Series Switches.
Step 13	**ipv6 flow-label** *flow-label-value* **Example:** `Device(config-mon-erspan-src-dst)# ipv6 flow-label 2`	(Optional) Configures the IPv6 flow label in the ERSPAN traffic. *flow-label-value*: The range is from 0 to 1048575. **Note** The **ipv6 flow-label** command is not supported on Cisco Catalyst 9500X Series Switches.
Step 14	**mtu** *mtu-size* **Example:** `Device(config-mon-erspan-src-dst)# mtu 512`	Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 176 to 9000 bytes. The default value is 9000 bytes. On Cisco Catalyst 9500X Series Switches, MTU size can be set up as 344 and 9000 bytes only.
Step 15	**origin ipv6-address** *ipv6-address* **Example:**	Configures the IPv6 address used as the source of the ERSPAN traffic.

	Command or Action	Purpose
	`Device(config-mon-erspan-src-dst)# origin ipv6 address 2001:DB8:1::1`	
Step 16	**vrf** *vrf-id* **Example:** `Device(config-mon-erspan-src-dst)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.
Step 17	**exit** **Example:** `Device(config-mon-erspan-src-dst)# exit`	Exits ERSPAN source session destination configuration mode, and returns to ERSPAN source session configuration mode.
Step 18	**no shutdown** **Example:** `Device(config-mon-erspan-src)# no shutdown`	Enables the configured sessions on an interface.
Step 19	**end** **Example:** `Device(config-mon-erspan-src)# end`	Exits ERSPAN source session configuration mode, and returns to privileged EXEC mode.

Configuring an ERSPAN Destination Session (IPv6)

The ERSPAN destination session defines the session configuration parameters and the ports that receives the monitored traffic. To define an IPv6 ERSPAN destination session, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *session-number* **type erspan-destination** **Example:** `Device(config)# monitor session 3 type erspan-destination`	Defines an ERSPAN destination session using the session ID and the session type, and enters ERSPAN monitor destination session configuration mode. • The *session-number* argument range is from 1 to 66. The session number must be unique and cannot be used more than once.

	Command or Action	Purpose
		• The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types. • The session ID (configured by the *session-number* argument) and the session type (configured by the **erspan-destination**) cannot be changed once entered. Use the **no** form of this command to remove the session, and then recreate the session with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-dst)# description source 1`	(Optional) Describes the ERSPAN destination session. • The *string* argument can be up to 240 characters in length and cannot contain special characters or spaces.
Step 5	**destination interface** *interface-type interface-number* **Example:** `Device(config-mon-erspan-dst)# destination interface fortygigabitethernet 1/0/3`	Associates the ERSPAN destination session number with source ports, and selects the traffic direction to be monitored.
Step 6	**source** **Example:** `Device(config-mon-erspan-dst)# source`	Enters ERSPAN destination session source configuration mode.
Step 7	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-dst-src)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN source session configuration.
Step 8	**ipv6 address** *ipv6-address* **Example:** `Device(config-mon-erspan-dst-src)# ip address 2001:DB8::1`	Configures the IPv6 address that is used as the destination of the ERSPAN traffic. This IPv6 address must be an address on a local interface or loopback interface, and match the address on the destination switch.
Step 9	**exit** **Example:** `Switch(config-mon-erspan-dst-src)#exit`	Exits ERSPAN destination session source configuration mode, and returns to ERSPAN destination session configuration mode.

	Command or Action	Purpose
Step 10	**no shutdown** **Example:** `Device(config-mon-erspan-dst)# no shutdown`	Enables the configured sessions on an interface.
Step 11	**end** **Example:** `Device(config-mon-erspan-dst)# end`	Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode.

Configuration examples for ERSPAN

The following sections provide configuration examples for ERSPAN.

Example: Configuring an ERSPAN Source Session

The following example shows how to configure an ERSPAN source session:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# ip address 10.1.0.2
Device(config-mon-erspan-src-dst)# ip dscp 10
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 512
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf monitoring
Device(config-mon-erspan-src-dst)# exit
Device(config-mon-erspan-src)# no shutdown
Device(config-mon-erspan-src)# end
```

Example: Configuring an ERSPAN Destination Session

The following example shows how to configure an ERSPAN destination session:

```
Device(config)# monitor session 2 type erspan-destination
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/3/2
Device(config-mon-erspan-dst)# destination interface GigabitEthernet2/2/0
Device(config-mon-erspan-dst)# source
Device(config-mon-erspan-dst-src)# erspan-id 100
Device(config-mon-erspan-dst-src)# ip address 10.1.0.2
```

The following example shows how to configure a source VRF for an ERSPAN destination session:

```
Device(config)# monitor session 2 type erspan-destination
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/3/2
Device(config-mon-erspan-dst)# destination interface GigabitEthernet2/2/0
Device(config-mon-erspan-dst)# source
Device(config-mon-erspan-dst-src)# erspan-id 100
Device(config-mon-erspan-dst-src)# ip address 10.1.0.2
Device(config-mon-erspan-dst-src)# vrf 1
```

Verifying ERSPAN

To verify the ERSPAN configuration, use the following commands:

The following is sample output from the **show monitor session** command:

```
Device# show monitor session 53

Session 53
----------
Type                    : ERSPAN Source Session
Status                  : Admin Enabled
Source Ports            :
MTU                     : Fo1/0/2
```

The following is sample output from the **show platform software monitor session** command:

```
Device# show platform software monitor session 53

Span Session 53 (FED Session 0):
Type: ERSPAN Source
Prev type: Unknown
Ingress Src Ports:
Egress Src Ports:
Ingress Local Src Ports: (null)
Egress Local Src Ports: (null)
Destination Ports:
Ingress Src Vlans:
Egress Src Vlans:
Ingress Up Src Vlans: (null)
Egress Up Src Vlans: (null)
Src Trunk filter Vlans:
RSPAN dst vlan: 0
RSPAN src vlan: 0
RSPAN src vlan sav: 0
Dest port encap = 0x0000
Dest port ingress encap = 0x0000
Dest port ingress vlan = 0x0
SrcSess: 1 DstSess: 0 DstPortCfgd: 0 RspnDstCfg: 0 RspnSrcVld: 0
DstCliCfg: 0 DstPrtInit: 0 PsLclCfgd: 0
Flags: 0x00000000
Remote dest port: 0 Dest port group: 0
FSPAN disabled
FSPAN not notified
ERSPAN Id : 0
ERSPAN Org Ip: 0.0.0.0
ERSPAN Dst Ip: 0.0.0.0
ERSPAN Ip Ttl: 255
ERSPAN DSCP : 0
ERSPAN MTU : 1500 >>>>
ERSPAN VRFID : 0
ERSPAN State : Disabled
```

```
ERSPAN Tun id: 61
ERSPAN header-type: 2
ERSPAN SGT :
```

The following is sample output from the **show monitor session erspan-source detail** command:

```
Device# show monitor session erspan-source detail

Type                    : ERSPAN Source Session
Status                  : Admin Enabled
Description             : -
Source Ports            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source Subinterfaces    :
    RX Only             : None
    TX Only             : None
    Both                : None
Source VLANs            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source Drop-cause       : None
Source EFPs             :
    RX Only             : None
    TX Only             : None
    Both                : None
Source RSPAN VLAN       : None
Destination Ports       : None
Filter VLANs            : None
Filter SGT              : None
Dest RSPAN VLAN         : None
IP Access-group         : None
MAC Access-group        : None
IPv6 Access-group       : None
Filter access-group  :None
smac for wan interface  : None
dmac for wan interface  : None
Destination IP Address  : 192.0.2.1
Destination IPv6 Address : None
Destination IP VRF      : None
MTU                     : 1500
Destination ERSPAN ID   : 251
Origin IP Address       : 10.10.10.216
Origin IPv6 Address     : None
IP QOS PREC             : 0
IPv6 Flow Label         : None
IP TTL                  : 255
ERSPAN header-type      : 3
```

The following output from the **show capability feature monitor erspan-source** command displays information about the configured ERSPAN source sessions:

```
Device# show capability feature monitor erspan-source

ERSPAN Source Session:ERSPAN Source Session Supported: TRUE
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II and III
ACL filter Supported: TRUE
SGT filter Supported: TRUE
Fragmentation Supported: TRUE
```

```
Truncation Supported: FALSE
Sequence number Supported: FALSE
QOS Supported: TRUE
```

The following output from the **show capability feature monitor erspan-source** command displays information about the configured ERSPAN source sessions for C9500X-28C8D model of Cisco Catalyst 9500 Series Switches:

```
Device#show capability feature monitor erspan-source
ERSPAN Source Session:ERSPAN Source Session Supported: TRUE
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: FALSE
SGT filter Supported: FALSE
Fragmentation Supported: TRUE
Truncation Supported: TRUE
Sequence number Supported: FALSE
QOS Supported: FALSE
```

The following output from the **show capability feature monitor erspan-destination** command displays all the configured global built-in templates:

```
Device# show capability feature monitor erspan-destination

ERSPAN Destination Session:ERSPAN Destination Session Supported: TRUE
Maximum No of ERSPAN destination session: 8
ERSPAN Header Type supported: II and III
```

Since ERSPAN destination session/type is not supported on C9500X-28C8D model of Cisco Catalyst 9500 Series Switches, the following is the output from the **show capability feature monitor erspan-destination**:

```
Device# show capability feature monitor erspan-destination
ERSPAN Destination Session:ERSPAN Destination Session Supported: FALSE
```

Additional References

RFCs

Standard/RFC	Title
RFC 2784	Generic Routing Encapsulation (GRE)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for ERSPAN

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	ERSPAN	The Cisco ERSPAN feature allows you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports. ERSPAN sends traffic to a network analyzer, such as a Switch Probe device or a Remote Monitoring (RMON) probe. This feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models.
Cisco IOS XE Fuji 16.8.1a	ERSPAN	This feature was implemented on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models.
Cisco IOS XE Gibraltar 16.10.1	ERSPAN truncation and timestamp	Support of ERSPAN truncation and timestamp was introduced.
Cisco IOS XE Gibraltar 16.11.1	ERSPAN -support for Destination Sessions	The ERSPAN destination session defines the session configuration parameters and the ports that receive the monitored traffic.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.1.1	ERSPAN IPv6	IPv6 support was introduced for ERSPAN. This enables configuration of an IPv6 ERSPAN source and destination session.
Cisco IOS XE Bengaluru 17.5.1	ERSPAN over MPLS VPN	MPLS VPN support was introduced for ERSPAN. ERSPAN traffic can be transported over an MPLS VPN. Support for ERSPAN is limited to L3VPN IPV4 MPLS.
Cisco IOS XE Dublin 17.11.1	ERSPAN	This feature was implemented on the C9500X-28C8D model.
Cisco IOS XE Dublin 17.10.1b	ERSPAN	This feature was implemented on the C9500X-60L4D model.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.