Configuring ERSPAN

Configuring ERSPAN

This module describes how to configure the Encapsulated Remote Switched Port Analyzer (ERSPAN). The Cisco ERSPAN feature allows you to monitor traffic on ports or VLANs and send the monitored traffic to destination ports.

Prerequisites for Configuring ERSPAN

• Access control list (ACL) filter is applied before sending the monitored traffic on to the tunnel.

Restrictions for Configuring ERSPAN

The following restrictions apply for this feature:

• Truncation is supported on IPv4 spanned packets only.

> **Note** Truncation is supported only on the Cisco Catalyst 9500 High Performance Series Switches.

• The **sgt**, **dscp**, **vrf**, **header-type 3** commands, Type-III ERSPAN header, and ERSPAN destination sessions are supported only on Cisco Catalyst 9500 Series Switches - High Performance.

• An ERSPAN destination interface can be part of only one session. The same destination interface cannot be configured for multiple ERSPANs/SPANs.

• You can configure either a list of ports or a list of VLANs as a source, but cannot configure both for a given session.

• Filter IP/IPv6/MAC/VLAN access-group and filter SGT cannot be configured at the same time.

• 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 RSPAN VLAN traffic from source trunk ports that carry RSPAN VLANs.

- 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.

Information for 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 helps 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, and 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.

A device supports up to 66 sessions. A maximum of 8 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 to be monitored by the session

- Optional attributes, such as, IP type of service (ToS) and IP Time to Live (TTL), related to the GRE envelope

- The destination and origin IP addresses, which are used as the destination and source IP addresses of the generic routing encapsulation (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.

- Only IPv4 delivery/transport header is supported.

Figure 1: ERSPAN Configuration
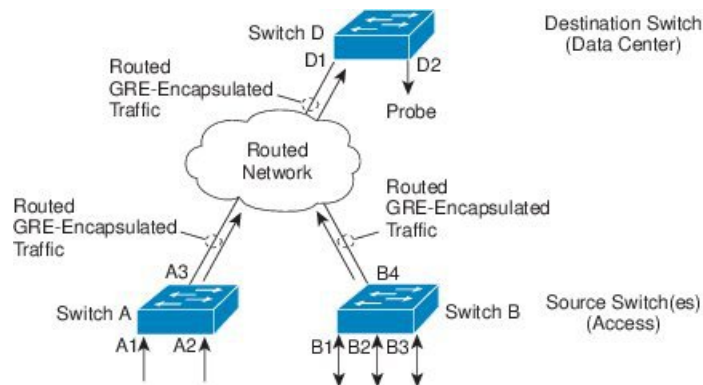
ERSPAN Sources

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, and 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.

How to Configure ERSPAN

Configuring an ERSPAN Source Session

The ERSPAN source session defines the session configuration parameters and the ports or VLANs to be monitored.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type* *interface-number*
4. **monitor session** *span-session-number* **type** **erspan-source**
5. **description** *string*
6. [**no**] **header-type 3**
7. **source** {**interface** *interface-type* *interface-number* | **vlan** *vlan-id*} [**,** | **-** | **both** | **rx** | **tx**]
8. **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* [**,** | **-**]}
9. **destination**
10. **erspan-id** *erspan-flow-id*
11. **ip address** *ip-address*
12. **ip dscp** *dscp-value*
13. **ip ttl** *ttl-value*
14. **mtu** *mtu-size*
15. **origin ip-address** *ip-address*
16. **vrf** *vrf-id*
17. **exit**
18. **no** **shutdown**
19. **end**

DETAILED STEPS

	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	**interface** *interface-type* *interface-number* **Example:** `Device(config)# interface GigabitEthernet 1/0/1`	Specifies the interface on which ERSPAN source session is configured.

	Command or Action	**Purpose**
Step 4	**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. • 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 5	**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 6	[**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.
Step 7	**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.
Step 8	**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.
Step 9	**destination** **Example:** Device(config-mon-erspan-src)# destination	Enters ERSPAN source session destination configuration mode.

	Command or Action	Purpose
Step 10	**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 11	**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 12	**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.
Step 13	**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.
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.
Step 15	**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 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 (IPv4)

The ERSPAN destination session defines the session configuration parameters and the ports that receives the monitored traffic. To define an IPv4 ERSPAN destination session, complete the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *session-number* **type erspan-destination**
4. **description** *string*
5. **destination interface** *interface-type interface-number*
6. **source**
7. **erspan-id** *erspan-flow-id*
8. **ip address** *ip-address* [**force**]
9. **no shutdown**
10. **end**

DETAILED STEPS

	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 to 66. The session number must be 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*	(Optional) Describes the ERSPAN destination session.

	Command or Action	Purpose
	Example: Device(config-mon-erspan-dst)# description source1	• 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 address for all ERSPAN destination sessions.
Step 9	**no shutdown** **Example:** Device(config-mon-erspan-dst-src)# no shutdown	Enables the configured sessions on an interface.
Step 10	**end** **Example:** Device(config-mon-erspan-dst-src)# end	Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode.

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
```

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-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
```

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 Information for Configuring ERSPAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring ERSPAN

Feature Name	Releases	Feature Information
ERSPAN	Cisco IOS XE Everest 16.5.1a	This feature was introduced.
ERSPAN	Cisco IOS XE Fuji 16.9.1	Support of destination sessions was introduced. The **vrf** and **ip dscp** commands, and the **sgt** keyword were introduced. ERSPAN has been enhanced to configure a device to Type-III header. The **header-type 3** command was introduced. These were implemented on the Cisco Catalyst 9500 Series High Performance Switches.
ERSPAN truncation and timestamp	Cisco IOS XE Gibraltar 16.10.1	Support of ERSPAN truncation and timestamp was introduced. The **mtu** command was introduced. These were implemented on the Cisco Catalyst 9500 Series High Performance Switches.
ERSPAN	Cisco IOS XE Gibraltar 16.11.1	Support of destination sessions was introduced. The **vrf** and **ip dscp** commands, and the **sgt** keyword were introduced. ERSPAN has been enhanced to configure a device to Type-III header. The **header-type 3** command was introduced. Support of ERSPAN truncation and timestamp was introduced. The **mtu** command was introduced. These were implemented on the Cisco Catalyst 9500 Series Switches.