Configuring ERSPAN

This module describes how to configure 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.

Note The ERSPAN feature is not supported on Layer 2 switching interfaces.

This module describes the feature and consists of these sections:

Note For complete syntax and usage information for the switch commands used in this chapter, see the Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch.

If a command is not in the *Cisco Catalyst 4500 Series Switch Command Reference* , you can locate it in the Cisco IOS Master Command List, All Releases.

Prerequisites for ERSPAN

- Only IPv4 delivery/transport header is supported.
- Access control list (ACL) filter is applied before sending the monitored traffic on to the tunnel.
- Only supports Type-II ERSPAN header.
- The extended VLAN ID that is reserved for each ERSPAN session cannot be used for any other purpose, until the ERSPAN source session is present in the configuration. Use the **show vlan internal usage** command to display the extended VLAN ID.
- This feature is supported on Cisco Catalyst 4500-E Supervisor Engines 7-E, 7L-E, 8-E, 8L-E, and 4500-X Series Switches.

Restrictions for ERSPAN

The following restrictions apply for this feature:

- The maximum number of available ports for each ERSPAN session is 128.

- A maximum of 8 ingress and 8 egress ERSPAN sessions (a total of 16 sessions) are supported.

- 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 configuration commands to remove the session and then reconfigure the session.

- ERSPAN source sessions do not copy locally-sourced Remote SPAN (RSPAN) VLAN traffic from source trunk ports that carry RSPAN VLANs.

- ERSPAN source sessions do not copy locally-sourced ERSPAN GRE-encapsulated traffic from source ports.

The Catalyst 4500 series switches do not support the following for this feature:

- ERSPAN destination type.

- Timestamp indication in the ERSPAN header.

- Bad/Short/Oversized (BSO) packet indication in the ERSPAN header.

- The original VLAN ID or Class of Service (COS) in the ERSPAN header.

- Generic routing encapsulation (GRE) header flags.

- GRE header sequence number or key.

- Maximum transmission unit (MTU) checking and fragmentation. Hence, traffic exceeding the configured MTU size (as determined by Layer 3 protocols) is dropped.

- Truncation of the original packet; because of which the T-bit in the ERSPAN header is always zero.

- Setting of the Differentiated Services Code Point (DSCP)/Time to Live (TTL) field for IP encapsulation differently for various ERSPAN source sessions. Use the **erspan** {**ttl** | **tos**} command to set these values. The configured values are used in all ERSPAN source sessions originating from the device.

- Simple Network Management Protocol (SNMP).

Information About 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.

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.

> **Note**   Catalyst 4500 series switches do not support ERSAPN destination type/session.

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.

An ERSPAN source session is defined by the following parameters:

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

> **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.
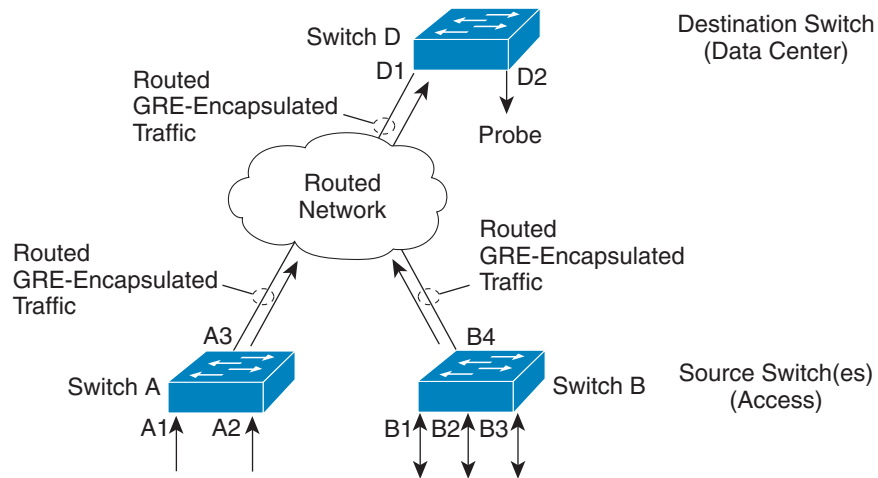
An ERSPAN destination session is defined by the following parameters:

- Session ID
- Destination ports
- Source IP address, which is the same as the destination IP address of the corresponding source session
- ERSPAN flow ID, which is used to match the destination session with the source session
- The ERSPAN source sessions copy traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destination ports

> **Note**   Because encapsulation is performed in the hardware, the CPU performance is not impacted.

Figure 62-1   ERSPAN Configuration

ERSAN 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.

The following tunnel interfaces are supported as source ports for a source session:

- GRE

- IPv6

- IPv6-over-IP tunnel

- Multipoint GRE (mGRE)

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.

	Command or Action	Purpose
Step 1	Switch> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	Switch# **configure terminal**	Enters global configuration mode.
Step 3	Switch(config)# **monitor session** *span-session-number* **type erspan-source**	Defines an ERSPAN source session using the session ID and the session type, and enters ERSPAN monitor source session configuration mode. • 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 *span-session-number* and the session type (configured by the **erspan-source** keyword) cannot be changed once configured. 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	Switch(config-mon-erspan-src)# **description** *description*	Describes the ERSPAN source session.
Step 5	Switch(config-mon-erspan-src)# **source** {**interface** *type number* | **vlan** *vlan-ID*} [, | - | *both* | *rx* | *tx*]	Configures the source interface or the VLAN, and the traffic direction to be monitored.
Step 6	Switch(config-mon-erspan-src)# **filter** {**ip** {*standard-access-list* | *expanded-access-list* | *acl-name*} | **ipv6** {**access-group** *acl-name*} | **vlan** *vlan-ID*}	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port. ✎ **Note** You cannot include source VLANs and filter VLANs in the same session.
Step 7	Switch(config-mon-erspan-src)# **no shutdown**	Disables the shutting down of the configured session.
Step 8	Switch(config-mon-erspan-src)# **destination**	Defines an ERSPAN destination session and enters ERSPAN monitor destination session configuration mode.
Step 9	Switch(config-mon-erspan-src-dst)# **ip address** *ip-address*	Configures an IP address for the ERSPAN destination session.
Step 10	Switch(config-mon-erspan-src-dst)# **erspan-id** *erspan-ID*	Configures the ID used by the destination session to identify the ERSPAN traffic.
Step 11	Switch(config-mon-erspan-src-dst)# **origin ip address** *ip-address*	Configures the IP address used as the source for the ERSPAN traffic.

	Command or Action	Purpose
Step 12	`Switch(config-mon-erspan-src-dst)# vrf vrf-ID`	(Optional) Configures the VRF name to use instead of the global routing table.
Step 13	`Switch(config-mon-erspan-src-dst)# exit`	Exits ERSPAN monitor destination session configuration mode and returns to ERSPAN monitor source session configuration mode.
Step 14	`Switch(config-mon-erspan-src)# exit`	Exits ERSPAN monitor source session configuration mode and returns to privileged EXEC mode.
Step 15	`Switch(config)# erspan {tos tos-value | ttl ttl-value}`	Configures type of service (ToS) and Time to Live (TTL) values for packets in the ERSPAN traffic. **Note** The configured ToS and TTL values apply to all configured ERSPAN sessions. The ToS and TTL values for ERSPAN are configured in global configuration mode.
Step 16	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for ERSPAN

Example: Configuring an ERSAPN Source Session

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 type erspan-source
Switch(config-mon-erspan-src)# description source1
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
Switch(config-mon-erspan-src)# filter vlan 3
Switch(config-mon-erspan-src)# no shutdown
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip address 192.0.2.9
Switch(config-mon-erspan-src-dst)# erspan-id 2
Switch(config-mon-erspan-src-dst)# origin ip address 203.0.113.2
Switch(config-mon-erspan-src-dst)# vrf 1
Switch(config-mon-erspan-src)# exit
Switch(config)# erspan ttl 32
Switch(config)# end
Switch#
```

Verifying ERSPAN

To verify the ERSPAN configuration, use the following commands:

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

```
Switch# show monitor session erspan-source session

Type : ERSPAN Source Session
```

```
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

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

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


Type : ERSPAN Source Session
Status : Admin Enabled
Description : -
Source Ports :
RX Only : Gi1/4/33
TX Only : None
Both : None
Source VLANs :
RX Only : None
TX Only : None
Both : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs : None
Filter Addr Type :
RX Only : None
TX Only : None
Both : None
Filter Pkt Type :
RX Only : None
Dest RSPAN VLAN : None
IP Access-group : None
IPv6 Access-group : None
Destination IP Address : 20.20.163.20
Destination IPv6 Address : None
Destination IP VRF : None
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
Origin IPv6 Address : None
IP QOS PREC : 0
IPv6 Flow Label : None
IP TTL : 255
```

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

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

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: true
Fragmentation Supported: false
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:

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

ERSPAN Destination Session Supported: false
```

Additional References for Configuring ERSPAN

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Catalyst 4500 switch commands	*Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch*

Standards & MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2784	Generic Routing Encapsulation (GRE)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ERSPAN

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note   Table 1 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.

Table 1   Feature Information for ERSPAN

Feature Name	Releases	Feature Information
ERSPAN	Cisco IOS Release 15.2(4)E1	This module describes how to configure 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 over a generic routing encapsulation (GRE) tunnel in any VRF. The following commands were introduced or modified: **destination (ERSPAN)**, **erspan, filter (ERSPAN),** and **show capability feature monitor**.