

# Configuring ERSPAN

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

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


- 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 12
- Additional References for Configuring ERSPAN, on page 14
- Feature Information for Configuring ERSPAN , on page 15


# Restrictions for Configuring ERSPAN

- The maximum number of allowed ERSPAN sessions on a Cisco ASR 1000 Series Router is 1024. A Cisco ASR 1000 Series Router can be used as an ERSPAN source device on which only source sessions are configured, an ERSPAN destination device on which only destination sessions are configured, or an ERSPAN source and destination device on which both source and destination sessions are configured. However, total number of sessions must not exceed 1024.
- The maximum number of available ports for each ERSPAN session is 128.
- ERSPAN on Cisco ASR 1000 Series Routers supports only Fast Ethernet, Gigabit Ethernet, TenGigabit Ethernet, and port-channel interfaces as source ports for a source session.
- ERSPAN on Cisco ASR 1000 Series Routers supports only Layer 3 interfaces. Ethernet interfaces are not supported on ERSPAN when configured as Layer 2 interfaces.
- ERSPAN users on Cisco ASR 1000 Series Routers can configure a list of ports as a source or a list of VLANs as a source, but cannot configure both for a given session.
- When a session is configured through the ERSPAN configuration CLI, the session ID and the session type cannot be changed. To change them, you must first use the **no** form of the configuration command to remove the session and then reconfigure the session.

- The **monitor session** *span-session-number* **type local** command is not supported on Cisco ASR 1000 Series Routers.
- The filter VLAN option is not functional in an ERSPAN monitoring session on WAN interfaces.

# Information About Configuring ERSPAN

## ERSPAN Overview

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

On a Cisco ASR 1000 Series Router, ERSPAN supports encapsulated packets of up to 9180 bytes. The default ERSPAN maximum transmission unit (MTU) size is 1500 bytes. If the ERSPAN payload length, which comprises the encapsulated IPv4 header, generic routing encapsulation (GRE) header, ERSPAN header, and the original packet, exceeds the ERSPAN MTU size, the replicated packet is truncated to the default ERSPAN MTU size.

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 Cisco ASR 1000 Series Router. A device that has only an ERSPAN source session configured is called an ERSPAN source device, and a device that has only an ERSPAN destination session configured is called an ERSPAN termination device. A Cisco ASR 1000 Series Router can act as both an ERSPAN source device and an ERSPAN termination device. You can terminate an ERSPAN session with a destination session on the same Cisco ASR 1000 Series Router.

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

An ERSPAN destination session is defined by the following:

- 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

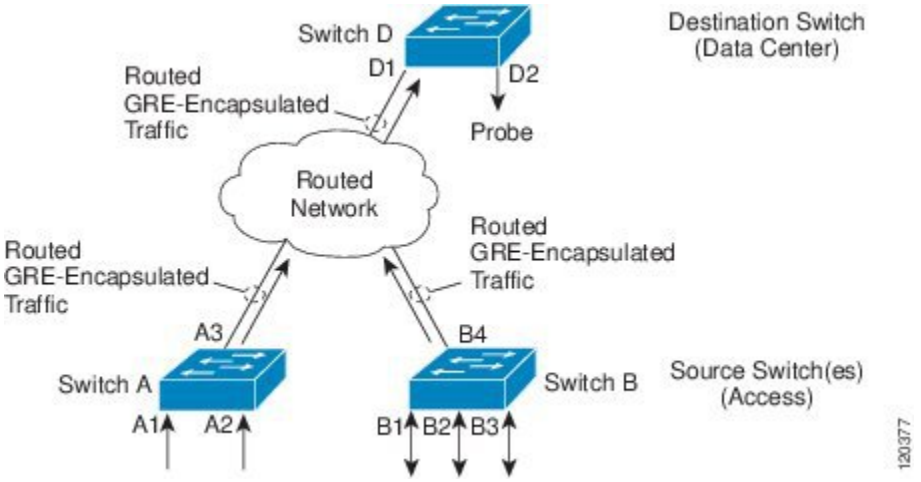
ERSPAN source sessions do not copy ERSPAN GRE-encapsulated traffic from source ports. Each ERSPAN source session can have either ports or VLANs as sources, but not both.

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** When there is a change in the routing topology, the routing path for the ERSPAN destination could also change. If the egress bandwidth is not sufficient for ERSPAN traffic, the excess traffic is dropped.

If the specific route for the ERSPAN destination is not available in the routing table and there is a default route set, the ERSPAN traffic is sent via the default route.

***Figure 1: ERSPAN Configuration***




**Monitored Traffic**

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.

# 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.

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

- GRE
- IPinIP
- IPv6
- IPv6 over IP tunnel

- Multipoint GRE (mGRE)
- Secure Virtual Tunnel Interfaces (SVTI)



**Note** SVTI and IPinIP tunnel interfaces support the monitoring of both IPsec-protected and non-IPsec-protected tunnel packets. Monitoring of tunnel packets allows you to see the clear-text tunnel packet after IPsec decryption if that tunnel is IPsec protected.

The following limitations apply to the enhancements introduced in Cisco IOS XE Release 3.4S:

- Monitoring of non-IPsec-protected tunnel packets is supported on IPv6 and IPv6 over IP tunnel interfaces.
- The enhancements apply only to ERSPAN source sessions, not to ERSPAN destination sessions.

ERSPAN has the following behavior in Cisco IOS XE Release 3.4S:

- The tunnel interface is removed from the ERSPAN database at all levels when the tunnel interface is deleted. If you want to create the same tunnel again, you must manually configure it in source monitor sessions to keep monitoring the tunnel traffic.
- The Layer 2 Ethernet header is generated with both source and destination MAC addresses set to zero.

In Cisco IOS XE Release 3.5S, support was added for the following types of WAN interfaces as source ports for a source session:

- Serial (T1/E1, T3/E3, DS0)
- Packet over SONET (POS) (OC3, OC12)
- Multilink PPP
- The **multilink**, **pos**, and **serial** keywords were added to the **source interface** command.

# ERSPAN Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which ERSPAN 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.

# Using ERSPAN as Local SPAN

To use ERSPAN to monitor traffic through one or more ports or VLANs, you must create an ERSPAN source and ERSPAN destination sessions.

You can create the two sessions either on the same router or on different routers. If the two sessions are created on two different routers, the monitoring traffic will be forwarded from the source to the destination by ERSPAN. However, if the two sessions are created on the same router, data flow takes place inside the router, which is similar to that in local SPAN.

The following factors are applicable while using ERSPAN as a local SPAN:

- Both sessions have the same ERSPAN ID.

- Both sessions have the same IP address. This IP address is the router's own IP address; that is, the loopback IP address or the IP address configured on any port.

## ERSPAN Support on WAN Interface

In Cisco IOS Release 3.5S an ERSPAN source on WAN is added to allow monitoring of traffic on WAN interfaces. ERSPAN replicates the original frame and encapsulates the replicated frame inside an IP or GRE packet by adding Fabric Interface ASIC (FIA) entries on the WAN interface. The frame header of the replicated packet is modified for capturing. After encapsulation, ERSPAN sends the IP or GRE packet through an IP network to a device on the network. This device sends the original frame to an analyzing device that is directly connected to the network device.

## ERSPAN Dummy MAC Address Rewrite

ERSPAN dummy MAC address rewrite supports customized MAC value for WAN interface and tunnel interface. It also allows you to monitor the traffic going through WAN interface.

## ERSPAN IP Access Control Lists

From Cisco IOS XE Everest 16.4.1 release, ERSPAN has been enhanced to better monitor packets and reduce network traffic. This enhancement supports ACL on ERSPAN source session to filter only specific IP traffic according to the ACL, and is supported on the IOS XE platform. Both IPv4 and IPv6 traffic can be monitored by associating an ACL with the ERSPAN session. The ERSPAN session can associate only one IP ACL entry with its name.

# How to Configure ERSPAN

ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on either the same router or on different routers.

## 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. **plim ethernet vlan filter disable**
5. **monitor session** *span-session-number* **type erspan-source**
6. **description** *string*
7. [**no**] **header-type 3**
8. **source interface** *interface-name interface-number*
9. **source vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} [**rx** | **tx** | **both**]

10. **filter vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*}
11. **filter access-group** *acl-filter*
12. **destination**
13. **erspan-id** *erspan-flow-id*
14. **ip address** *ip-address*
15. **ip prec** *prec-value*
16. **ip dscp** *dscp-value*
17. **ip ttl** *ttl-value*
18. **mtu** *mtu-size*
19. **origin ip address** *ip-address* [**force**]
20. **vrf** *vrf-id*
21. **no shutdown**
22. **end**

## DETAILED STEPS

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-type interface-number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet1/0/1` | Specifies the interface on which ERSPAN source session is configured. |
| **Step 4** | **plim ethernet vlan filter disable**<br>**Example:**<br>`Device(config-if)# plim ethernet vlan filter disable` | (Optional) Disables the VLAN filtering option for Ethernet interfaces. Use this command if you are using the **vlan filter** command or if the source interface is using dot1q encapsulation. |
| **Step 5** | **monitor session** *span-session-number* **type erspan-source**<br>**Example:**<br>`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.<br>• The *span-session-number* argument range is from 1 to 1024. The same session number cannot be used more than once.<br>• 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 6** | **description** *string*<br>**Example:**<br>`Device(config-mon-erspan-src)# description source1` | (Optional) Describes the ERSPAN source session.<br>• The *string* argument can be up to 240 characters and cannot contain special characters or spaces. |
| **Step 7** | [**no**] **header-type 3**<br>**Example:**<br>`Device(config-mon-erspan-src)# header-type 3` | Configures a switch to ERSPAN header type III. |
| **Step 8** | **source interface** *interface-name interface-number*<br>**Example:**<br>`Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx` | Configures more than one WAN interface in a single ERSPAN session. |
| **Step 9** | **source vlan** {*id-single* \| *id-list* \| *id-range* \| *id-mixed*} [**rx** \| **tx** \| **both**]<br>**Example:**<br>`Device(config-mon-erspan-src)# source vlan 1` | (Optional) Associates the ERSPAN source session number with the VLANs, and selects the traffic direction to be monitored.<br>• You cannot include source VLANs and filter VLANs in the same session. You can either include source VLANs or filter VLANs, but not both at the same time. |
| **Step 10** | **filter vlan** {*id-single* \| *id-list* \| *id-range* \| *id-mixed*}<br>**Example:**<br>`Device(config-mon-erspan-src)# filter vlan 1` | (Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port.<br>• You cannot include source VLANs and filter VLANs in the same session. You can have source VLANs or filter VLANs, but not both at the same time. |
| **Step 11** | **filter access-group** *acl-filter*<br>**Example:**<br>`Device(config-mon-erspan-src)# filter access-group ACL1` | (Optional) Associates an ACL with the ERSPAN session.<br>• Use the **no filter access-group** *acl-filter* command to detach the ACL from the ERSPAN session.<br>• Only ACL name is supported to associate to the ERSPAN source session. If the ACL does not exist or if there is no entry defined in the access control list, the ACL name is not attached to the ERSPAN source session.<br>• When the ERSPAN source session is active, you cannot detach the ACL from the ERSPAN source |

| | Command or Action | Purpose |
|---|---|---|
| | | session. The source session must be shut down before detaching the ACL. After the session shutdown, you must exit the session for the **shutdown** command to execute, and then re-enter the session to detach the ACL. |
| **Step 12** | **destination**<br>**Example:**<br>`Device(config-mon-erspan-src)# destination` | Enters ERSPAN source session destination configuration mode. |
| **Step 13** | **erspan-id** *erspan-flow-id*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# erspan-id 100` | Configures the ID used by the source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN destination session configuration. |
| **Step 14** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# ip address 10.10.0.1` | Configures the IP address that is used as the destination of the ERSPAN traffic. |
| **Step 15** | **ip prec** *prec-value*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# ip prec 5` | (Optional) Configures the IP precedence value of the packets in the ERSPAN traffic.<br>• You can optionally use either the **ip prec** command or the **ip dscp** command, but not both. |
| **Step 16** | **ip dscp** *dscp-value*<br>**Example:**<br>`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.<br>• You can optionally use either the **ip prec** command or the **ip dscp** command, but not both. |
| **Step 17** | **ip ttl** *ttl-value*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# ip ttl 32` | (Optional) Configures the IP TTL value of the packets in the ERSPAN traffic. |
| **Step 18** | **mtu** *mtu-size*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# mtu 1500` | Configures the maximum transmission unit (MTU) size, in bytes, for ERSPAN encapsulation.<br>• Valid values are from 64 to 9180. The default value is 1500. |
| **Step 19** | **origin ip address** *ip-address* [**force**]<br>**Example:**<br>`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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 20** | **vrf** *vrf-id*<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# vrf 1` | (Optional) Configures the VRF name to use instead of the global routing table. |
| **Step 21** | **no shutdown**<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# no shutdown` | Enables the configured sessions on an interface. |
| **Step 22** | **end**<br>**Example:**<br>`Device(config-mon-erspan-src-dst)# end` | Exits ERSPAN source session destination configuration mode, and returns to privileged EXEC mode. |

# Configuring an ERSPAN Destination Session

Perform this task to configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination session. The ERSPAN destination session defines the session configuration parameters and the ports that will receive the monitored traffic.

### SUMMARY STEPS

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

### DETAILED STEPS

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# configure terminal` | |
| **Step 3** | **monitor session** *session-number* **type erspan-destination**<br>**Example:**<br>`Device(config)# monitor session 1 type erspan-destination` | Defines an ERSPAN destination session using the session ID and the session type, and enters in ERSPAN monitor destination session configuration mode.<br>• The *session-number* argument range is from 1 to 1024. The session number must be unique and cannot be used more than once.<br>• 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.<br>• 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*<br>**Example:**<br>`Device(config-mon-erspan-dst)# description source1` | (Optional) Describes the ERSPAN destination session.<br>• The *string* argument can be up to 240 characters in length and cannot contain special characters or spaces. |
| **Step 5** | **destination interface** {**gigabitethernet** \| **port-channel**} [*interface-number*]<br>**Example:**<br>`Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1` | Associates the ERSPAN destination session number with the source ports, and selects the traffic direction to be monitored. |
| **Step 6** | **source**<br>**Example:**<br>`Device(config-mon-erspan-dst)# source` | Enters ERSPAN destination session source configuration mode. |
| **Step 7** | **erspan-id** *erspan-flow-id*<br>**Example:**<br>`Device(config-mon-erspan-dst-src)# erspan-id 100` | Configures the ID used by the 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**]<br>**Example:**<br>`Device(config-mon-erspan-dst-src)# ip address 10.10.0.1` | Configures the IP address that is used as the source of the ERSPAN traffic.<br>• The **ip address** *ip-address* **force** command changes the source IP address for all ERSPAN destination sessions. |
| **Step 9** | **vrf** *vrf-id*<br>**Example:** | (Optional) Configures the VRF name to use instead of the global routing table. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-mon-erspan-dst-src)# vrf 1` | |
| **Step 10** | **no shutdown**<br>**Example:**<br>`Device(config-mon-erspan-dst-src)# no shutdown` | Enables the configured sessions on an interface. |
| **Step 11** | **end**<br>**Example:**<br>`Device(config-mon-erspan-dst-src)# end` | Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode. |

# Configuring ERSPAN Dummy MAC Address Rewrite

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *span-session-number* **type erspan-source**
4. **source interface** *interface-name interface-number*
5. **s-mac** *address*
6. **d-mac** *address*
7. **end**

### DETAILED STEPS

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **monitor session** *span-session-number* **type erspan-source**<br>**Example:**<br>`Device(config)# monitor session 100 type erspan-source` | Defines an ERSPAN source session using the session ID and the session type, and enters ERSPAN monitor source session configuration mode.<br>• The *span-session-number* argument range is from 1 to 1024. 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.<br>• 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** | **source interface** *interface-name interface-number*<br>**Example:**<br>`Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx` | Configures more than one WAN interface in a single ERSPAN session. |
| **Step 5** | **s-mac** *address*<br>**Example:**<br>`Device(config-mon-erspan-src)# s-mac 1111.1111.1111` | Defines source pseudo mac for wan interface. |
| **Step 6** | **d-mac** *address*<br>**Example:**<br>`Device(config-mon-erspan-src)# d-mac 2222.2222.2222` | Defines destination pseudo mac for wan interface. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-mon-erspan-src)# end` | Exits ERSPAN source session destination 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 GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
```

```
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

# Example: Configuring an ERSPAN Source Session on a WAN Interface

The following example shows how to configure more than one WAN interface in a single ERSPAN source monitor session. Multiple interfaces have been separated by a commas.

```
monitor session 100 type erspan-source
    source interface Serial 0/1/0:0, Serial 0/1/0:6
```

# Example: Configuring an ERSPAN Destination Session

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

```
monitor session 2 type erspan-destination
 destination interface GigabitEthernet1/3/2
 destination interface GigabitEthernet2/2/0
 source
  erspan-id 100
  ip address 10.10.0.1
```

# Example: Configuring an ERSPAN as a Local SPAN

The following example shows how to configure an ERSPAN as a local SPAN.

```
monitor session 10 type erspan-source
 source interface GigabitEthernet0/0/0
 destination
 erspan-id 10
 ip address 10.10.10.1
 origin ip address 10.10.10.1
monitor session 20 type erspan-destination
destination interface GigabitEthernet0/0/1
 source
  erspan-id 10
  ip address 10.10.0.1
```

# Example: Configuring ERSPAN Dummy MAC Address Rewrite

```
monitor session 1 type erspan-source
 s-mac 1111.1111.1111
 d-mac 2222.2222.2222
 source interface Gi2/2/0
 destination
  erspan-id 100
  mtu 1464
  ip address 200.0.0.1
  origin ip address 100.0.0.1
```

# Example: Configuring UDF-Based ERSPAN

This example shows how to configure UDF-based ERSPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20, but TCP flags at 13th byte)
- Offset from packet-start: 14 + 20 + 20 + 13 = 67
- UDF match value: 0x20 • UDF mask: 0xFF

```
udf udf_tcpflags packet-start 67 1
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf
```

This example shows how to configure UDF-based ERSPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + IP (20) + TCP (20) + Payload: 112233445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```
udf udf_pktsig_msb header outer l3 26 2
udf udf_pktsig_lsb header outer l3 28 2
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf-pktsig
```

# Additional References for Configuring ERSPAN

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| LAN Switching commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | LAN Switching Command Reference |

### 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/techsupport |

# 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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

***Table 1: Feature Information for Configuring ERSPAN***

| Feature Name | Releases | Feature Information |
|---|---|---|
| ERSPAN | Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 3.8S | The Cisco ERSPAN feature allows you to monitor traffic on one or more ports or VLANs, and send the monitored traffic to one or more destination ports.<br>The following commands were introduced or modified by this feature: **description**, **destination**, **erspan-id**, **filter**, **ip dscp**, **ip prec**, **ip ttl, monitor permit-list**, **monitor session**, **origin ip address**, **show monitor permit-list**, **source**, **switchport**, **switchport mode trunk**, **switchport nonegotiate**, **switchport trunk encapsulation**, **vrf**.<br>In Cisco IOS XE 3.8S release, ERSPAN was enhanced to support MTU data size up to 9180 bytes. The following command was added by this feature: **mtu**. |
| ERSPAN Support on WAN Interface | Cisco IOS XE Release 3.5S | ERSPAN has been enhanced to support WAN interface as an ERSPAN source.<br>The following command was modified by this feature: **source interface**. |
| ERSPAN Type III Header | Cisco IOS XE Denali 16.2 | ERSPAN has been enhanced to configure a switch to ERSPAN type III header.<br>The following command was introduced by this feature: **header-type 3**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| ERSPAN IP ACL | Cisco IOS XE Everest 16.4.1 | ERSPAN has been enhanced to better monitor packets and reduce network traffic. This enhancement supports ACL on ERSPAN source session to filter only specific IP traffic according to the ACL.<br>The following command was introduced by this feature: **filter access-group** *acl-filter*. |