

Encapsulated Remote Switched Port Analyzer

An encapsulated remote switched port analyzer (ERSPAN) transports mirrored traffic over an IPv4 or IPv6 network, which provides remote monitoring of multiple switches across your network. The traffic is encapsulated at the source router and is transferred across the network. The packet is decapsulated at the destination router and then sent to the destination interface. Another method is that the destination can be the analyzer itself, which needs to understand the ERSPAN encapsulation format to parse the packet and access the inner (SPAN copy) frame.

- Overview, on page 1
- Guidelines and Limitations, on page 3
- Configure an ERSPAN Source Session, on page 10
- Configure an ERSPAN Destination Session, on page 13
- Configure an ERSPAN ACL, on page 16
- Configure UDF-Based ERSPAN, on page 18
- Configure ERSPAN Truncation, on page 21
- Configuration Examples, on page 23

Overview

Encapsulated Remote Switched Port Analyzer (ERSPAN) enables remote traffic monitoring on Cisco switches by designating sources, destinations, and session behaviors.

Sources

The interfaces from which traffic can be monitored are called ERSPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. ERSPAN sources include the following:

- Ethernet ports (but not subinterfaces)
- Port channels
- The inband interface to the control plane CPU

Note When you specify the supervisor inband interface as a SPAN source, the device monitors all packets that are sent by the Supervisor CPU.

Note If you use the supervisor inband interface as a SPAN source, all packets generated by the supervisor hardware (egress) are monitored.

Rx is from the perspective of the ASIC (traffic egresses from the supervisor over the inband and is received by the ASIC/SPAN).

- VLANs
  - When a VLAN is specified as an ERSPAN source, all supported interfaces in the VLAN are ERSPAN sources.
  - VLANs can be ERSPAN sources only in the ingress direction, except for Cisco Nexus 9300-FX/-FX2/-FX3/-GX series platform switches, and Cisco Nexus 9500 series platform switches with -EX/-FX line cards.

Note A single ERSPAN session can include mixed sources in any combination of the above.

Destinations

Destination ports receive the copied traffic from ERSPAN sources. The destination port is a port that is connected to the device such as a Remote Monitoring (RMON) probe or security device that can receive and analyze the copied packets from single or multiple source port. Destination ports do not participate in any spanning tree instance or any Layer 3 protocols

Cisco Nexus 9200, 9300-FX, and 9300-FX2 platform switches support an ERSPAN destination session configured on physical or port-channel interfaces in switchport mode through the use of GRE header traffic flow. The source IP address should be configured on the default VRF. Multiple ERSPAN destination sessions should be configured with the same source IP address.

Sessions

You can create ERSPAN sessions that designate sources to monitor. An ERSPAN session is localized when all of the source interfaces are on the same line card.

Note An ERSPAN session with a VLAN source is not localized

Truncation

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure the truncation of source packets for each ERSPAN session based on the size of the MTU. Truncation helps to decrease ERSPAN bandwidth by reducing the size of monitored packets. Any ERSPAN packet that is larger than the configured MTU size is truncated to the given size. For ERSPAN, an additional ERSPAN header is added to the truncated packet from 54 to 166 bytes depending on the ERSPAN header type. For example, if you configure the MTU as 300 bytes, the packets are replicated with an ERSPAN header size from 354 to 466 bytes depending on the ERSPAN header type configuration.

ERSPAN truncation is disabled by default. To use truncation, you must enable it for each ERSPAN session.

Default Settings

The following table lists the default settings for ERSPAN parameters.

Table 1: Default ERSPAN Parameters

Parameters	Default
ERSPAN sessions	Created in the shut state

Guidelines and Limitations

Platform-specific guidelines and limitations apply, including support for jumbo frames, session limits, and feature restrictions. Some features, such as ERSPAN mirroring for PBR traffic, VLAN as source, and ERSPAN over VXLAN overlay, are not supported on certain platforms or configurations.

Prerequisites

You must first configure the ports on each device to support the desired ERSPAN configuration. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

For ERSPAN session limits and scale information, see the release specific, *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide.*

Configuration Guidelines

- **ERSPAN destination handles jumbo frames for MTU differently based on the platform.**

  For the following Cisco Nexus 9300 platform switches and Cisco Nexus 9500 platform switches with supporting line cards, ERSPAN destination drops the jumbo frames.

  - 9300 Supported Line Cards - Cisco Nexus 9332PQ, Cisco Nexus 9372PX, Cisco Nexus 9372PX-E, Cisco Nexus 9372T, Cisco Nexus 9372TX-E, Cisco Nexus 93120TX
  - 9500 Supported Line Cards - Cisco Nexus 9564PX, Cisco Nexus 9464TX, Cisco Nexus 9464TX2, Cisco Nexus 9564TX, Cisco Nexus 9464PX, Cisco Nexus 9536PQ, Cisco Nexus 9636PQ, Cisco Nexus 9432PQ

  For Cisco Nexus 9200 platform switches and Cisco Nexus 9500 platform switches with supporting line cards, ERSPAN truncates the packets at port MTU and issues a TX Output error.

  - 9200 Supported Line Cards - Cisco Nexus 92160YC-X, Cisco Nexus 92304QC, Cisco Nexus 9272Q, Cisco Nexus 9232C, Cisco Nexus 9236C, Cisco Nexus 92300YC, Cisco Nexus 93108TC-EX, Cisco Nexus 93180LC-EX, Cisco Nexus 93180YC-EX
  - 9500 Supported Line Cards - Cisco Nexus 9736C-EX, Cisco Nexus 97160YC-EX, Cisco Nexus 9732C-EX, Cisco Nexus 9732C-EXM

- An access-group filter in an ERSPAN session must be configured as vlan-accessmap.
- Control plane packets that are generated by the Supervisor cannot be ERSPAN encapsulated or filtered by an ERSPAN access control list (ACL).

- A VLAN can be part of only one session when it is used as an ERSPAN source or filter.
- VLAN ERSPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
- If you enable ERSPAN on a vPC and ERSPAN packets must be routed to the destination through the vPC, packets that come through the vPC peer link cannot be captured.
- ERSPAN copies for multicast packets are made before rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on, are not captured in the ERSPAN copy.
- The timestamp granularity of ERSPAN Type III sessions is not configurable through the CLI. It is 100 picoseconds and driven through PTP.
- ERSPAN works on default and nondefault VRFs, but ERSPAN marker packets work only on the default VRF.

Unsupported Features

- Using the ACL filter to ERSPAN subinterface traffic on the parent interface is not supported on the Cisco Nexus 9200 platform switches and the Cisco Nexus 9300-FX/FX2/FX3/GX platform switches.
- ERSPAN mirroring is not supported for PBR traffic.
- ERSPAN with a Type three header is not supported in Cisco NX-OS Release 9.3(3).
- Statistics are not supported for the filter access group.
- ERSPAN is not supported for management ports.
- ERSPAN does not support destinations on Layer 3 port-channel subinterfaces.
- VLAN as a source is not supported with ERSPAN configuration on R-series linecards and N3K-C36180YC-R, N3KC36480LD-R2, and N3K-C3636C-R platform switches.
- ERSPAN is not supported over a VXLAN overlay.
- Configuring two SPAN or ERSPAN sessions on the same source interface with only one filter is not supported. If the same source is used in multiple SPAN or ERSPAN sessions either all the sessions must have different filters or no sessions should have filters. UDF-based ERSPAN is not supported.

Release Specification Limitations

Beginning with Cisco NX-OS Release 9.3(5)

- ERSPAN Type III Header is supported on Cisco Nexus 9300-GX platform switch.
- ERSPAN Destination Support is available on Cisco Nexus 9300-GX platform switch.

Beginning with Cisco NX-OS Release 10.1(2)

- ERSPAN is supported on the Cisco N9K-X9624D-R2 Line Card.
- IPv6 is supported on ERSPAN destination/termination on Cisco Nexus 9300-GX2, 9300-GX, 9300-FXP, 9300-FX2, 9300-EX, 9300-FX3, 9300-FX3S, and 9300-FX3P platform switches and N9K-X9716D-GX, N9K-X9736C-EX, N9K-X9732C-EX(X86_64 Atom), N9K-X9732C-EXM, N9K-X97160YC-EX, and N9K-X9736C-FX line cards.

- Only VRF default is supported on IPv6.
- You can only have one IPv6 address per switch.
- IPv6 is not supported with other tunnel features.
- You can bring up four ERSPAN destination sessions at a time on IPv6
- ERSPAN ID is unique per session and the range is 1–32 for IPv6.

Beginning with Cisco NX-OS Release 10.3(1)F

- ERSPAN is supported on Cisco Nexus 9808 platform switches.
- Only RX is supported on ERSPAN.
- Type 3 header is not supported on ERSPAN.
- ERSPAN destination/termination is not supported.

Beginning with Cisco NX-OS Release 10.4(1)F

- ERSPAN is supported on the Cisco Nexus 9332D-H2R switch.
- ERSPAN is supported on the Cisco Nexus 9804 switch but Type 3 header and ERSPAN destination/termination is not supported.
- ERSPAN is supported on the Cisco Nexus X98900CD-A and X9836DM-A line cards with Cisco Nexus 9808 and 9804 switches.

Beginning with Cisco NX-OS Release 10.4(2)F

- Cisco Nexus 9300-H2R platform switches supports SPAN on ACL drop in ingress direction for the ERSPAN source session.
- Layer 3 Port-channel interface as ERSPAN source and destination is supported on 9804 and 9808 platform switches. However, the following guidelines and limitations are applicable:
  - Load balancing of mirrored traffic on port channel is not supported.
  - Sharing of the same source port or interface across sessions is not supported.
  - A maximum of 10 monitor sessions are supported at a time.
  - 10 active ERSPAN sessions are supported at a time.
  - ERSPAN MTU truncation is only supported for 343 bytes on 9804 and 9808 switches excluding FCS.
  - ERSPAN Type 3 header is not supported.
  - ERSPAN destination/termination is not supported.
  - ERSPAN Layer 2 interface (switch port) and VLAN as source is not supported. However, beginning with Cisco NX-OS Release 10.6(1)F, Layer 2 switch port (Ethernet/Port-channel) as source is supported.
- ERSPAN is supported on Cisco Nexus 93400LD-H1 platform switch.

Beginning with Cisco NX-OS Release 10.4(3)F

- ERSPAN is supported on Cisco Nexus 9364C-H1 platform switch.

Egress (Tx) ERSPAN Guidelines

- The flows for post-routed unknown unicast flooded packets are in the ERSPAN session, even if the ERSPAN session is configured to not monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and ERSPAN sessions that have TX port sources.
- For ERSPAN Tx multicast for Layer 2, ERSPAN copies are created independent of multicast replication. Due to this, multicast and SPAN packet have different values for VLAN tag, which is the ingress interface VLAN ID.
- The following guidelines and limitations apply to ingress (Rx) ERSPAN:
  - VLAN sources are spanned only in the Rx direction.
  - Session filtering functionality (VLAN or ACL filters) is supported only for Rx sources.
  - VLANs are supported as ERSPAN sources only in the ingress direction.
- Priority flow control (PFC) ERSPAN has the following guidelines and limitations:
  - It cannot coexist with filters.
  - It is supported only in the Rx direction on physical or port-channel interfaces. It is not supported in the Rx direction on VLAN interfaces or in the Tx direction.
- The following guidelines and limitations apply to FEX ports:
  - If the sources used in bidirectional ERSPAN sessions are from the same FEX, the hardware resources are limited to two ERSPAN sessions.
  - FEX ports are supported as ERSPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.
  - Cisco Nexus 9300 platform switches do not support ERSPAN destination being connected on a FEX interface. The ERSPAN destination must be connected to a front panel port.
  - VLAN and ACL filters are not supported for FEX ports. It cannot coexist with filters.
- The following guidelines and limitations apply to ERSPAN destination:
  - Cisco Nexus 9200, 9300-EX, 9300-FX, and 9300-FX2 platform switches support an ERSPAN destination session that is configured on physical or port-channel interfaces in switchport mode by using GRE header traffic flow.
  - ERSPAN destination cannot coexist with other tunnel features such as MPLS and VXLAN for Cisco Nexus 9200, 9300, 9300-EX, 9300-FX, and 9300-FX2 platform switches.
  - On Cisco Nexus 9300-GX switches, dot1q-tagged broadcast or multicast packets passing through a device where the ERSPAN destination session is active, get tagged with the native VLAN instead of the correct VLAN due to a hardware limitation.
  - ERSPAN destination supports only default VRF.

- Cisco Nexus 9300-EX/FX switches cannot serve as an ERSPAN destination for Cisco Nexus 3000 and non-EX/FX Cisco Nexus 9000 switches.

ERSPAN over IPv6 Guidelines

-
- This feature is not supported for Load balancing across egress port-channel members and egress ECMP path.
- This feature is not supported for header-type 3, udf in filter ACL, and marker-packets.
- This feature is not supported for FEX host interface as ERSPAN source with IPv6.

Platform-Specific Limitations

- A maximum of 48 source interfaces are supported per ERSPAN session (Rx and Tx, Rx, or Tx).
- The number of ERSPAN sessions per line card reduces to two if the same interface is configured as a bidirectional source in more than one session.
- Packets with FCS errors are not mirrored in an ERSPAN session.
- TCAM carving is not required for SPAN/ERSPAN on the following line cards:
  - Cisco Nexus 9636C-R
  - Cisco Nexus 9636Q-R
  - Cisco Nexus 9636C-RX
  - Cisco Nexus 96136YC-R
  - Cisco Nexus 9624D-R2



Note All other switches supporting SPAN/ERSPAN must use TCAM carving.

- The same source can be part of multiple sessions.
- ERSPAN mirrored packets do not have separate SPAN egress queue, they take the default queue.
- When port-channel interface (with more than one member port) is configured as ERSPAN destination, only one member interface is used for sending out mirrored traffic.
- The member selection is done in software, so there will be packet loss when membership changes.
- When configuring local SPAN sessions or ERSPAN-source monitor sessions with a filter access-group rule, we recommend to configure the necessary sub-commands of the VLAN access-map too, such as the match rule. For more information, see Configuration Example for an ERSPAN ACL.

ERSPAN Guidelines and Limitations for Cisco Nexus 9364E-SG2 Switches

Beginning with Cisco NX-OS Release 10.5(3)F, ERSPAN is supported on Cisco N9364E-SG2-O and N9364E-SG2-Q ToR switches. This section lists the guidelines and limitations that you need to follow.

- **Sessions**

  —The switch supports a maximum of four active monitor sessions at a time, with session ID 4 reserved for SPAN on drop.

- **MTU truncation**

  — . MTU truncation is supported for ERSPAN Rx mirroring. Beginning with Cisco NX-OS Release 10.6(1)F, MTU truncation is supported for ERSPAN Tx mirroring. MTU truncation for ERSPAN supports 218 bytes excluding FCS. For Rx mirroring, packets are truncated to the configured 218 bytes and, for Tx mirroring, packets are truncated to 154 bytes excluding FCS. ERSPAN encapsulation is done on the truncated packets.

- **Port-channel interface**

  —When port-channel interface with more than one member port is configured as ERSPAN destination, only one member interface is used to send mirrored traffic. Member selection is done in software, which can lead to packet loss when membership changes.

- **Drop stats**

  —For drops on the ERSPAN destination interface, drop stats per interface per queue are not available.

- **Packet mirroring**

  —In ERSPAN, multicast mirrored packet is accounted as unicast under ERSPAN destination interface. ERSPAN mirrored packets do not have separate SPAN egress queue, they take the default queue.

- **Unsupported features**

  —The features that are not supported include:

  - load balancing of mirrored traffic on port channel,
  - sharing of the same source port or interface across sessions,
  - ERSPAN Type 3 header,
  - ERSPAN destination/termination,
  - VLAN as source, and
  - ACL filter.

ERSPAN Guidelines and Limitations for N9300 Smart and Nexus 9324C-SE1U Switches

Beginning with NX-OS Release 10. 6(2)F , ERSPAN is supported on N9324C-SE1U and N9348Y2C6D-SE1U ToR switches. This section lists the guidelines and limitations that you need to follow while configuring ERSPAN on this switch.

- **Sessions**

  —The switch supports a maximum of 10 active monitor sessions at a time, irrespective of the sessions being local SPAN or ERSPAN.

- **MTU truncation**

  —MTU truncation for ERSPAN supports 144 bytes. Rx mirrored packets are truncated to 144 bytes excluding FCS but Tx mirrored packets are truncated to 80 bytes, excluding FCS.

- **Port-channel interface**

  —When port-channel interface with more than one member port is used as ERSPAN destination, only one member interface is used to send mirrored traffic. Member selection is done in software, which can lead to packet loss when membership changes.

- **Packet mirroring**

  —N9324C-SE1U and N9348Y2C6D-SE1U mirrors packets on sub-interface when parent service-port-channel interface is configured as source. Beginning with NX-OS Release 10.6(2), mirrored packets are queued up in a dedicate SPAN Q on ESPRAN destination port.ERSPAN can be used to mirror traffic ingress or egress out of service- port-channel interface.

- **Unsupported features**

  —The features that are not supported include:

  - mirroring packets on Layer 3 sub interfaces or Layer 3 port-channel sub interfaces when the respective parent interface is configured as source,
  - sharing of the same source port or interface across sessions,
  - tunnel ports, VLAN, SUP Ethernet, and management interface as a source,
  - ERSPAN Type 3 header,
  - ERSPAN destination/termination, and
  - UDF and ERSPAN ACL filter.

ERSPAN Guidelines and Limitations for Cisco Nexus 9336C-SE1 Switch

Beginning with Cisco NX-OS Release 10.6(1)F, ERSPAN is supported on Cisco N9336C-SE1 switch. The guidelines and limitations include:

- **Sessions**

  —A maximum of 10 active monitor (ERSPAN) sessions are supported at a time.

- **Packet mirroring**

  —Sharing of the same source port or interface across multiple sessions is not supported. ERSPAN mirrored packets use the default egress queue and do not have a dedicated ERSPAN egress queue.

- **MTU truncation**

  — MTU truncation is supported only for 144 bytes in Rx mirroring and 80 bytes in Tx mirroring, excluding FCS.

- **Port-channel interface**

  —When port-channel interface with multiple member ports is configured as an ERSPAN destination, only one member interface is used for mirrored traffic. Member selection is handled in software, which results in packet loss when membership changes.

- **Unsupported features**

  —The features that are not supported include:

  - ERSPAN on subinterfaces

- sharing of the same source port or interface across sessions,
- tunnel ports,
- VLAN as source,
- UDF, and
- ACL filter.

Configure an ERSPAN Source Session



Note Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

You can configure an ERSPAN session on the local device only. By default, ERSPAN sessions are created in the shut state.



Note ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Configure the ERSPAN global origin IP v4 or IPv6 address using the command **monitor erspan origin ip-address** *ip-address* **global** or **monitor erspan origin ipv6-address** *ipv6-address* **global**

Example:

```
switch(config)# monitor erspan origin ip-address 10.0.0.1 global
switch(config)# monitor erspan origin ipv6-address 2001:DB8:1::1 global
```

Step 3 Clear the configuration of the specified ERSPAN session using the command **no monitor session** { *session-number* | **all** }

Example:

```
switch(config)# no monitor session 3
```

The new session configuration is added to the existing session configuration.

Step 4 Configure an ERSPAN Type II source session using the command **monitor session** { *session-number* | **all** } **type erspan-source** [**shut**] and configure a description for the session using the command **description** *description* .

Example:

```
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)#
```

Example:

```
switch(config-erspan-src)# description erspan_src_session_3
```

By default the session is bidirectional. The optional keyword shut specifies a shut state for the selected session. By default, no description is defined. The description can be up to 32 alphanumeric characters.

Step 5 Configure the sources and traffic direction in which to copy packets using the command **source** { **interface** *type* [**tx** | **rx** | **both**] **vlan** { **number** | **range** } [**rx**]}

Example:

```
switch(config-erspan-src)# source interface
ethernet 2/1-3, ethernet 3/1 rx
```

Example:

```
switch(config-erspan-src)# source interface
port-channel 2
```

Example:

```
switch(config-erspan-src)# source interface
sup-eth 0 rx
```

Example:

```
switch(config-erspan-src)# source vlan 3, 6-8 rx
```

Example:

```
switch(config-erspan-src)# source interface
ethernet 101/1/1-3
```

You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, or a satellite port or host interface port channel on the Cisco Nexus 2000 Series Fabric Extender (FEX). You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify the traffic direction to copy as ingress, egress, or both. For a unidirectional session, the direction of the source must match the direction specified in the session.

Repeat this step to configure all ERSPAN sources.

Note
Source VLANs are supported only in the ingress direction. Source FEX ports are supported in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic. Supervisor as a source is only supported in the Rx direction.

Step 6 Configure which VLANs to select from the configured sources using the command **filter vlan** { *number* | *range* }

Example:

```
switch(config-erspan-src)# filter vlan 3-5, 7
```

You can configure one or more VLANs, as either a series of comma-separated entries or a range of numbers. For information on the VLAN range, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.

Repeat this step to configure all source VLANs and to filter.

Note
A FEX port that is configured as an ERSPAN source does not support VLAN filters.

Step 7 Associate an ACL with the ERSPAN session using the command **filter access-group** *acl-filter*

Example:

```
switch(config-erspan-src)# filter access-group
ACL1
```

This is an optional step. You can create an ACL using the standard ACL configuration process. For more information, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Note
Before executing this command, configure ip access list and associated vlan access map . See Configuring ERSPAN ACL .

Step 8 Follow the following commands to configure the various values for the ERSPAN session.

- Configure the destination IP v4 or IPv6 address in the ERSPAN session (Mandatory) - **destination ip** *ip-address*
- Configure the ERSPAN ID for the ERSPAN source session (Mandatory) - **erspan-id** *erspan-id*
- Configure the virtual routing and forwarding (VRF) instance that the ERSPAN source session uses for traffic forwarding (Mandatory) - **vrf** *vrf-name*
- Configure the IP time-to-live (TTL) value for the ERSPAN traffic (Optional) - **ip ttl** *ttl-number*
- Configure the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic (Optional) - **ip dscp** *dscp-number*
- Enable the ERSPAN marker packet for a session in order to recover the real value of the ERSPAN timestamp (Optional) - [**no**] **marker-packet** *milliseconds*

Example:

```
switch(config-erspan-src)# destination ip 10.1.1.1
```

```
switch(config-erspan-src)# destination ipv6 2001:DB8:1::1
```

Example:

```
switch(config-erspan-src)# erspan-id 5
```

Example:

```
switch(config-erspan-src)# vrf default
```

Example:

```
switch(config-erspan-src)# ip ttl 25
```

Example:

```
switch(config-erspan-src)# ip dscp 42
```

Example:

```
switch(config-erspan-src)# marker-packet 100
```

Note
Only one destination IP v4 or IPv6 address is supported per ERSPAN source session. The ERSPAN ID range is from 1 to 1023. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters. The range for IP TTL is from 1 to 255. The range for IP DSCP is from 0 to 63. The interval for marker packet can range from 100 to 1000 milliseconds. The **no** form of this command disables the marker packet for the session. ERSPAN marker packets only apply to Type 3 sessions.

Step 9 Enable the ERSPAN source session using the command **no shut** and exit the monitor configuration mode using the command **exit**

Example:

```
switch(config-erspan-src)# no shut
```

Example:

```
switch(config-erspan-src)# exit
switch(config)#
```

By default, the session is created in the shut state.

This example shows how to configure an ERSPAN source session over IPv6:

```
switch# configure terminal
switch(config)# monitor erspan origin ipv6-address 2001::10:0:0:9 global
switch(config)# moni session 10 type erspan-source
switch(config-erspan-src)# erspan-id 10
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# source interface ethernet 1/64
switch(config-erspan-src)# destination ipv6 2001:DB8:1::1
```

What to do next

Verify ERSPAN Source Session

To display the ERSPAN configuration, perform one of the following tasks:

Command	Purpose
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	Displays the ERSPAN session configuration.
show running-config monitor	Displays the running ERSPAN configuration.
show startup-config monitor	Displays the ERSPAN startup configuration.

Configure an ERSPAN Destination Session

Use this task to configure an ERSPAN destination session, which allows you to copy packets from a source IP address to destination ports on the local device.

You can configure an ERSPAN destination session to copy packets from a source IP address to destination ports on the local device. By default, ERSPAN destination sessions are created in the shut state.

Before you begin

Ensure that you have already configured the destination ports in switchport monitor mode.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal** and enter interface configuration mode on the selected slot and port or range of ports using the command **interface ethernet** *slot/port* [*-port*]

Example:

```
switch# configure terminal
switch(config)#
```

Example:

```
switch(config)# interface ethernet 2/5
switch(config-if)#
```

Step 2 Configure the switchport parameters for the selected slot and port or range of ports using the command **switchport** and configure the switchport modes for the selected slot and port or range of ports using the command **switchport mode access** | **trunk**

Example:

```
switch(config-if)# switchport
```

Example:

```
switch(config-if)# switchport mode trunk
```

Step 3 Configure the switchport interface as an ERSPAN destination using the command **switchport monitor** and repeat steps 1 to 3 to configure monitoring on additional ERSPAN destinations.

Example:

```
switch(config-if)# switchport monitor
```

Step 4 Clear the configuration of the specified ERSPAN session using the command **no monitor session** { *session-number* | **all** } and configure an ERSPAN destination session using the command **type erspan-destination**

Example:

```
switch(config-if)# no monitor session 3
```

Example:

```
switch(config-if)# monitor session 3 type erspan-destination
switch(config-erspan-dst)#
```

The new session configuration is added to the existing session configuration.

Step 5 Configure a description for the session using the command **description** *description*

Example:

```
switch(config-erspan-dst)# description erspan_dst_session_3
```

By default, no description is defined. The description can be up to 32 alphanumeric characters.

Step 6 Configure the source IPv4 or IPv6 address in the ERSPAN session using the command **source ip** *ip-address*

source ipv6 *ipv6-address*

Example:

```
switch(config-erspan-dst)# source ip 10.1.1.1
```

```
switch(config-erspan-dst)# source ipv6 2001:DB8:1::1
```

The source IPv4 or IPv6 address is a locally configured IPv4 or IPv6 address. The source IPv4 or IPv6 address in an ERSPAN destination session must match the destination IPv4 or IPv6 address configured in the ERSPAN source session from which the encapsulated data is received. Only one source IPv4 or IPv6 address is supported per ERSPAN destination session.

Note
IPv6 is supported from Cisco NX-OS Release 10.2(3)F.

Step 7 Configure a destination for copied source packets using the command **destination** {[**interface** [*type slot/port* [*-port*]]] [**port-channel** *channel-number*]]} . Repeat the step to configure all the ERSPAN destinations.

Example:

```
switch(config-erspan-dst)# destination interface ethernet 2/5
```

You can configure a destination interface.

Note
You can configure destination ports as trunk ports.

Step 8 Configure the ERSPAN ID for the ERSPAN session using the command **erspan-id** *erspan-id* and enable the ERSPAN destination session using the command **no shut** .

Example:

```
switch(config-erspan-dst)# erspan-id 5
```

Example:

```
switch(config-erspan-dst)# no shut
```

The range for the ERSPAN ID is from 1 to 1023. By default, the destination session is created in the shut state.

Step 9 Exit monitor configuration mode and exit the global configuration mode using the command **exit**

Example:

```
switch(config-erspan-dst)# exit
```

Example:

```
switch(config)# exit
```

This example shows how to configure an ERSPAN destination session over IPv4:

The **destination interface eth1/1** is in switchport monitor mode. This interface can not co-exist with mpls strip, tunnel, nv overlay, vn-segment-vlan-based, mpls segment-routing, mpls evpn, mpls static, mpls oam, mpls l3vpn , mpls ldp, and nv overlay evpn features.

```
switch# monitor session 1 type erspan-destination
switch(config)# erspan-id 1
switch(config-erspan-dst)# source ip 10.1.1.1
switch(config-erspan-dst)# destination interface eth1/1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
```

This example shows how to configure an ERSPAN destination session over IPv6:

The **destination interface eth1/1** is in switchport monitor mode. This interface can not co-exist with mpls strip, tunnel, nv overlay, vn-segment-vlan-based, mpls segment-routing, mpls evpn, mpls static, mpls oam, mpls l3vpn , mpls ldp, and nv overlay evpn features.

```
switch# monitor session 1 type erspan-destination
switch(config)# erspan-id 1
switch(config-erspan-dst)# source ipv6 2001:DB8:1::1
switch(config-erspan-dst)# destination interface eth1/1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
```

What to do next

Verify ERSPAN Destination Session

Use the following optional commands to verify the destination session:

- Display the ERSPAN session configuration using the command **show monitor session** { **all** | *session-number* | **range** *session-range* }
- Display the running ERSPAN configuration using the command **show running-config monitor**
- Display the ERSPAN startup configuration using the command **show startup-config monitor**
- Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Configure an ERSPAN ACL

You can create an IPv4 ERSPAN ACL on the device and add rules to it.

To modify the DSCP value or the GRE protocol, you need to allocate a new destination monitor session. A maximum of four destination monitor sessions are supported.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Create the ERSPAN ACL and enter IP ACL configuration mode using the command **ip access-list** *acl-name*

Example:

```
switch(config)# ip access-list erspan-acl
switch(config-acl)#
```

The *acl-name* argument can be up to 64 characters.

Step 3 Create a rule in the ERSPAN ACL using the command [*sequence-number*] { **permit** | **deny** } *protocol source destination*

Example:

```
switch(config-acl)# permit ip 192.168.2.0/24 any
```

Example:

```
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 10.0.0.0/24 any
switch(config-acl)# exit
```

You can create many rules.

The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic.

Step 4 Enter VLAN access-map configuration mode for the VLAN access map specified using the command **vlan access-map erpsan-acl** *map name* [*sequence-number*]

Example:

```
switch(config)# vlan access-map erspan_filter
```

If the VLAN access map does not exist, the device creates it. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.

Step 5 Specify an ACL for the access-map entry using the command **match ip address** *acl-name* and specify the action that the device applies to traffic that matches the ACL using the command **action forward** .

Example:

```
switch(config-access-map)# match ip address erspan-acl
```

Example:

```
switch(config-access-map)# action forward
```

Step 6 Exit the VLAN access-map configuration mode using the command **exit** and configure an ERSPAN Type II source session using the command **monitor session** [*session-number* | **all**] **type erspan-source** [**shut**] .

Example:

```
switch(config-access-map)# exit
```

Example:

```
switch(config)# monitor session 1 type erspan-source
```

By default, the session is bidirectional. The optional keyword **shut** specifies a shut state for the selected session.

Step 7 Associate an ACL with the ERSPAN session using the command **filter access_group** *name* and display the ERSPAN ACL configuration using the command **show ip access-lists** *name* .

Example:

```
 switch(config-erspan-src)# filter access_group erspan_filter
```

Example:

```
switch(config-acl)# show ip access-lists erpsan-acl
```

You can create an ACL using the standard ACL configuration process. For more information, see *Cisco Nexus 9000 Series NX-OS Security Configuration Guide.*

Step 8 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config-acl)# copy running-config startup-config
```

This is an optional step.

This example shows how to configure an ERSPAN ACL:

```
switch# configure terminal
switch(config)# ip access-list match_10_pkts
switch(config-acl)# permit ip 10.0.0.0/24 any
switch(config-acl)# exit
switch(config)# ip access-list match_172_pkts
switch(config-acl)# permit ip 172.16.0.0/24 any
switch(config-acl)# exit
```

In the case of different ERSPAN destinations where the interesting traffic is chosen based on the defined ACL filters, the last configured session would always have the higher priority.

For example, if Monitor Session 1 is configured; then Monitor Session 2 is configured; then ERSPAN traffic filter works as intended. But, if the user goes back to Monitor Session 1 and re-applies one of the existing configuration line (no new changes in the config); then the spanned traffic switches back to Monitor Session 1.

What to do next

To display the ERSPAN ACL configuration, execute the appropriate show commands from the following table.

Command	Purpose
show ip access-lists *name* Example: `switch(config-acl)# show ip access-lists erpsan-acl`	Displays the ERSPAN ACL configuration.
show vlan access-map *name* Example: `switch(config-acl)# show vlan access-map erspan_filter`	Displays information about VLAN access maps.
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**] Example: `switch(config-acl)# show monitor session 1`	Displays the ERSPAN session configuration.

Configure UDF-Based ERSPAN

Configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields and send the matching packets to the ERSPAN destination. This helps analyze and isolate packet drops in the network.

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the **hardware access-list tcam region** command to provide enough free space to enable UDF-based ERSPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
 switch(config)#
```

Step 2 Define the UDF using the command **udf** *udf-name offset-base offset length*

Example:

```
switch(config)# udf udf-x packet-start 12 1
 switch(config)# udf udf-y header outer l3 20 2
```

- *udf-name* —Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name.
- *offset-base* —Specifies the UDF offset base as follows, where **header** is the packet header to consider for the offset: **packet-start** | **header** { **outer** | **inner** { **l3** | **l4** }} .
- *offset* —Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.
- *length* —Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.

You can define multiple UDFs, but Cisco recommends defining only required UDFs.

Step 3 Attach the UDFs to one of the following TCAM regions using the command **hardware access-list tcam region** { **racl | ifacl | vacl** } **qualify udf** *udf-names*

Example:

```
switch(config)# hardware access-list tcam region
      racl qualify udf udf-x udf-y
```

- racl—Applies to Layer 3 ports.—Applies to layer 2 and Layer 3 ports.
- ifacl—Applies to Layer 2 ports.
- vacl—Applies to source VLANs.

You can attach up to 8 UDFs to a TCAM region.

Note
When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Note

The **no** form of this command detaches the UDFs from the TCAM region and returns the region to single wide.

Step 4 Save the change persistently through reboots and restart by copying the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

Step 5 **reload**

Example:

```
switch(config)# reload
```

Reloads the device.

Note
Your UDF configuration is effective only after you enter **copy running-config startup-config** + **reload** .

Step 6 Create an IPv4 access control list (ACL) and enters IP access list configuration mode using the command **ip access-list** *erspan-acl*

Example:

```
switch(config)# ip access-list erspan-acl-udf-only
 switch(config-acl)#
```

Step 7 Configure the ACL to match only on UDFs (example 1) or to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2). Enter one of the following commands to con:

- **permit udf** *udf-name value mask*
- **permit ip** *source destination* **udf** *udf-name value mask*

Example:

```
switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F
```

Example:

```
switch(config-acl)# permit ip 10.0.0.0/24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F
```

A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.

Step 8 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

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
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
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
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
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
```

Configure ERSPAN Truncation

You can configure truncation for local and ERSPAN source sessions only.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
                        switch(config)#
```

Step 2 Enter monitor configuration mode for the specified ERSPAN session using the command **monitor session** *session-number* **type erspan-source**

Example:

```
switch(config)# monitor session 10 type erspan-source
                        switch(config-erspan-src)#
```

Step 3 Configure the source interface using the command **source interface** *type slot* / *port* [**rx** | **tx** | **both**]

Example:

```
switch(config-erspan-src)# source interface ethernet 1/5 both
```

Step 4 Configure the MTU size for truncation using the command **mtu** *size*

Example:

```
switch(config-erspan-src)# mtu 512
```

Example:

```
switch(config-erspan-src)# mtu ?
<512-1518> Enter the value of MTU truncation size for
                        ERSPAN packets (erspan header + truncated original packet)
```

Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU ranges for ERSPAN packet truncation are:

- The MTU size range is 64 to 1518 bytes for Cisco Nexus 9300-FX Series switches.
- The MTU size is 343 bytes (excluding FCS) for Cisco Nexus 9808 and 9804 platform switches.

Step 5 Configure the Ethernet ERSPAN destination port using the command **destination interface** *type slot* / *port*

Example:

```
switch(config-erspan-src)# destination interface Ethernet 1/39
```

Step 6 Enable the ERSPAN session using the command **no shut**

Example:

```
switch(config-erspan-src)# no shut
```

By default, the session is created in the shut state.

Step 7 Display the ERSPAN configuration using the command **show monitor session** *session*

Example:

```
switch(config-erspan-src)# show monitor session 5
```

This is an optional step.

Step 8 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config-erspan-src)# copy running-config startup-config
```

This example shows how to configure ERSPAN truncation for use with MPLS stripping:

```
mpls strip
ip access-list mpls
  statistics per-entry
  20 permit ip any any redirect Ethernet1/5

interface Ethernet1/5
  switchport
  switchport mode trunk
  mtu 9216
  no shutdown

monitor session 1
  source interface Ethernet1/5 tx
  mtu 64
  destination interface Ethernet1/6
  no shut
monitor session 21 type erspan-source
  description "ERSPAN Session 21"
  header-type 3
  erspan-id 21
  vrf default
  destination ip 10.1.1.2
  source interface Ethernet1/5 tx
  mtu 64
  no shut
monitor session 22 type erspan-source
  description "ERSPAN Session 22"
  erspan-id 22
  vrf default
  destination ip 10.2.1.2
  source interface Ethernet1/5 tx
  mtu 750
  no shut
monitor session 23 type erspan-source
  description "ERSPAN Session 23"
  header-type 3
  marker-packet 1000
  erspan-id 23
  vrf default
  destination ip 10.3.1.2
  source interface Ethernet1/5 tx
  mtu 1000
  no shut
```

Configuration Examples

This section helps understand the following

- Enable ERSPAN marker packets
- Configure a unidirectional ERSPAN session
- Shut Down or Activate an ERSPAN session

Enable ERSPAN Marker Packet

This example shows how to enable the ERSPAN marker packet with an interval of 2 seconds:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 10.1.1.2
switch(config-erspan-src)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
session 1
---------------
type              : erspan-source
state             : up
granularity       : nanoseconds
erspan-id         : 1
vrf-name          : default
destination-ip    : 10.1.1.2
ip-ttl            : 16
ip-dscp           : 5
header-type       : 3
origin-ip         : 172.28.15.250 (global)
source intf       :
    rx            : Eth1/15
    tx            : Eth1/15
    both          : Eth1/15
    rx            :
marker-packet     : enabled
packet interval   : 100
packet sent       : 25
packet failed     : 0
egress-intf       :
```

Configure a Unidirectional ERSPAN Session

This example shows how to configure a unidirectional ERSPAN session :

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# source interface ethernet 2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 10.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

Shut Down or Activate an ERSPAN Session

You can shut down ERSPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, ERSPAN sessions are created in the shut state.

You can enable ERSPAN sessions to activate the copying of packets from sources to destinations. To enable an ERSPAN session that is already enabled but operationally down, you must first shut it down and then enable it. You can shut down and enable the ERSPAN session states with either a global or monitor configuration mode command.

1. Enter the global configuration mode using the command **configure terminal**
2. Shut down the specified ERSPAN sessions using the command **monitor session** {*session-range* | **all**} **shut**. By default, sessions are created in the shut state.
3. Resume (enables) the specified ERSPAN sessions using the command **no monitor session** {*session-range* | **all**} **shut**. By default, sessions are created in the shut state.



Note If a monitor session is enabled but its operational status is down, then to enable the session, you must first specify the **monitor session shut** command followed by the **no monitor session shut** command.

4. Enter the monitor configuration mode for the ERSPAN source type using the command **monitor session** *session-number* **type erspan-source**. The new session configuration is added to the existing session configuration.
5. Shut down the ERSPAN session using the command **shut**. By default, the session is created in the shut state.
6. Enable the ERSPAN session using the command **no shut**. By default, the session is created in the shut state.
7. Exit the monitor configuration mode using the command **exit**.
8. Display the status of ERSPAN sessions using the command **show monitor session all**. This is an optional step.
9. Display the ERSPAN running configuration and the ERSPAN startup configuration using the commands **show running-config monitor** and **show startup-config monitor**. This is an optional step.

```
switch# configure terminal
switch(config)# monitor session 3 shut
switch(config)# no monitor session 3 shut
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# shut
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session all
switch(config)# show running-config monitor
switch(config)# show startup-config monitor
witch(config)# copy running-config startup-config
```