ERSPAN

This chapter, Encapsulated Remote Switched Port Analyzer (ERSPAN), explains its function in mirroring network traffic via GRE tunnels for analysis. It covers features like higher payload support, GRE IPv6 and MPLS integration, partial packet capture, rate limiting, DSCP-based traffic classification, and multi-session monitoring with ACLs.

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) is a traffic mirroring feature that

- monitors network traffic from one or more source ports on a router
- mirrors traffic from one or more source ports, and
- sends the mirrored traffic through GRE tunnels to destinations for analysis.

The destination may be a network analyzer or other monitoring devices.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Higher payload analysis with eight ERSPAN sessions	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) This feature is now supported on: • 8011-4G24Y4H-I
ERSPAN over GRE IPv6	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100] , 8010 [ASIC: A100]) This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I
Higher payload analysis with eight ERSPAN sessions	Release 24.4.1	Introduced in this release on: Fixed Systems(8200 , 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100]) (select variants only*). This feature now enables the Cisco 8000 Series routers to support eight ERSPAN sessions on the following hardware thus allowing you to analyze higher payloads in real time across Layer 3 domains on your network. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH

Feature Name	Release Information	Feature Description
ERSPAN over GRE IPv6	Release 24.4.1	Introduced in this release on: Fixed Systems(8200 , 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100]) (select variants only*). With this release, the router allows you to mirror IPv4 or IPv6 traffic with ERSPAN over GRE IPv6 sessions to monitor traffic on remote traffic analyzers on the following hardware. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH
Partial packet capture ability for ERSPAN (Rx)	Release 7.5.3	With this feature, you can perform partial packet capture in the Rx direction. Earlier, the ability for entire packet capture was available, now you can choose entire or partial packet capture in the Rx direction. Here, partial packet capture is also known as truncation.
ERSPAN over MPLS traffic	Release 7.3.5 Release 7.5.3	With this release, the router allows you to mirror MPLS traffic and set up the GRE tunnel with the next hop over a labeled path. This feature helps you to remote-monitor the traffic on traffic analyzers.
Higher payload analysis with eight ERSPAN sessions	Release 7.3.2	With this release, Cisco 8000 Series routers support eight ERSPAN sessions. This functionality helps you analyze higher payloads in real time across Layer 3 domains on your network.

Feature Name	Release Information	Feature Description
ERSPAN over GRE IPv6	Release 7.3.2	With this release, the router allows you to mirror IPv4 or IPv6 traffic with ERSPAN over GRE IPv6 sessions to monitor traffic on remote traffic analyzers. In earlier releases, ERSPAN traffic monitoring was possible only on IPv4 networks.

Benefits of ERSPAN

These are the benefits of ERSPAN:

- It enables real-time network troubleshooting.
- It automates configuration processes, allowing network operators to troubleshoot issues in real-time and send specific flows to management servers for detailed analysis.
- It transports mirrored traffic over an IP network and encapsulates it at the source router for transfer across the network

Configuration guidelines for ERSPAN

These guidelines apply for ERSPAN:

Source and destination interface requirements

- The source interfaces are Layer 3 interfaces, such as physical and bundle interfaces, or subinterface.
- Each monitor session allows only one destination interface.
- The next hop interface must be a main interface. It can be a physical or bundle interface.

Traffic types and protocol support

- The routers mirror IPv4 and IPv6 traffic.
- The router supports MPLS traffic mirroring and GRE tunnel configuration with the next hop over a labeled path.
- The router supports only ERSPAN TYPE II header. The value of the index field is always 0. The value of the session-ID field is an internal number that is used by the data path to distinguish between sessions.
- The router mirrors only unicast traffic. However, from Cisco IOS XR Software Release 7.5.3 onwards, the router can mirror multicast traffic.
- ERSPAN will be functional regardless of any configuration related to MPLS or LDP present on the router.

Encapsulation and tunneling

- ERSPAN with GRE IPv4 or IPv6 has tunnel destinations.

- In ERSPAN over GRE IPv6, the **HopLimit** and **TrafficClass** fields in outer IPv6 header can be edited under the tunnel configuration.

Mirroring support

- ERSPAN supports only Rx direction.
- MPLS packet mirroring is supported only from Cisco IOS XR Software Release 7.5.3 onwards.

Access Control List (ACL) integration

- ERSPAN over GRE IPv4 and IPv6 supports SPAN ACL.
- For ACL ERSPAN, the ERSPAN next-hop must have ARP resolved. Any other traffic or protocol triggers ARP.
- ACL permit or deny entries with capture action are part of mirroring features.

Packet capture capabilities

The router supports full packet capture.

Monitor session support

- Starting from Cisco IOS XR Release 24.3.1, the system creates one default monitor session and users can configure up to three additional monitor sessions, totaling four sessions, which is the maximum number of monitor sessions that the router allows.

Release-wise feature summary

This table summarizes key feature changes across different software releases.

Table 2: Release-wise feature summary

Feature	Release	Details
GRE sequence bit for ERSPAN	7.0.14	GRE header sequence bit is set; sequence number is always 0 for ERSPAN packets.
Sequence bit	7.5.3	The sequence number bit is always set one and the sequence number field, which is 4 bytes, is always set to zero.
Packet truncation over remote GRE tunnels	7.5.3	Allows flexible packet truncation for mirrored traffic.

Restrictions for ERSPAN

These restrictions apply for ERSPAN

- GRE tunnels are exclusively dedicated to ERSPAN mirrored packets. Do not configure any IPv4 and IPv6 addresses under the GRE tunnel.
- Traffic accounting of the ERSPAN mirrored packets is not supported.

Note You can view the SPAN packet count per session, using the **show monitor-session status internal** command.

- ERSPAN decapsulation is not supported.
- ERSPAN does not work if the GRE next hop is reachable over subinterface. For ERSPAN to work, the next hop must be reachable over the main interface. From Cisco IOS XR Software Release 7.5.3 onwards, GRE next hop can be resolved over subinterface or the main interface.
- ERSPAN will be functional regardless of any configuration related to MPLS or LDP present on the router.
- MPLS packet mirroring is supported only from Cisco IOS XR Software Release 7.5.3 onwards.
- On Cisco Silicon One Q100 ASIC-based systems, only the upper 64-bits of the source IPv6 address in the outer IPv6 header of an ERSPAN packet are valid because of data path limitations; the lower 64-bits are set to zero. The destination GREv6 IPv6 address must use the full 128-bit value.
- If you have upgraded the router from Cisco IOS XR Release 24.3.2 to later releases, one of the four user-configured sessions (created in Cisco IOS XR Release 24.3.x) will be lost, as the router allows only a maximum of three user-configured sessions.

Supported ERSPAN sessions

These tables detail the supported sessions for various releases and SPAN types:

Table 3: Maximum SPAN sessions support on prior and later releases

SPAN type	7.3.1 and prior releases	7.3.2 and later releases
ERSPAN (GRE IPv4, GRE IPv6, or GRE IPv4 + GRE IPv6)	4	8
Local SPAN	4	4
SPAN to File	4	4
Combined SPAN (GRE IPv4 + GRE IPv6 + Local SPAN + SPAN to File)	4	8

Table 4: Maximum sessions supported on various SPAN types

Starting Cisco IOS XR release	SPAN type	Maximum supported sessions
Release 7.2.12	ERSPAN (GRE IPv4, GRE IPv6, or GRE IPv4 + GRE IPv6)	4
	Local SPAN	4
	SPAN to File	4
	Combined SPAN (GRE IPv4 + GRE IPv6 + Local SPAN + SPAN to File)	4
Release 24.2.11 Details sessions supported on the 88-LC1-52Y8H-EM and 88-LC1-12TH24FH-E line cards on all Egress Traffic Management (ETM)-based platforms, when the NPU compatibility mode is set to P100.	ERSPAN (GRE IPv4, GRE IPv6, or GRE IPv4 + GRE IPv6)	4
	Local SPAN	4
	SPAN to File	4
	Combined SPAN (GRE IPv4 + GRE IPv6 + Local SPAN + SPAN to File)	4

For more information on NPU compatibility mode, see Configure the Compatibility Mode.

ERSPAN over GRE

The ERSPAN over GRE IPv6 is a traffic mirroring feature that

- enables mirroring IPv4 or IPv6 traffic in your network
- uses GRE IPv6 for secure encapsulation of mirrored data, and
- sends mirrored traffic to remote analyzers for detailed examination.

Configuration guidelines for ERSPAN over GRE

These guidelines apply to ERSPAN over GRE:

Configuration commands use

Use the **cef proactive-arp-nd enable** command to configure missing adjacency information for the next hop.

How ERSPAN over GRE works

Summary

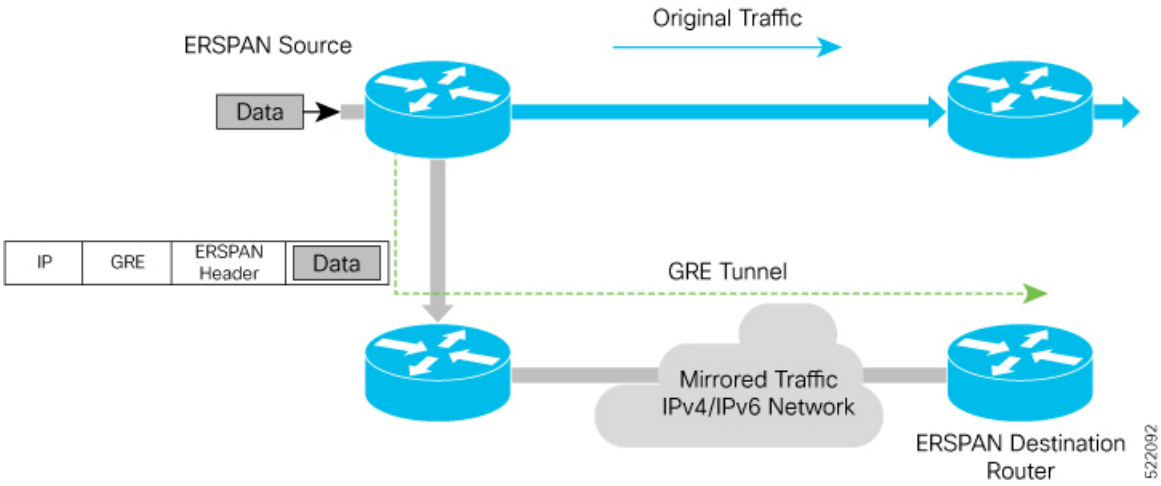
The router encapsulates and mirrors traffic using ERSPAN over GRE IPv6 with the sequence number set to 0, sends it to a remote analyzer, and resolves the next-hop address for successful delivery.

The key components involved in the process are:

- ERSPAN header: Used to encapsulate the mirrored traffic.
- GRE IPv6 packet: Provides the tunneling mechanism for carrying ERSPAN traffic.
- Sequence number: Set to 0 in the GRE header for ERSPAN packets.
- Remote Traffic Analyzer: Receives and monitors the mirrored traffic.
- Next-Hop address resolution: Ensures the router can deliver packets by resolving ARP or neighbor information for the GRE IPv6 tunnel.

Workflow

Figure 1: ERSPAN over GRE



These are the stages of how ERSPAN over GRE works:

1. The router encapsulates the trafficby adding an ERSPAN header inside the GRE IPv6 packet. The GRE header of the ERSPAN encapsulated packets has the sequence number set to 0.
2. The router sends the replicated traffic packet to the destination for monitoring through the GRE IPv6 channel for traffic mirroring.
3. The router sends the mirrored traffic to a remote traffic analyzer for monitoring.
4. The router must resolve the ARP or neighbor for ERSPAN GRE IPv6 tunnel next-hop. We recommend using the **cef proactive-arp-nd enable** command to configure missing adjacency information for the next hop.

Configure ERSPAN over GRE

Use these steps to configure ERSPAN over GRE IPv6:

Procedure

Step 1 Enable GRE IPv6 tunnel configuration.

Example:

```
Router#configure
Router(config)#interface tunnel-ip1
Router(config-if)#tunnel mode gre ipv6
Router(config-if)#tunnel source 2001:DB8:1::1
Router(config-if)#tunnel destination 2001:DB8:2::1
Router(config-if)#no shut
Router(config)#commit
```

A GRE IPv6 tunnel is configured on an interface.

Step 2 Enable an ERSPAN session.

Example:

```
Router#configure
Router(config)#monitor-session mon1 ethernet
Router(config-mon)#destination interface tunnel-ip1
Router(config-mon)#commit
Router(config-mon)#end
```

Step 3 Configure the ERSPAN session under the port to be monitored.

Example:

```
Router(config)#interface HundredGigE0/1/0/14
Router(config-if)#monitor-session mon1 ethernet direction rx-only
Router(config-if-mon)#exit
Router(config-if)#exit
Router(config)#interface Bundle-Ether1
Router(config-if)#monitor-session mon1 ethernet direction rx-only
Router(config-if-mon)#exit
Router(config-if)#exit
Router(config)#interface HundredGigE0/1/0/15.100
Router(config-subif)#monitor-session mon1 ethernet direction rx-only
```

Step 4 Verify the configuration of the ERSPAN over GRE IPv6 feature using the `show monitor-session status` command.

```
Router#show monitor-session mon1 status
Monitor-session mon1
Destination interface tunnel-ip1
================================================================================
Source Interface            Dir         Status
---------------------      ----  --------------------------------------------------
Hu0/1/0/14                  Rx    Operational
Hu0/1/0/15.100              Rx    Operational
BE1                         Rx    Operational
BE1.1                       Rx    Operational


Router#show monitor-session erspan3 status internal
Thu Jul 15 06:00:14.720 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session erspan3 (ID 0x00000007) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip372 (0x0f00049c)
          Last error: Success
          Tunnel data:
```

```
            Mode: GREoIPv6
            Source IP: 77:3:1::79
            Dest IP: 95::90
            VRF:
            ToS: 100
            TTL: 200
            DFbit: Not set
0/3/CPU0: Destination interface tunnel-ip372 (0x0f00049c)
          Tunnel data:
            Mode: GREoIPv6
            Source IP: 77:3:1::79
            Dest IP: 95::90
            VRF:
            ToS: 100
            TTL: 200
            DFbit: Not set
0/RP0/CPU0: Destination interface tunnel-ip372 (0x0f00049c)
          Tunnel data:
            Mode: GREoIPv6
            Source IP: 77:3:1::79
            Dest IP: 95::90
            VRF:
            ToS: 100
            TTL: 200
            DFbit: Not set
Information from SPAN EA on all nodes:
Monitor-session 0x00000007 (Ethernet)
0/3/CPU0: Name 'erspan3', destination interface tunnel-ip372 (0x0f00049c)
Platform, 0/3/CPU0:
  Monitor Session ID: 7

  Monitor Session Packets: 2427313444
  Monitor Session Bytes: 480591627492
```

Partial packet capture for ERSPAN

Partial packet capture is a traffic mirroring mechanism that:

- allows ERSPAN to capture only a portion of incoming packets (Rx), rather than capturing the entire packet, and
- allows you to focus on specific header information without needing the entire payload

Benefits of partial packet capture

These are the benefits of capturing partial packets for ERSPAN:

- With less data to process, network analysis and troubleshooting can be faster, allowing quicker identification of issues.
- By capturing only part of the packet, you reduce the amount of data that needs to be mirrored for monitoring. This can alleviate bandwidth consumption and memory requirements.

Configuration guidelines for partial packet capture

These are the guidelines for configuring partial packet capture:

- Enables the new ERSPAN GREv4 and GREv6 truncation configuration per device.
- Configures truncation settings specifically on monitor sessions. Packets received from all sources are truncated if truncation is enabled on a monitor session.
- By default, the whole packet is mirrored without the **mirror first** *number* (truncation size) configuration.
- If the truncation size configured for a monitor session is less than 343 bytes, the entire packet is mirrored instead of being truncated.
- If the truncation size configured for a monitor session exceeds 343 bytes, the configuration is accepted; however, only 343 bytes will be truncated as this is the maximum supported size.
- Displays an informative system message, **ios-msg**, to warn the user when the configured truncation size exceeds 343 bytes. Example message:

  ```
  ERSPAN only supports a 343-byte truncation size. The monitor session with session ID
  <id> will be set to 343 bytes only.
  ```

Restrictions for partial packet capture

These restrictions apply to partial packet capture:

- Partial packet capture or packet trucation is per monitor session.
- Truncation per interface is not supported.
- Packet truncation applies for SPAN to file and ERSPAN interfaces only. If you change the destination to local SPAN, then an **ios_msg** is displayed as a warning. The entire packet is mirrored after this message is displayed.

  ios_msg example:

  ```
  The Partial Packet Capture feature is not supported by Local SPAN. The entire
  Packet will be mirrored.
  ```

Configure partial packet capture for ERSPAN

Use this procedure to configure partial packet capturing for ERSPAN on incoming (Rx) traffic.

Procedure

Step 1 Create an ERSPAN monitor session for mirroring the packets to the tunnel-ip 30 with truncation enabled, and use the **mirror first** option to enable partial packet capturing.

Example:

```
monitor-session mon1 ethernet
 destination interface tunnel-ip 30
```

```
 mirror first  343
!
```

The **mon1** monitoring session sets the size of truncation packets for an ERSPAN session to 343.

Step 2 Attach the session to interfaces and specify the **direction** as **`rx-only`**.

Example:

```
interface HundredGigE0/0/0/12
  monitor-session mon1 ethernet direction rx-only
!
```

Step 3 Verify the configuration by using the **show monitor-session status internal** command.

Example:

```
Router#show monitor-session mon1 status internal
Fri Apr 12 18:50:45.006 UTC
Information from SPAN Manager and MA on all nodes:
Packet truncation size: 343B
Monitor-session mon1 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface Tunnel-IP 20 (0x0f000250)
          Last error: Success

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/RP0/CPU0: Name 'mon1', destination interface Tunnel-IP 20 (0x0f000250)
Platform, 0/RP0/CPU0:

  Monitor Session Packets: 142462

  Monitor Session Bytes: 7653237
```

ERSPAN with flexible CLI

ERSPAN with flexible CLI is an option to configure ERSPAN to

- function as a standalone configuration object that includes all ERSPAN session properties, tunnel properties, and source interfaces
- allow easy removal and re-addition of configurations, and
- minimize user error and support operational simplicity.

Benefits

The flexible CLI for ERSPAN provides benefits, such as:

- Simplifies configuration by consolidating settings into one object.
- Reduces the risk of user errors during configuration changes.
- Enables easy removal and re-application of settings.

ERSPAN rate limit

ERSPAN rate limit is a feature that:

- controls the amount of mirrored traffic sent to an ERSPAN destination over a network.
- enables you to monitor traffic flow through any IP network, including third-party switches and routers.
- prevents network congestion, and
- ensures ERSPAN traffic avoids overloading the network infrastructure.

Table 5: Feature History Table

Feature Name	Release Information	Description
ERSPAN rate limit	Release 25.2.1	Introduced in this release on: Fixed Systems (8200 , 8400 [ASIC: K100], 8700)(select variants only*); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: K100]) This feature provides rate limiting of the mirroring traffic that helps monitor the traffic flow through any IP network including third-party switches and routers. *This feature is now supported on Cisco 8404-SYS-D routers.
ERSPAN rate limit	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I
ERSPAN rate limit	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature helps you monitor traffic flow through any IP network including third-party switches and routers by providing rate limiting of the mirroring traffic. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH

Benefits

The ERSPAN rate limit feature offers these advantages:

- Limits mirrored traffic to prevent network congestion.
- Enables the use of mirrored traffic for data analysis without overwhelming resources.
- Supports traffic monitoring across various network devices.

Configuration guidelines and restrictions for ERSPAN rate limit

ERSPAN rate limit configuration guidelines

Consider these guidelines for using ERSPAN rate limit effectively:

- Configure the rate limit to prevent exceeding network capacity.
- Monitor traffic flow through any IP network to ensure compatibility with third-party devices.
- Set Quality of Service (QoS) parameters, Traffic Class (0 to 7), on the traffic monitor session to prioritize traffic.

Note Traffic class 0 has the lowest priority and class 7 has the highest. The default traffic class remains the same as the original traffic class.

- Intermediate switches carrying ERSPAN traffic from source session to termination session can belong to any Layer 3 network.
- The ERSPAN rate limit feature is applied on router interfaces to manage monitored traffic.

ERSPAN rate limit restrictions

These restrictions apply to ERSPAN rate limit:

- Exceeding the rate limit may result in the router capping or dropping monitored traffic.
- ERSPAN operates in source and destination sessions, requiring careful configuration to avoid data loss.

How ERSPAN rate limit works

Summary

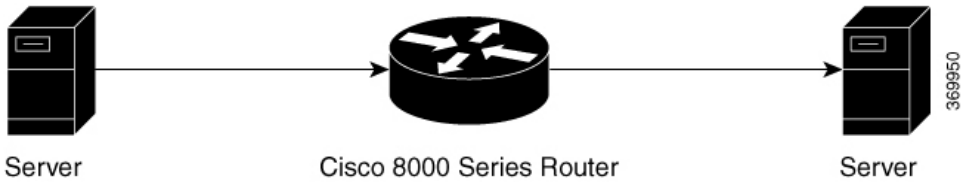
ERSPAN rate limit operates by encapsulating packets in ARPA or IP format using GRE encapsulation.

The key components involved in ERSPAN are:

- ERSPAN source session: The box where the traffic originates or is SPANned.
- ERSPAN termination session or destination session: The box where the traffic is analyzed.

Workflow

Figure 2: Topology for ERSPAN rate limit



These stages describe how ERSPAN rate limit works:

- The router sends GRE tunneled packets to a destination that is identified by an IP address.
- At the destination, SPAN-ASIC decodes and forwards the packets through a port.
- The router analyzes the traffic received at the destination.

Result

The ERSPAN rate limit process results in efficiently managing network traffic by controlling the amount of mirrored traffic sent to a destination.

Configure ERSPAN rate limit

Use this procedure to configure the rate limit for ERSPAN.

Procedure

Step 1 Start a monitor session by using the **monitor-session ERSPAN ethernet** command.

Example:

```
Router# configure
Router(config-if)# monitor-session ERSPAN ethernet
!
```

Step 2 Set the destination interface.

Example:

```
Router(config-if)# destination interface tunnel-ip100
```

Sets the destination interface as **tunnel-ip100**.

Step 3 Configure the interface with the necessary IP address and tunnel mode.

Example:

```
Router(config-if)# interface tunnel-ip1
Router(config-if)# ipv4 address 4.4.4.1 255.255.255.0
Router(config-if)# tunnel mode gre ipv4
Router(config-if)# source 20.1.1.1
Router(config-if)# tunnel destination 20.1.1.2
```

Step 4 Install the policy-map on the appropriate interface to manage traffic in the ingress direction.

Example:

```
Router# configure
Router(config)# interface HundredGigE0/0/0/16
Router(config-if)# ipv4 address 4.4.4.1 255.255.255.0
Router(config-if)# ipv6 address 3001::2/64
Router(config-if)# monitor-session ERSPAN ethernet direction rx-only port-level
acl
!
```

Step 5 Verify the configuration.

Example:

```
Router#show monitor-session FOO status detail
Monitor-session FOO
Destination interface tunnel-ip100
Source Interfaces
-----------------
TenGigE0/6/0/4/0
Direction: Both
Port level: True
ACL match: Disabled
```

ERSPAN rate-limit per destination

ERSPAN rate-limit per destination is an ERSPAN (Encapsulated Remote SPAN) feature that controls the amount of mirrored traffic sent to ERSPAN destinations by applying a rate-limit per source NPU.

Table 6: Feature History Table

Feature Name	Release Information	Description
ERSPAN rate-limit per destination	Release 25.3.1	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can now control the amount of mirrored traffic sent to ERSPAN destinations by applying a rate-limit per source NPU. This helps prevent network congestion and optimize resource usage. The feature introduces these changes. **CLI:** The **rate-limit** *value* keyword is introduced in the **monitor-session** command. **Yang Data Model:** • New Xpaths for `Cisco-IOS-XR-um-monitor-session-cfg.yang` • New Xpaths for `Cisco-IOS-XR-Ethernet-SPAN-cfg.yang`

Benefits

The ERSPAN rate-limit per destination feature offers these advantages:

- Allows you to apply rate-limiting directly to SPAN mirrored traffic.
- Streamlines configuration with a single command by using **monitor-session** *session-name* **rate-limit** *value* command.
- Provides enhanced control over the amount of mirrored traffic.
- Improves monitoring capabilities by delivering per-session statistics.
- Simplifies tracking of mirrored traffic and aiding troubleshooting of network monitoring issues.

Configuration guidelines for ERSPAN rate-limit per destination

ERSPAN rate-limit per destination configuration guidelines

- You can only apply the rate-limit to ERSPAN destinations. These destinations use tunnel interfaces. The system rejects configurations for local SPAN, which uses physical interfaces.
- Cisco IOS XR Release 25.3.1 supports rate-limit in kilobits per second (kbps). The supported values range from 40000 kbps (40 Mbps) as the minimum to 40000000 kbps (40 Gbps) as the maximum.
- The system applies the configured rate-limit per ingress NPU. An NPU can host multiple source interfaces.
- The effective rate-limit scales with the number of NPUs that contain source interfaces for a given session. This means the actual rate-limit can be higher than the configured value.

  For example, if you configure 200 kbps on a system with 48 NPUs:

  - If only one NPU has SPAN source interfaces, the rate-limit is 200 kbps.
  - If two NPUs each have SPAN source interfaces, the rate-limit is 400 kbps.
  - If all 48 NPUs have SPAN source interfaces, the rate-limit scales to 9600 kbps.

- Do not configure rate-limiting with **drops** or **protocol-capture** options. The system rejects such configurations.

Restrictions for ERSPAN rate-limit per destination

ERSPAN rate-limit per destination restrictions

- Rate-limit applies only to ERSPAN (mirroring over GRE tunnel), not supported for local SPAN (mirroring over a physical interface).
- Rate-limit configuration is supported only for tunnel interfaces and rejected for Local SPAN (non-tunnel interfaces).
- Rate-limiting applies only to transient (forwarded) traffic. It does not support packet drops, for-us packets, or locally sourced packets.
- The system provides per-session counters. It does not provide per-interface or per-direction statistics.

Configure ERSPAN rate-limit per destination

Use this procedure to configure the rate-limit per destination for ERSPAN.

Procedure

Step 1 Start a monitor session by using the **monitor-session ERSPAN ethernet** command.

Example:

```
Router# configure
Router(config-if)# monitor-session ERSPAN ethernet
!
```

Step 2 Apply the rate-limit for the selected destination.

Example:

```
Router(config-if)# destination interface tunnel-ip100 rate-limit 200kpbs
```

The rate-limit of **200kpbs** is applied for the destination interface **tunnel-ip100**.

Step 3 Verify the configuration.

Example:

```
Router# show monitor-session ERSPAN ethernet status detail
Monitor-session FOO
Destination interface tunnel-ip100
rate-limit: 200kpbs per NPU
Source Interfaces
-----------------
TenGigE0/6/0/4/0
Direction: Both
Port level: True
ACL match: Disabled
```

Step 4 To display statistics related information, such as the source interfaces and the replicated packet statistics for that interface, use the **show monitor-session counters per-session** command.

Example:

```
Router# show monitor-session foo counters per-session
Monitor session foo
  GigabitEthernet 0/3/0/0.100:
    Rx Replicated: 100 Packets 8000 Bytes
    Tx Replicated: 2 Packets 3000 Bytes
    Non Replicated: 0 Packets 0 Bytes
Per-session counters:
  Monitor-session foo
    Total replicated: 45 packets, 3600 octets
    Non-replicated: 0 packets, 0 octets
```

Note
With a rate-limit applied, counters are availbale at a session level, rather than per source interface.

Traffic mirroring with DSCP

Traffic mirroring with Differentiated Service Code Point (DSCP) is a traffic mirroring feature that:

- uses the DSCP value in the Differentiated Services (DS) field of an IP packet to classify network traffic
- sets the DSCP value in the six most significant bits of the DS field in the IP header, allowing for 64 different values ranging from 0 to 63
- these six bits affect the Per Hop Behavior (PHB) and determine how a packet is moved forward, and
- places packets into limited traffic classes for prioritization by routers.

Note The DS field was formerly known as Type of Service (ToS).

The table summarizes the service class names as defined in RFC 2474.

Table 7: DSCP, DS, and ToS values

DSCPValue in Decimal	DS Binary	DSHex	DSCPName	DS/ToSValue	ServiceClass
0	000000	0x00	DF/CS0	0	Standard
-	-	-	none	2	
1	000001	0x01	None	4	
1	000001	0x01	LE	4	Lower-effort
2	000010	0x02	None	8	
4	000100	0x04	None	16	
8	001 000	0x08	CS1	32	Low-priority data
10	001 010	0x0a	AF11	40	High-throughput data
12	001 100	0x0c	AF12	48	High-throughput data
14	001 110	0x0e	AF13	56	High-throughput data
16	010 000	0x10	CS2	64	OAM
18	010 010	0x12	AF21	72	Low-latency data
20	010 100	0x14	AF22	80	Low-latency data
22	010 010	0x16	AF23	88	Low-latency data
24	011 000	0x18	CS3	96	Broadcast video
26	011 000	0x1a	AF31	104	Multimedia streaming
28	011 100	0x1c	AF32	112	Multimedia streaming
30	011 110	0x1e	AF33	120	Multimedia streaming

32	100 000	0x20	CS4	128	Real-time interactive
34	100 010	0x22	AF41	136	Multimedia conferencing
36	100 100	0x24	AF42	144	Multimedia conferencing
38	100 110	0x26	AF43	152	Multimedia conferencing
40	101 000	0x28	CS5	160	Signaling(IP telephony, etc)
44	101 100	0x2c	Voice-admit	176	
46	101 110	0x2e	EF	184	Telephony
48	110 000	0x30	CS6	192	Network routing control
56	111 000	0x38	CS7	224	“reserved”

Benefits of traffic mirroring with DSCP

Benefits of using Traffic mirroring with DSCP are:

- It classifies and manages network traffic.
- It assigns different priority levels to packets.
- It enhances the Quality of Service (QoS) for mirrored packets.

DSCP marking on egress GRE tunnel in ERSPAN

Differentiated Service Code Point (DSCP) marking on egress GRE tunnel in ERSPAN is a mechanism that:

- classifies and manages network traffic by assigning different priority levels to packets, and
- defines the Quality of Service (QoS) for the mirrored packets by configuring the DSCP marking on an egress GRE tunnel for ERSPAN traffic.

Starting with Cisco IOS XR Software Release 7.5.4, you can set or modify the DSCP marking on ERSPAN GRE tunnels. This allows captured traffic routing using GRE encapsulation.

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
DSCP marking on egress GRE tunnel in ERSPAN	Release 25.2.1	Introduced in this release on: Fixed Systems (8200 , 8400 [ASIC: K100], 8700)(select variants only*); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: K100]) This feature helps you set or modify DSCP value on the ERSPAN GRE tunnel header to control the QoS for your network's ERSPAN GRE tunnel traffic. DSCP marking on the egress ERSPAN GRE tunnel eases the effort to control your customer's bandwidth across the next-hop routers. *This feature is now supported on Cisco 8404-SYS-D routers.
DSCP marking on egress GRE tunnel in ERSPAN	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I

Feature Name	Release Information	Feature Description
DSCP marking on egress GRE tunnel in ERSPAN	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature which allows you to control the QoS for your network's ERSPAN GRE tunnel traffic and eases the effort to control your customers' bandwidth across next-hop routers is supported on the following hardware. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH
DSCP marking on egress GRE tunnel in ERSPAN	Release 7.5.4	You can now set or modify Differentiated Service Code Point (DSCP) value on the ERSPAN GRE tunnel header. This feature allows you to control the QoS for your network's ERSPAN GRE tunnel traffic and eases the effort to control your customers' bandwidth across next-hop routers.

Configure DSCP marking on egress GRE tunnel in ERSPAN

Follow this procedure to configure DSCP marking on egress GRE tunnel in ERSPAN. You can configure DSCP value on both IPv4 and IPv6 headers.

Procedure

Step 1 Enter the terminal configuration mode.

Example:

```
Router#configure terminal
```

Step 2 Specify the tunnel interface and configure the DSCP value.

Example:

```
Router(config)#interface tunnel-ip1
Router(config-if)#tunnel tos 96
Router(config-if)#tunnel mode gre ipv4
Router(config-if)#tunnel source 192.0.2.1
Router(config-if)#tunnel destination 192.0.2.254
Router(config-if)#commit
```

The router configures the DSCP or ToS value as **96** on the **tunnel-ip1** interface.

Step 3 Verify the configuration.

Example:

```
Router#show run interface tunnel-ip1
interface tunnel-ip1
ipv4 address 192.0.2.0/24
tunnel tos 96
tunnel mode gre ipv4
tunnel source 192.0.2.1
tunnel vrf red
tunnel destination 192.0.2.254
Router#show monitor-session ERSPAN-2 status internal
Information from SPAN Manager and MA on all nodes:
Monitor-session ERSPAN-2 (ID 0x00000003) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip1 (0x20008024)
Last error: Success
Tunnel data:
Mode: GREoIPv4
Source IP: 192.0.2.1
Dest IP: 192.0.2.254
VRF: red
VRF TBL ID: 0
ToS: 96
TTL: 255
DFbit: Not set
```

This setup confirms the DSCP marking and ensures the correct configuration and operation of traffic mirroring with DSCP.

DSCP bitmask to filter ingress ERSPAN traffic

DSCP bitmask to filter ingress ERSPAN traffic is a mechanism that:

- filters ingress ERSPAN traffic with a specific DSCP value
- matches the bitmask in the Access Control List (ACL) rule with the DSCP field in the IP packet header, and
- determines if the packet aligns with the desired bitmask, classifying and prioritizing traffic as it enters the network.

Table 9: Feature History Table

Feature Name	Release Information	Feature Description
DSCP bitmask to filter ingress ERSPAN traffic	Release 25.2.1	Introduced in this release on: Fixed Systems (8200 , 8400 [ASIC: K100], 8700)(select variants only*); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: K100]) You can now mirror multiple traffic flows for matched Differentiated Service Code Point (DSCP) value of IP header on the Encapsulated remote SPAN (ERSPAN). *This feature is now supported on Cisco 8404-SYS-D routers.
DSCP bitmask to filter ingress ERSPAN traffic	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I
DSCP bitmask to filter ingress ERSPAN traffic	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature now allows to mirror multiple traffic flows for matched DSCP value of IP header on the ERSPAN on the following hardware. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH

Feature Name	Release Information	Feature Description
DSCP bitmask to filter ingress ERSPAN traffic	Release 7.5.4	You can now mirror multiple traffic flows for matched Differentiated Service Code Point (DSCP) value of IP header on the Encapsulated remote SPAN (ERSPAN). The matched DSCP value is based on the DSCP value and the bitmask configured in Access Control List (ACL) rule. Earlier, you could monitor single traffic flow by setting the RFC 4594 defined DSCP values in the GRE tunnel header. This feature introduces the following changes: • **CLI:** deny (IPv4), deny (IPv6), permit (IPv4), and permit (IPv6) are modified to include new keyword **bitmask**. • **YANG DATA Model:** New XPaths for Cisco-IOS-XR-um-ipv4-access-list-cfg and Cisco-IOS-XR-um-ipv6-access-list-cfg (see Github, YANG Data Models Navigator).

Benefits of using DSCP bitmask to filter ingress ERSPAN traffic (Reference)

Using a DSCP bitmask to filter ingress ERSPAN traffic offers these advantages:

- It allows for specific traffic flow mirroring.
- It enhances traffic classification and prioritization.
- It reduces unnecessary traffic mirroring on incoming ports.

Configuration guidelines for DSCP bitmask to filter ingress ERSPAN traffic

Use these guidelines to configure the DSCP bitmask to filter ingress ERSPAN traffic:

- Starting , you can configure an ACL rule with DSCP bitmask on the ERSPAN GRE tunnels to mirror specific traffic flows.
- When you configure an ACL with DSCP and DSCP mask on ERSPAN, ERSPAN mirrors the traffic whose DSCP value lies within the combination of DSCP value and the specified mask.
- Without ACL rule, ERSPAN mirrors all the traffic on the incoming port.
- Verify that the DSCP value lies within the specified mask range.
- The router maps the DSCP value to a single traffic class according to the values defined in RFC2474.
- Masking the DSCP value in ACL rule allows mirroring multiple traffic flows.
- DSCP value and mask operate similarly to IPv4 address and mask.

Configure DSCP bitmask to filter ingress ERSPAN traffic

To configure DSCP bitmask, use the **bitmask** option along with the **dscp** option while configuring the ACL.

Use these steps to configure DSCP bitmask on ingress ERSPAN for IPv4 traffic.

Procedure

Step 1 Configure an ACL.

Example:

```
Router# config
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit
```

Step 2 Attach the created ACL to an interface.

Example:

```
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0
```

Step 3 Monitor the ingress ACL applied and DSCP-masked IPv4 traffic on ERSPAN.

Example:

```
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
Router(config-if)# commit
```

Monitor ERSPAN sessions with SPAN and security ACLs

Monitoring multiple ERSPAN sessions is a functionality that:

- uses GREv4 and GREv6 under the same source interface to monitor multiple ERSPAN sessions
- allows you to choose the destination interface for the mirrored traffic from the multiple ERSPAN monitor sessions configured on an interface, and
- uses SPAN and security ACLs together for the configuration of monitor sessions.

Table 10: Feature History Table

Feature Name	Release Information	Feature Description
Monitor multiple ERSPAN sessions with SPAN and security ACL	Release 25.2.1	Introduced in this release on: Centralized Systems (8400 [ASIC:K100]))(select variants only*) This feature allows you to use SPAN and security ACL together to monitor multiple ERSPAN sessions under the same source interface. When the SPAN ACL distributes mirrored traffic over different destination interfaces, the security ACL allows selective incoming traffic. *This feature is now supported on Cisco 8404-SYS-D routers.
Monitor multiple ERSPAN sessions with SPAN and security ACL	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I

Feature Name	Release Information	Feature Description
Monitor multiple ERSPAN sessions with SPAN and security ACL	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature now enables you to use SPAN and security ACL together to monitor multiple ERSPAN sessions under the same source interface thus distributing the mirrored traffic over different destination interfaces and allowing selective incoming traffic on the following hardware. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH
Monitor multiple ERSPAN sessions with SPAN and security ACL	Release 7.5.4	With this feature, you can use SPAN and security ACL together to monitor multiple ERSPAN sessions under the same source interface. SPAN ACL helps you to distribute the mirrored traffic over different destination interfaces and Security ACL helps you to allow selective incoming traffic.

Configure multiple monitor ERSPAN sessions with SPAN and security ACL

Use this procedure to configure SPAN and security ACL with GREv4 and GREv6 monitor sessions.

Procedure

Step 1 Start a monitor session and attach the SPAN ACL to an interface.

Example:

```
Router# configure
Router(config-if)#monitor-session always-on-v4
Router(config-if)#monitor-session always-on-v4 ethernet direction rx-only port-level
Router(config-if-mon)#acl ipv4 v4-monitor-acl1
Router(config-if-mon)#acl ipv6 v6-monitor-acl1
Router(config-if-mon)#exit
Router(config-if)#monitor-session on-demand-v4 ethernet direction rx-only port-level
Router(config-if-mon)#acl ipv4 v4-monitor-acl2
Router(config-if-mon)#acl ipv6 v6-monitor-acl2
Router(config-if-mon)#exit
```

Step 2 Attach the security ACL to an interface.

Example:

```
Router(config-if)#ipv4 access-group sec_aclv4 ingress
Router(config-if)#ipv6 access-group sec_aclv6 ingress
Router(config-if)#commit
```