Configuring Traffic Mirroring

This module describes the configuration of the traffic mirroring feature. Traffic mirroring is sometimes called port mirroring, or switched port analyzer (SPAN).

Feature History for Traffic Mirroring

Release	Modification
Release 7.0.2	SPAN over Pseudo-Wire was introduced.
Release 7.1.2	SPAN to File was introduced.
Release 7.2.1	File Mirroring was introduced. Traffic Mirroring was introduced on Cisco NC57 line cards.
Release 7.3.1	PCAPng file format was introduced.
Release 7.5.2	Mirror first option in global configuration mode was introduced.

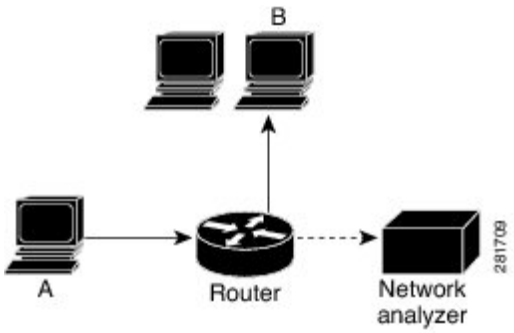
Introduction to Traffic Mirroring

Traffic mirroring, sometimes called port mirroring or Switched Port Analyzer (SPAN), is a Cisco proprietary feature that enables you to monitor network traffic passing in or out of a set of ports. You can then pass this traffic to a destination port on the same router.

Traffic mirroring copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device. Traffic mirroring does not affect the flow of traffic on the source interfaces or sub-interfaces. It allows the mirrored traffic to be sent to a destination interface or sub-interface.

For example, you can attach a traffic analyzer to the router and capture Ethernet traffic that is sent by host A to host B.

Figure 1: Traffic Mirroring Operation



When local traffic mirroring is enabled, the traffic analyzer gets directly attached to the port that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port.

Note

- From Release 7.2.1, traffic mirroring is introduced on Cisco NCS 5700 line cards.
- From Release 7.4.2, you can mirror incoming (Rx) and outgoing (Tx) traffic from the source ports to separate destinations on Cisco NC57 line cards. During a session, you can configure one destination port for incoming traffic and one for outgoing traffic.
- From Release 7.6.1, support for sub-interface as source is introduced on SPAN.

Traffic Mirroring Types

The following types of traffic mirroring are supported:

- **Local traffic mirroring**: This is the most basic form of traffic mirroring. The network analyzer or sniffer is attached directly to the destination interface. In other words, all monitored ports are located on the same router as the destination port.
- **Layer 2 traffic mirroring**: Layer 2 source ports can be mirrored on Cisco NC57 line cards.
- **ACL-based traffic mirroring**: Traffic is mirrored based on the configuration of the interface ACL.

You can mirror traffic based on the definition of an interface access control list. When you are mirroring Layer 3 traffic, the ACL is configured using the **ipv4 access-list** or the **ipv6 access-list** command with the **capture** option. The **permit** and **deny** commands determine the behavior of regular traffic. The **capture** option designates the packet is to be mirrored to the destination port, and it is supported only on permit type of access control entries (ACEs).

Note Prior to Release 6.5.1, ACL-based traffic mirroring required the use of UDK (User-Defined TCAM Key) with the **enable-capture** option so that the **capture** option can be configured in the ACL.

- **Encapsulated remote SPAN (ERSPAN)**: ERSPAN enables generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains.

Note A copy of every packet includes the Layer 2 header if the ethernet keyword is configured. As this renders the mirrored packets unroutable, the end point of the GRE tunnel must be the network analyzer.

- **SPAN over Pseudo-Wire**: Pseudo-wire traffic mirroring (known as PW-SPAN) is an extra functionality on the existing SPAN solutions. In PW-SPAN, the traffic mirroring destination port is configured as pseudo-wire rather than a physical port. Here, the designated traffic on the source port is mirrored over the pseudo-wire to a central location.
- **File Mirroring**: File mirroring feature enables the router to copy files or directories automatically from `/harddisk:/mirror` location in active RP to `/harddisk:/mirror` location in standby RP or RSP without user intervention or EEM scripts.

Traffic Mirroring Terminology

- Ingress Traffic — Traffic that comes into the router.
- Egress Traffic — Traffic that goes out of the router.
- Source (SPAN) interface — An interface that is monitored using the SPAN feature.
- Source port—A port that is monitored with the use of traffic mirroring. It is also called a monitored port.
- Destination port—A port that monitors source ports, usually where a network analyzer is connected. It is also called a monitoring port.
- Monitor session—A designation for a collection of SPAN configurations consisting of a single destination and, potentially, one or many source interfaces.

Characteristics of Source Port

A source port, also called a monitored port, is a routed port that you monitor for network traffic analysis. In a single traffic mirroring session, you can monitor source port traffic. The Cisco NCS 5500 Series router support a maximum of up to 800 source ports.

A source port has these characteristics:

- It can be any data port type, such as Bundle Interface, 100 Gigabit Ethernet, or 10 Gigabit Ethernet.

Note
- Bridge group virtual interfaces (BVIs) are not supported.
- Bundle members cannot be used as source ports.

- Each source port can be monitored in only one traffic mirroring session.
- When a port is used as a source port, the same port cannot be used as a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor local traffic mirroring. Remote traffic mirroring is supported both in the ingress and egress directions. For bundles, the monitored direction applies to all physical ports in the group.

Characteristics of Destination Port

Each session must have a destination port or file that receives a copy of the traffic from the source ports.

A destination port has these characteristics:

- A destination port must reside on the same router as the source port for local traffic mirroring. For remote mirroring, the destination is always a GRE tunnel.
- For remote mirroring, the destination is a GRE tunnel. From Release 7.4.1, the destination can be an L2 sub-interface on NC57 line cards.
- A destination port for local mirroring can be any Ethernet physical port, EFP, GRE tunnel interface, or bundle interface. It can be a Layer 2 or Layer 3 transport interface.

Note Bridge group virtual interfaces (BVIs) as destination ports are not supported.

- At any one time, a destination port can participate in only one traffic mirroring session. A destination port in one traffic mirroring session cannot be a destination port for a second traffic mirroring session. In other words, no two monitor sessions can have the same destination port.
- A destination port cannot also be a source port.

Characteristics of Monitor Session

A monitor session is a collection of traffic mirroring configurations consisting of a single destination and, potentially, many source interfaces. For any given monitor session, the traffic from the source interfaces (called *source ports*) is sent to the monitoring port or destination port. If there are more than one source port in a monitoring session, the traffic from the several mirrored traffic streams is combined at the destination port. The result is that the traffic that comes out of the destination port is a combination of the traffic from one or more source ports.

Monitor sessions have these characteristics:

- Prior to Cisco IOS XR Software Release 7.8.1, a single router could support up to four monitor sessions. However, configuring SPAN and CFM on the router reduced the maximum number of monitor sessions to two, as both shared the mirror profiles.

  Maximum number of monitor sessions supported can vary from 2 to 4, based on the directions (rx| tx| both) we enable for the sessions.

  The following table summarizes the maximum number of monitor sessions supported for various combinations of sessions direction.

Combinations of Sessions Direction	Maximum Number of Sessions Supported
{both, both}	2
{rx|tx, rx|tx, both}	3
{rx|tx, rx|tx, rx|tx, rx|tx}	4

  Starting from Cisco IOS XR Software Release 7.8.1, a limit of three monitor sessions on the router is introduced. But, if you configure SPAN and CFM on the router, the maximum number of monitor sessions decreases to one, as both functions use the same mirror profiles.

  From 7.2.1 to 7.3.1, Cisco NC57 line cards support only four Rx and three Tx monitor sessions for both compatibility and native mode. From Cisco IOS XR Software Release 7.4.1, up to 24 sessions are supported for native mode. Sessions can be configured as Rx-only, Tx-only, or Rx/Tx.

- A single monitor session can have only one destination port.
- A single destination port can belong to only one monitor session.
- A monitor session can have a maximum of 800 source ports, as long as the maximum number of source ports from all monitoring sessions does not exceed 800.

Restrictions

Generic Restrictions

The following are the generic restriction(s) related to traffic mirroring:

- Partial mirroring and sampled mirroring are not supported.
- The destination bundle interfaces flap when:
  - both the mirror source and destination are bundle interfaces in LACP mode and
  - mirror packets next-hop is a router or a switch instead of a traffic analyzer.

  This behavior is observed due to a mismatch of LACP packets on the next-hop bundle interface due to the mirroring of LACP packets on the source bundle interface.
- Both SPAN and ERSPAN features cannot be configured on a router simultaneously. Either SPAN or ERSPAN feature can be configured on the same router.
- Sub-interface with only one VLAN is supported as source for traffic mirroring.
- For NCS 5500 line cards in NCS 5500 Modular routers, sub-interface with only one VLAN is supported as source for traffic mirroring.

- Bundle members cannot be used as destination ports.
- From Cisco IOS XR Software Release 7.2.1 to 7.3.1, Cisco NC57 line cards support only four Rx and three Tx monitor sessions.
- Prior to Cisco IOS XR Software Release 7.8.1, a single router could support up to four monitor sessions. However, configuring SPAN and CFM on the router reduced the maximum number of monitor sessions to two, as both shared the mirror profiles.
- Cisco NC57 line cards support a total of 24 sessions, which can be configured as Rx-only, Tx-only, or Rx/Tx.
- Starting from Cisco IOS XR Software Release 7.8.1, a limit of three monitor sessions on the NCS 5500 router is introduced. But, if you configure SPAN and CFM on the router, the maximum number of monitor sessions decreases to one, as both functions use the same mirror profiles.
- From Cisco IOS XR Software Release 7.10.1, a single router can have a maximum of four monitor sessions. However, both SPAN and CFM share common mirror profiles.If you configure SPAN and CFM together on the router, the maximum number of monitor sessions may reduce to two.
- Fragmentation of mirror copies is not handled by SPAN when SPAN destination MTU is less than the packet size.Existing behaviour if the MTU of destination interface is less than the packet size is as below:

Platforms	Rx SPAN	Tx SPAN
NCS 5500	You get single mirror copy in the destination. Fragmentation is not attempted in this case.	Mirror copies are fragmented before sending out of the destination. This is because the packets are fragmented before egressing out of the original destination and the mirror copy is generated after recycle.
NCS 5700	You do not receive mirror copy here. Here fragmentation is attempted but fails, as the packets are dropped in SPP due to NULL SSP value in the system header of the mirror copy.	Mirror copies are fragmented before sending out of the destination.

  You can configure the SPAN destination with an MTU which is greater than the packet size.
- Until Cisco IOS XR Software Release 7.6.1, SPAN only supports port-level source interfaces.

SPAN over Pseudo-Wire Restrictions

ERSPAN Restrictions

The following restrictions apply to ERSPAN:

- The value of ERSPAN session-ID is always zero. IOS XR Command for configuring ERPAN is not available.
- ERSPAN next-hop must have ARP resolved. Any other traffic or protocol will trigger ARP.
- ERSPAN cannot travel over MPLS.

- Additional routers may encapsulate in MPLS.

- ERSPAN decapsulation is not supported.
- ERSPAN does not work if the GRE next hop is reachable over sub-interface. For ERSPAN to work, the next hop must be reachable over the main interface.
- When you use the same ACEs defined in both the IPv4 and IPv6 ACLs, the router doesn't perform ERSPAN mirroring for the ACLs that have the priority set as 2 ms.

SPAN-ACL Restrictions

The following restrictions apply to SPAN-ACL:

- SPAN-ACL is only supported in the Rx direction, that is, in the ingress direction v4 or v6 ACL.
- MPLS traffic cannot be captured with SPAN-ACL.
  - ACL for any MPLS traffic is not supported.

Configure Traffic Mirroring

These tasks describe how to configure traffic mirroring:

Configure Remote Traffic Mirroring

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 **monitor-session** *session-name*

Example:

```
RP/0/RP0/CPU0:router(config)# monitor-session mon1 ethernet
RP/0/RP0/CPU0:router(config-mon)#
```

Defines a monitor session and enters monitor session configuration mode.

Step 3 **destination interface** *tunnel-ip*

Example:

```
RP/0/RP0/CPU0:router(config-mon)# destination interface tunnelip3
```

Specifies the destination subinterface to which traffic is replicated.

Step 4 **exit**

Example:

```
RP/0/RP0/CPU0:router(config-mon)# exit
RP/0/RP0/CPU0:router(config)#
```

Exits monitor session configuration mode and returns to global configuration mode.

Step 5 **interface** *type number*

Example:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/1
```

Enters interface configuration mode for the specified source interface. The interface number is entered in *rack*/*slot*/*module*/*port* notation. For more information about the syntax for the router, use the question mark (?) online help function.

Step 6 **monitor-session** *session-name* **ethernet direction rx-onlyport-only**

Example:

```
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1 ethernet
direction rx-only port-only
```

Specifies the monitor session to be used on this interface. Use the **direction** keyword to specify that only ingress or egress traffic is mirrored.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0/CPU0:router(config-if)# end
```

or

```
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  ```
  Uncommitted changes found, commit them before exiting (yes/no/cancel)?
  [cancel]:
  ```

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 8 **show monitor-session [session-name] status** [**detail**] [**error**]

Example:

```
RP/0/RP0/CPU0:router# show monitor-session
```

Displays information about the traffic mirroring session.

Example

This example shows the basic configuration for traffic mirroring with physical interfaces.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# monitor-session ms1
RP/0/RP0/CPU0:router(config-mon)# destination interface HundredGigE0/2/0/15
RP/0/RP0/CPU0:router(config-mon)# commit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE0/2/0/19
RP/0/RP0/CPU0:router(config-if)# monitor-session ms1 port-level
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE0/2/0/19
RP/0/RP0/CPU0:router(config-if)# monitor-session ms1 direction rx-only port-level
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE0/2/0/19
RP/0/RP0/CPU0:router(config-if)# monitor-session ms1 direction tx-only port-level
RP/0/RP0/CPU0:router(config-if)# commit
```

This example shows sample output of the show monitor-session command with the status keyword:

```
RP/0/RSP0/CPU0:router# show monitor-session status
Monitor-session cisco-rtp1
Destination interface HundredGigE 0/5/0/38
================================================================================
Source Interface Dir Status
---------------------- ---- -------------------------------------------------
TenGigE0/5/0/4 Both Operational
TenGigE0/5/0/17 Both Operational
RP/0/RSP0/CPU0:router# show monitor-session status detail
Monitor-session sess1
Destination interface is not configured
Source Interfaces
-----------------
TenGigE0/1/0/0
Direction: Both
ACL match: Disabled
Portion: Full packet
Status: Not operational (destination interface not known).
TenGigE0/1/0/1
Direction: Both
ACL match: Disabled
Portion: First 100 bytes

RP/0/RSP0/CPU0:router# show monitor-session status error
Monitor-session ms1
Destination interface TenGigE0/2/0/15 is not configured
================================================================================
Source Interface Dir Status
---------------------- ---- -------------------------------------------------
```

```
Monitor-session ms2
Destination interface is not configured
================================================================================
Source Interface Dir Status
-------------------- ---- ------------------------------------------------------
RP/0/RP0/CPU0:router# show monitor-session test status
Monitor-session test (ipv4)
Destination Nexthop 255.254.254.4
================================================================================================
Source Interface Dir Status
------------------------------------------------------------------------------------------------
Gi0/0/0/2.2 Rx Not operational (source same as destination)
Gi0/0/0/2.3 Rx Not operational (Destination not active)
Gi0/0/0/2.4 Rx Operational
Gi0/0/0/4 Rx Error: see detailed output for explanation
RP/0/RP0/CPU0:router# show monitor-session test status error
Monitor-session test
Destination Nexthop ipv4 address 255.254.254.4
================================================================
Source Interface Status
----------------------------------------------------------------
Gi0/0/0/4 < Error: FULL Error Details >
```

Configuring ACLs for Traffic Mirroring

This section describes the configuration for creating ACLs for traffic mirroring.

In ACL-based traffic mirroring, traffic is mirrored based on the configuration of the interface ACL. You can mirror traffic based on the definition of an interface access control list. When you're mirroring Layer 3 or Layer 2 traffic, the ACL is configured using the **ipv4 access-list** or the **ipv6 access-list** command with the **capture** option. The **permit** and **deny** commands determine the behavior of the regular traffic.

Guidelines and Restrictions

The following general restrictions apply to traffic mirroring using ACLs:

- Traffic mirroring counters are not supported.
- ACL-based traffic mirroring is not supported with Layer 2 (ethernet-services) ACLs.
- Main interface as span source interface and ACL with capture keyword on same main interface's sub-interface are not supported.
- If a SPAN session with **acl** keyword is applied on an interface with no ACL rule attached to that interface, SPAN happens without any filtering.
- Configure one or more ACLs on the source interface or any interface on the same network processing unit as the source interface, to avoid default mirroring of traffic. If a Bundle interface is a source interface, configure the ACL on any interface on the same network processing unit as all active bundle-members. Bundle members can be on multiple NPUs. Also, ensure that the ACLs configured are of the same protocol type and direction as the SPAN configuration. For example, if you configure SPAN with ACL for IPv4 or IPv6, configure an ingress IPv4 or IPv6 ACL on that network processing unit respectively.

Configure an IPv4 ACL

Use the following steps to configure ACLs for traffic mirroring.

```
/* Create an IPv4 ACL (TM-ACL) for traffic mirroring */
Router(config)# ipv4 access-list TM-ACL
Router(config-ipv4-acl)# 10 permit udp 10.1.1.0 0.0.0.255 eq 10 any capture
Router(config-ipv4-acl)# 20 permit udp 10.1.1.0 0.0.0.255 eq 20 any
Router(config-ipv4-acl)# exit
Router(config)# commit

/* Validate the configuration */
Router(config)# show run
Thu May 17 11:17:49.968 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Thu May 17 11:17:47 2018 by user
…
ipv4 access-list TM-ACL
 10 permit udp 10.1.1.0 0.0.0.255 eq 10 any capture
 20 permit udp 10.1.1.0 0.0.0.255 eq 20 any
!
…
```

You have successfully configured an IPv4 ACL for traffic mirroring.

ACL-based Traffic Mirroring for Outgoing (Tx) Traffic on Cisco NCS 5700 Series Line Cards and Routers

Table 1: Feature History Table

Feature Name	Release Information	Description
Egress Hybrid ACL-based Traffic Mirroring on Cisco NCS 5700 Series Line Cards and Routers	Release 7.10.1	Introduced in this release on: NCS 5700 fixed port routers (select variants only*); NCS 5700 line cards [Mode: Native] (select variants only*) We've now made it possible for you to narrow down the outgoing (Tx) traffic that you want to mirror and troubleshoot the captured traffic for any anomalous or malicious activity. You can do this by enabling the **capture** option on an L3 interface that has a hybrid ACL configured and Egress Traffic Management (ETM) mode enabled. The traffic matching the rules defined in the egress hybrid ACL gets captured and mirrored. This feature introduces the following changes: **CLI**: The **capture** keyword is introduced in the **ipv4 access-list** and **ipv6 access-list** commands. * This feature is supported on: • NCS-57B1-5DSE-SYS • NCS-57C3-MODS-SYS • NC57-18DD-SE • NC57-36H-SE

With ACL-based traffic mirroring, you can create an ACL and attach that ACL to an L3 interface. The Tx traffic on that interface, when matches with the rules defined in the ACLs, are mirrored. The mirrored traffic is used to troubleshoot issues such as packet drops, packet fields getting modified, virus attacks, or any other network threat.

Guidelines and Restrictions for ACL-based Traffic Mirroring for Outgoing (Tx) Traffic

The following are the general guidelines and restrictions that apply to traffic mirroring using ACLs for outgoing (Tx) traffic on Cisco NCS 5700 Series line cards and routers:

- SPAN configuration with **port mode** on the main interface and Tx SPAN ACL configuration on the sub-interface of the same port isn't supported.
- BVI interface as a SPAN source interface is not supported.
- Hybrid ACLs with only compress level 3 are supported.
- 24 SPAN sessions are supported for both Rx and Tx destinations.
- ACL-based traffic mirroring for the outgoing (Tx) traffic is supported on the following routers and line cards for L3 interfaces:
  - NCS-57B1-5DSE
  - NCS-57C3-MODS-SYS
  - NC57-18DD-SE
  - NC57-36H-SE

Prerequisites for ACL-based Traffic Mirroring for Outgoing (Tx) Traffic

To configure ACL-based traffic mirroring on Cisco NCS 5700 Series line cards and routers for Tx traffic, ensure that you perform the following prerequisites:

- You must have the native mode enabled. To enable the native mode, use the **hw-module profile npu native-mode-enable** command in the configuration mode. Ensure that you reload the router after configuring the native mode.
- To enable egress hybrid ACL, enable the **hw-module profile acl compress enable ingress** and **hw-module profile acl compress enable egress** commands.
- The SPAN source interface must have the ETM mode enabled. To enable the ETM mode, use the **controller optics***r*/*s*/*i*/*p***mode etm** command. For more information on the ETM mode, see the Configure Egress Traffic Management chapter.

Configure ACL-based Traffic Mirroring for Outgoing (Tx) Traffic

Perform the following steps to enable ACL-based traffic mirroring on Cisco NCS 5700 Series line cards and routers for outgoing (Tx) traffic:

1. Create an IPv4 or IPv6 ACL with **capture** option to define the traffic that you want to mirror.
2. Configure a source L3 interface for outgoing (Tx) traffic.
3. Start a monitor session, configure the destination interface, and the ACL to start capturing the outgoing (Tx) traffic.

Configuration Example

The following example displays the outgoing (Tx) traffic or packets captured for IPv4 (v4-acl-tx) and IPv6 (v6-acl-tx) ACLs:

```
/* Create a SPAN IPv4 ACL (v4-acl-tx) for traffic mirroring */
Router(config)# ipv4 access-list v4-acl-tx
Router(config-ipv4-acl)# 10 permit icmp net-group sip net-group dip capture
Router(config-ipv4-acl)# 20 permit udp net-group sip net-group dip port-group dport
Router(config-ipv4-acl)# 30 permit ipv4 net-group sip_traffic net-group dip_traffic capture
```

```
Router(config-ipv4-acl)# exit
Router(config)# commit

/*Create a SPAN IPv6 ACL (v6-acl-tx) for traffic mirroring */
Router(config)# ipv6 access-list v6-acl-tx
Router(config-ipv6-acl)# 10 permit icmpv6 net-group sip net-group dip
Router(config-ipv6-acl)# 20 permit udp net-group sip net-group dip port-group dport
Router(config-ipv6-acl)# 30 permit ipv6 net-group sip_traffic net-group dip_traffic capture
Router(config-ipv6-acl)# exit
Router(config)# commit

/* Start a monitor session on your source interface for incoming (Rx) traffic and specify
the destination interface*/
Router(config)# interface HundredGigE0/4/0/18
Router(config)# monitor-session mon1
Router(config-mon)# destination interface HundredGigE0/1/0/30
Router(config-mon)#commit
Router(config-mon)#exit

/* Configure the ACL on the source interface to capture the outgoing (Tx) traffic */
Router(config)# interface HundredGigE0/4/0/18
Router(config-if)# monitor-session mon1 ethernet direction tx-only port-level
acl
Router(config-if)# ipv4 access-group v4-acl-tx egress compress level 3
Router(config-if)# ipv6 access-group v6-acl-tx egress compress level 3
!
```

Running Configuration

Use the **show run monitor-session** to and **show running-config interface** commands to display a running configuration on your router.

```
Router#show run monitor-session mon1
monitor-session mon1 ethernet
 destination interface HundredGigE0/1/0/30
!

Router#show run interface hundredGigE 0/4/0/18
interface HundredGigE0/4/0/18
 ipv4 address 20.71.103.1 255.255.255.0
 ipv6 address abc::20:71:103:1/112
 monitor-session mon1 ethernet direction tx-only
  acl
 !
 encapsulation dot1ad 10 dot1q 201
 ipv4 access-group v4-acl-tx egress compress level 3
 ipv6 access-group v6-acl-tx egress compress level 3


Router#sh access-lists ipv4 v4-acl-tx
ipv4 access-list v4-acl-tx
 10 permit udp net-group sip port-group sport net-group dip-v4-acl-tx-cap capture
 20 permit udp net-group sip port-group sport net-group dip-v4-acl-tx-DNcap
 100 permit udp any any capture
 101 permit ipv4 any any
 102 permit tcp any any

Router#sh access-lists ipv6 v6-acl-tx
ipv6 access-list v6-acl-tx
 10 permit udp net-group sip-v6 port-group sport net-group dip-v6-acl-tx-cap-v6 capture
 20 permit udp net-group sip-v6 port-group sport net-group dip-v6-acl-tx-DNcap-v6
```

```
 100 permit udp any any
 101 permit ipv6 any any
 102 permit tcp any any


Router#sh access-lists ipv6 v6-acl-tx hardware egress location 0/4/CPU0
ipv6 access-list v6-acl-tx
 10 permit udp net-group sip-v6 port-group sport net-group dip-v6-acl-tx-cap-v6 capture
(2100 matches) (252004 bytes)
 20 permit udp net-group sip-v6 port-group sport net-group dip-v6-acl-tx-DNcap-v6
 100 permit udp any any
 101 permit ipv6 any any
 102 permit tcp any any

Router#sh access-lists ipv4 v4-acl-tx hardware egress location 0/4/CPU0
ipv4 access-list v4-acl-tx
 10 permit udp net-group sip port-group sport net-group dip-v4-acl-tx-cap capture (2095
matches) (209500 bytes)
 20 permit udp net-group sip port-group sport net-group dip-v4-acl-tx-DNcap
 100 permit udp any any capture
 101 permit ipv4 any any
 102 permit tcp any any
```

Verification

To verify that the outgoing (Tx) traffic is configured on the source interface, use the **show monitor-session status** command.

```
/* Verify the status of the outgoing (Tx) traffic on the source interface */
Router:ios#show monitor-session mon1 status
Monitor-session mon1
Destination interface HundredGigE0/1/0/30
================================================================================
Source Interface      Dir   Status
--------------------- ----  ------------------------------------------------
Hu0/4/0/18        Tx    Operational

Router#sh run monitor-session mon1
monitor-session mon1 ethernet
 destination interface HundredGigE0/1/0/30
!
```

To verify that the IPv4 and IPv6 ACL captures the ACL information, use the **show access-lists** [**ipv4** | **ipv6**] *acl-name* **hardware ingress span** [**detail** | **interface** | **location** | **sequence** | **verify**] **location** *x* command. Notice that the traffic or the packets are getting captured(256500356 matches) and also getting incremented.

```
/* Verification for IPv4 ACL */
Router#show access-lists ipv4 v4-acl-tx hardware egress location 0/4/CPU0
ipv4 access-list v4-acl-tx
 10 permit udp net-group sip port-group sport net-group dip capture (2095 matches) (209500
 bytes)
 20 permit udp net-group sip port-group sport net-group dip port-group dport
 100 permit udp any any capture
 101 permit ipv4 any any
 102 permit tcp any any
Router#show interface HundredGigE0/4/0/18
HundredGigE0/4/0/18 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 00bc.602b.0a88
  Internet address is 20.71.103.1/24
```

```
  MTU 1522 bytes, BW 100000000 Kbit (Max: 100000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation 802.1ad-802.1Q Virtual LAN,  loopback not set,
  Last link flapped 12:12:06
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     982 packets input, 86352 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
     4942 packets output, 523002 bytes, 0 total output drops
     Output 0 broadcast packets, 256 multicast packets

Router#show interfaces hundredGigE 0/4/0/18 accounting
HundredGigE0/4/0/18
  Protocol              Pkts In         Chars In     Pkts Out        Chars Out
  IPV4_UNICAST                0                0         2099           209900
  IPV6_UNICAST              489            44034         2103           252364
  ARP                         4              240            5              250
  IPV6_ND                   489            42078          745            61592


Router#show interfaces hundredGigE 0/1/0/30
HundredGigE0/1/0/30 is up, line protocol is up
  Interface state transitions: 3
  Hardware is HundredGigE, address is 00bc.602b.0908 (bia 00bc.602b.0908)
  Internet address is 20.21.3.1/30
  MTU 1514 bytes, BW 100000000 Kbit (Max: 100000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 100000Mb/s, 100GBASE-LR4, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  Last link flapped 00:04:08
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output 00:00:05
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4908 packets output, 519403 bytes, 0 total output drops
     Output 10 broadcast packets, 65 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     3 carrier transitions

/* Verification for IPv6 ACL */
Router#show access-lists ipv6 v6-acl-tx hardware egress location 0/4/CPU0
ipv6 access-list v6-acl-tx
 10 permit udp net-group sip-v6 port-group sport net-group dip-v6-acl-tx capture (2100
matches) (252004 bytes)
 20 permit udp net-group sip-v6 port-group sport net-group dip-v6-DNacl-tx
 100 permit udp any any
 101 permit ipv6 any any
 102 permit tcp any any
```

Attaching the Configurable Source Interface

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 **interface** *type number*

Example:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/1
```

Enters interface configuration mode for the specified source interface. The interface number is entered in *rack*/*slot*/*module*/*port* notation. For more information about the syntax for the router, use the question mark (?) online help function.

Step 3 **ipv4 access-group** *acl-name* {**ingress** | **egress**}

Example:

```
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group acl1 ingress
```

Controls access to an interface.

Step 4 **monitor-session** *session-name* **ethernet direction rx-onlyport-level acl**

Example:

```
RP/0/RP0/CPU0:router(config-if)# monitor-session mon1 ethernet direction rx-only port-level acl
RP/0/RP0/CPU0:router(config-if-mon)#
```

Attaches a monitor session to the source interface and enters monitor session configuration mode.

Note **rx-only** specifies that only ingress traffic is replicated.

Step 5 **acl**

Example:

```
RP/0/RP0/CPU0:router(config-if-mon)# acl
```

Specifies that the traffic mirrored is according to the defined ACL.

Note If an ACL is configured by name, then this step overrides any ACL that may be configured on the interface.

Step 6 **exit**

Example:

```
RP/0/RP0/CPU0:router(config-if-mon)# exit
RP/0/RP0/CPU0:router(config-if)#
```

Exits monitor session configuration mode and returns to interface configuration mode.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0/CPU0:router(config-if)# end
```

or

```
RP/0/RP0/CPU0:router(config-if)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting (yes/no/cancel)?
[cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 8 **show monitor-session [session-name] status** [**detail**] [**error**]

Example:

```
RP/0/RP0/CPU0:router# show monitor-session status
```

Displays information about the monitor session.

VLAN Subinterface as Source for Traffic Mirroring

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
VLAN Subinterface as Source for Traffic Mirroring	Release 7.5.2	You can now configure the VLAN subinterface as a source for traffic mirroring for: • Traffic ingressing at the interface • Traffic egressing at the interface • Traffic egressing and ingressing at the same interface You could configure mirror functionality only at the main interface level in earlier releases.

VLAN subinterface provides the flexibility to monitor ingress or egress or both directions traffic from all the active subinterfaces of the source VLAN. The active subinterfaces in the source VLAN are considered as source subinterfaces. When subinterfaces are added or removed from the source VLAN, the corresponding traffic is added or removed from the monitoring sources.

Restrictions

The following restrictions apply to VLAN subinterface as source for traffic mirroring:

VLAN Interface as Source for Traffic Mirroring

Configuration Example

```
Router# configure
Router(config)# monitor-session mon1 ethernet
Router(config-mon)# destination interface tunnel-ip 3
Router(config-mon)# exit
Router(config)# interface HundredGigE 0/1/0/1.10
Router(config-subif)#
monitor-session mon1 ethernet
Router(config-if-mon)# commit
```

Running Configuration

```
Router# show run monitor-session mon1
monitor-session mon1 ethernet
 destination interface tunnel-ip3
!
```

```
Router# show run interface HundredGigE 0/1/0/1.10
 interface HundredGigE0/1/0/1.10
  encapsulation dot1q 10
   ipv4 address 101.1.2.1 255.255.255.252
    monitor-session mon1 ethernet
    !
   !
  !
```

Verification

```
Router# show monitor-session status
Monitor-session mon1
Destination interface tunnel-ip3
================================================================================
Source Interface Dir Status
---------------------- ---- -----------------------------------------------------
HundredGigE 0/1/0/1.10  Both Operational
```

Configuring UDF-Based ACL for Traffic Mirroring

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

Step 2	**udf** *udf-name* **header** {**inner** | **outer**} {**l2** | **l3** | **l4**} **offset** *offset-in-bytes* **length** *length-in-bytes*
	Example:
	`RP/0/RP0/CPU0:router(config)# udf udf3 header outer l4 offset 0 length 1`
	`(config-mon)#`
	Example:
	`RP/0/RP0/CPU0:router(config)# udf udf3 header inner l4 offset 10 length 2`
	`(config-mon)#`
	Example:
	`RP/0/RP0/CPU0:router(config)# udf udf3 header outer l4 offset 50 length 1`
	`(config-mon)#`
		Configures individual UDF definitions. You can specify the name of the UDF, the networking header from which offset, and the length of data to be extracted.
		The **inner** or **outer** keywords indicate the start of the offset from the unencapsulated Layer 3 or Layer 4 headers, or if there is an encapsulated packet, they indicate the start of offset from the inner L3/L4.
		Note The maximum offset allowed, from the start of any header, is 63 bytes
		The **length** keyword specifies, in bytes, the length from the offset. The range is from 1 to 4.

Step 3	**ipv4 access-list** *acl-name* **Example:** `RP/0/RP0/CPU0:router(config))# ipv4 access-list acl1`	Creates ACL and enters IP ACL configuration mode. The length of the *acl-name* argument can be up to 64 characters.

Step 4	**permit** *regular-ace-match-criteria* **udf** *udf-name1 value1 ... udf-name8 value8*
	Example:
	`RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 any any udf udf1 0x1234 0xffff udf3 0x56 0xff capture`
	`RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit ipv4 any any dscp af11 udf udf5 0x22 0x22 capture`
		Configures ACL with UDF match.

Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(config-ipv4-acl)# exit`	Exits IP ACL configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**interface***type number* **Example:** `RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/2/0/2`	Configures interface and enters interface configuration mode.
Step 7	**ipv4 access-group** *acl-name* **ingress** **Example:** `RP/0/RP0/CPU0:router(config-if)# ipv4 access-group acl1 ingress`	Applies access list to an interface.
Step 8	**commit** **Example:** `RP/0/RP0/CPU0:router(config-if)# commit`	Applies access list to an interface.

Verifying UDF-based ACL

Use the **show monitor-session status detail** command to verify the configuration of UDF on ACL.

```
RP/0/RP0/CPU0:leaf1# show monitor-session 1 status detail

Fri May 12 19:40:39.429 UTC
Monitor-session 1
  Destination interface tunnel-ip3
  Source Interfaces
  -----------------
  TenGigE0/0/0/15
    Direction:  Rx-only
    Port level: True
    ACL match:  Enabled
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Not operational (destination not active)
```

Traffic Mirroring on Layer 2 Interfaces

Monitoring Traffic Mirroring on a Layer 2 Interface

This section describes the configuration for monitoring traffic on a Layer 2 interface.

Configuration

To monitor traffic mirroring on a Layer 2 interface, configure the monitor under `l2transport` sub-config of the interface:

```
RP/0/RP0/CPU0:router(config)# interface TenGigE0/0/0/42
RP/0/RP0/CPU0:router(config-if)# l2transport
RP/0/RP0/CPU0:router(config-if-l2)# monitor-session EASTON ethernet port-level
```

Verification

```
RP/0/RP0/CPU0:router# show monitor-session status
Thu Aug 29 21:42:22.829 UTC
Monitor-session EASTON
Destination interface TenGigE0/0/0/20
=============================================
Source Interface      Dir   Status
--------------------- ----  -----------------
Te0/0/0/42 (port)     Both  Operational
```

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) transports mirrored traffic over an IP 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.

ERSPAN involves mirroring traffic through a GRE tunnel to a remote site. For more information on configuring the GRE tunnel that is used as the destination for the monitor sessions, see the chapter *Configuring GRE Tunnels*.

Multiple ERSPAN Sessions in Single Interface

Table 3: Feature History Table

Feature Name	Release Information	Description
Multiple ERSPAN Sessions in a Single Interface	Release 7.5.4	With this release, you can configure multiple ERSPAN sessions under a single interface. A maximum of four sessions can be configured simultaneously. This feature, which is supported on layer 3 interfaces, helps you in monitoring traffic from different parts of your network simultaneously to see the network's overall performance. In addition, using this feature, you can get a better network visibility, more efficient use of network resources, and flexibility. You should specify the monitor sessions to be used on the interface. Use the following command with the direction keyword to specify that only the ingress traffic is mirrored: **monitor-session** *session name***ethernet direction rx-only port-level**

This feature allows you to configure multiple ERSPAN sessions in the same source interface. The maximum number of sessions that are supported under an interface is four. The ACL is applicable only in the ingress direction (direction Rx). This configuration is supported only on Layer 3 interfaces.

To differentiate multiple SPAN sessions under the same source interface, span session ID is used. When a packet matches multiple entries at the router, priority attribute is used to choose the correct destination for the packet. When a single packet tries to match multiple SPAN sessions, you should configure correct priority fields to identify the correct destination. The ACL with the lowest priority is chosen.

For Cisco NCS 5500 routers, the merge group value is always 1, and the priority value can be of any value within the supported range of 1 to1000.

Multiple ERSPAN sessions in a single interface help the administrators in the following ways:

- Monitor traffic from different parts of your network simultaneously to see the overall network performance.
- Isolate traffic from specific networks for troubleshooting network issues.
- Segment traffic for different purposes, such as security, compliance, or performance analysis.

Limitations and Restrictions

- All sessions under the source port should have SPAN access control list (ACL) enabled.
- A few sessions with SPAN ACL and a few without SPAN ACLs in the same source interface are not supported.
- No two sessions should have the same ACL in the same source interface. Each session should have a different ACL.
- Multiple sessions without ACL in the same interface are not supported.
- One SPAN session with the keyword ACL (use security acl as the keyword) and other SPAN sessions with the keyword SPAN ACL are not supported.
- At a time, you can make only one mirror copy of a packet.
- Capturing keywords is not required.
- Multiple sessions under the same interface cannot have a combination of directions. Only RX is supported.

Configuring Multiple ERSPAN Sessions

Configuring Multiple Sessions with ACL

Specify the monitor sessions to be used on the interface. Use the direction keyword to specify that only ingress traffic is mirrored. See the following example:

```
Router(config)#interface TenGigE0/0/0/26
Router(config-if)#monitor-session ses1 ethernet direction rx-only port-level
Router(config-if)#acl ipv4 acl1
!
Router(config-if)#monitor-session ses2 ethernet direction rx-only port-level
Router(config-if)#acl ipv4 acl2
!
Router(config-if)#monitor-session ses3 ethernet direction rx-only port-level
Router(config-if)#acl ipv4 acl3
!
Router(config-if)#monitor-session ses4 ethernet direction rx-only port-level
Router(config-if)#acl ipv4 acl4
!
!
```

Verifying the Sessions

The following example shows the details of the monitor sessions.

```
Router##sh monitor-session status
Tue Mar 21 16:14:15.879 UTC
Monitor-session ses1
Destination interface TenGigE0/0/0/9
================================================================================
Source Interface      Dir   Status
--------------------- ----  --------------------------------------------------
Te0/0/0/0 (port)      Rx    Operational

Monitor-session ses2
Destination interface TenGigE0/0/0/1
================================================================================
Source Interface      Dir   Status
--------------------- ----  --------------------------------------------------
Te0/0/0/0 (port)      Rx    Operational

Monitor-session ses3
Destination interface TenGigE0/0/0/2
================================================================================
Source Interface      Dir   Status
--------------------- ----  --------------------------------------------------
Te0/0/0/0 (port)      Rx    Operational

Monitor-session ses4
Destination interface TenGigE0/0/0/6
================================================================================
Source Interface      Dir   Status
--------------------- ----  --------------------------------------------------
Te0/0/0/0 (port)      Rx    Operational
RP/0/RP0/CPU0:ios#
```

Configuring the Correct Priority

When one packet tries to match more than one SPAN session, the priority field helps in identifying the correct destination.

Note Merge group and priority fields are not mandatory. But if used, configure both fields.

```
Router(config)#interface tenGigE 0/0/0/24
Router(config-if)#monitor-session ses1 ethernet port-level
Router(config-if)#acl ipv4 acl1 merge-group 1 priority 30
```

To verify the traffic, use the following sample **show monitor-session** command:

```
Router#show monitor-session status detail
Tue Mar 21 16:15:02.741 UTC
Monitor-session ses1
  Destination interface TenGigE0/0/0/9
  Source Interfaces
  -----------------
  TenGigE0/0/0/0
    Direction:    Rx-only
    Port level:   True
    ACL match:    Disabled
    IPv4 ACL:     Enabled (acl1, merge-group: 1,priority: 1)
    IPv6 ACL:     Disabled
    Portion:      Full packet
    Interval:     Mirror all packets
    Mirror drops: Disabled
    Status:       Operational

Monitor-session ses2
```

```
  Destination interface TenGigE0/0/0/1
  Source Interfaces
  -----------------
  TenGigE0/0/0/0
    Direction:    Rx-only
    Port level:   True
    ACL match:    Disabled
    IPv4 ACL:     Enabled (acl2)
    IPv6 ACL:     Disabled
    Portion:      Full packet
    Interval:     Mirror all packets
    Mirror drops: Disabled
    Status:       Operational

Monitor-session ses3
  Destination interface TenGigE0/0/0/2
  Source Interfaces
  -----------------
  TenGigE0/0/0/0
    Direction:    Rx-only
    Port level:   True
    ACL match:    Disabled
    IPv4 ACL:     Enabled (acl3)
    IPv6 ACL:     Disabled
    Portion:      Full packet
    Interval:     Mirror all packets
    Mirror drops: Disabled
    Status:       Operational

Monitor-session ses4
  Destination interface TenGigE0/0/0/6
  Source Interfaces
  -----------------
  TenGigE0/0/0/0
    Direction:    Rx-only
    Port level:   True
    ACL match:    Disabled
    IPv4 ACL:     Enabled (acl4)
    IPv6 ACL:     Disabled
    Portion:      Full packet
    Interval:     Mirror all packets
    Mirror drops: Disabled
    Status:       Operational
Router#
```

Monitor Multiple ERSPAN Sessions with SPAN and Security ACL

Table 4: Feature History Table

Feature Name	Release Information	Feature Description
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.

Starting Cisco IOS XR Software Release 7.5.4 you can monitor multiple ERSPAN sessions using GREv4 under the same source interface. Multiple ERSPAN monitor sessions configured on an interface allow you to choose the destination interface for the mirrored traffic. For the configuration of monitor sessions, you can use SPAN and security ACLs together.

The SPAN and security ACLs are applicable only in the ingress traffic.

Configure Multiple ERSPAN monitor Sessions with SPAN and Security ACL

This example shows how to attach the SPAN and security ACLs to configure multiple monitoring sessions.

Configuration example

Use the following configuration to attach SPAN and security ACLs for traffic mirroring.

```
Router# config
/*Perform the following configurations to attach the SPAN ACL to an interface*/
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
/*Perform the following configurations to attach the security ACL to an interface*/
Router(config-if)#ipv4 access-group sec_aclv4 ingress
Router(config-if)#ipv6 access-group sec_aclv6 ingress
Router(config-if)#commit
```

Running configuration

```
Router(config)#show running-config interface
monitor-session always-on-v4 ethernet direction rx-only port-level
  acl ipv4 v4-monitor-acl2
```

```
  acl ipv6 v6-monitor-acl2
!
monitor-session on-demand-v4 ethernet direction rx-only port-level
  acl ipv4 v4-monitor-acl2
  acl ipv6 v6-monitor-acl2
!
ipv4 access-group sec_aclv4 ingress
ipv6 access-group sec_aclv6 ingress
!
!
```

Introduction to ERSPAN Egress Rate Limit

With ERSPAN egress rate limit feature, you can monitor traffic flow through any IP network. This includes third-party switches and routers.

ERSAPN operates in the following modes:

- ERSPAN Source Session – box where the traffic originates (is SPANned).
- ERSPAN Termination Session or Destination Session – box where the traffic is analyzed.

This feature provides rate limiting of the mirroring traffic or the egress traffic. With rate limiting, you can limit the amount of egress traffic to a specific rate, which prevents the network and remote ERSPAN destination traffic overloading. Be informed, if the egress rate-limit exceeds then the system may cap or drop the monitored traffic.

You can configure the QoS parameters on the traffic monitor session.

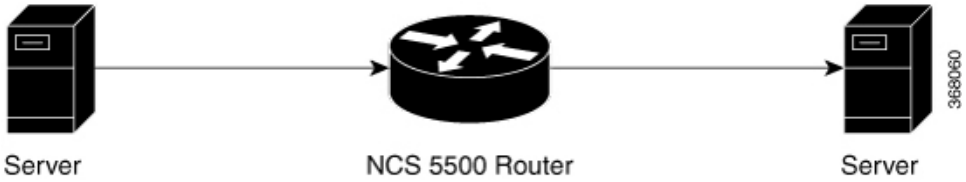
- Traffic Class (0 through 7)
  - Traffic class 0 has the lowest priority and 7 the highest.
  - The default traffic class is the same as that of the original traffic class.
- The Discard Class (0 through 2):
  - The default is 0.
  - The discard class configuration is used in WRED.

Benefits

With ERSPAN Egress rate limit feature, you can limit the egress traffic or the mirrored and use the mirrored traffic for data analysis.

Topology

Figure 2: Topology for ERSPAN Egress Rate Limit



The encapsulated packet for ERSPAN is in ARPA/IP format with GRE encapsulation. The system sends the GRE tunneled packet to the destination box identified by an IP address. At the destination box, SPAN-ASIC decodes this packet and sends out the packets through a port. ERSPAN egress rate limit feature is applied on the router egress interface to rate limit the monitored traffic.

The intermediate switches carrying ERSPAN traffic from source session to termination session can belong to any L3 network.

Configure ERSPAN Egress Rate Limit

Use the following steps to configure ERSPAN egress rate limit:

```
monitor-session ERSPAN ethernet
destination interface tunnel-ip1
!

RP/0/RP0/CPU0:pyke-008#sh run int tunnel-ip 1

interface tunnel-ip1
ipv4 address 4.4.4.1 255.255.255.0
tunnel mode gre ipv4
tunnel source 20.1.1.1
tunnel destination 20.1.1.2
!

RP/0/RP0/CPU0:pyke-008#sh run int hundredGigE 0/0/0/16

interface HundredGigE0/0/0/16
ipv4 address 215.1.1.1 255.255.255.0
ipv6 address 3001::2/64
monitor-session ERSPAN ethernet direction rx-only port-level
  acl
!
ipv4 access-group ACL6 ingress
```

Running Configuration

```
!! Policy-map to be used with the ERSPAN Destination (egress interface)
!! Traffic class is set to 5. For packets in this class, apply shaping
!! as well as WRED.
class-map match-any TC5
 match traffic-class 5
 end-class-map
!
policy-map shape-foo
 class TC5
  random-detect discard-class 0 10000 bytes 40000 bytes
  random-detect discard-class 1 40000 bytes 80000 bytes
  random-detect discard-class 2 80000 bytes 200000 bytes
```

```
  shape average percent 15
 !
 class class-default
 !
 end-policy-map
!
!!GRE Tunnel Interface
interface Loopback49
 ipv4 address 49.49.49.49 255.255.255.255
!
interface tunnel-ip100
 ipv4 address 130.100.1.1 255.255.255.0
 tunnel mode gre ipv4
 tunnel source 49.49.49.49
 tunnel destination 10.8.1.2
!
!!ERSPAN Monitor Session with GRE tunnel as the Destination Interface, and with QoS
configuration
monitor-session FOO ethernet
 destination interface tunnel-ip100
 traffic-class 5
 discard-class 1
!
!!ERSPAN Source Interface
interface TenGigE0/6/0/4/0
 description connected to TGEN 9/5
 ipv4 address 10.4.90.1 255.255.255.0
 monitor-session FOO ethernet port-level
 !
!
!!ERSPAN Destination ip-tunnel00’s underlying interface, with egress policy-map shape-foo
attached
interface TenGigE0/6/0/9/0
 service-policy output shape-foo
 ipv4 address 10.8.1.1 255.255.255.0
```

Verification

```
RP/0/RP0/CPU0:ios#show monitor-session FOO status detail
Wed May  2 15:14:05.762 UTC
Monitor-session FOO
  Destination interface tunnel-ip100
  Source Interfaces
  -----------------
  TenGigE0/6/0/4/0
    Direction:  Both
    Port level: True
    ACL match:  Disabled
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Operational
RP/0/RP0/CPU0:ios#
show monitor-session <sess-id> status internal

RP/0/RP0/CPU0:ios#show monitor-session FOO status internal
Wed May  2 15:13:06.063 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session FOO (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip100 (0x0800001c)
          Last error: Success
          Tunnel data:
            Mode: GREoIPv4
            Source IP: 49.49.49.49
            Dest IP: 10.8.1.2
```

```
            VRF:
            ToS: 0 (copied)
            TTL: 255
            DFbit: Not set
0/6/CPU0: Destination interface tunnel-ip100 (0x0800001c)
          Tunnel data:
            Mode: GREoIPv4
            Source IP: 49.49.49.49
            Dest IP: 10.8.1.2
            VRF:
            ToS: 0 (copied)
            TTL: 255
            DFbit: Not set

Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/6/CPU0: Name 'FOO', destination interface tunnel-ip100 (0x0800001c)
Platform, 0/6/CPU0:

  Dest Port: 0xe7d

  ERSPAN Encap:
    Tunnel ID: 0x4001380b
    ERSPAN Tunnel ID: 0x4001380c
    IP-NH Grp key: 0x3140000cc5
    IP-NH hdl: 0x308a5fa5e0
    IP-NH IFH: 0x30002a0
    IP-NH IPAddr: 10.4.91.2

  NPU   MirrorRx     MirrorTx
  00    0x00000003   0x00000004
  01    0x00000003   0x00000004
  02    0x00000003   0x00000004
  03    0x00000003   0x00000004
  04    0x00000003   0x00000004
  05    0x00000003   0x00000004
RP/0/RP0/CPU0:ios#
```

ERSPAN Traffic to a Destination Tunnel in a Non-Default VRF

Table 5: Feature History Table

Feature Name	Release Information	Description
ERSPAN Traffic to a Destination Tunnel in a Non-Default VRF	Release 7.5.3	The tunnels are grouped under the VRFs and you can segregate the traffic towards a specific VRF domain. Encapsulated Remote Switched Port Analyzer (ERSPAN) now transports mirrored traffic through GRE tunnels with multiple VRFs, helping you design your network with multiple Layer 3 partitions. In earlier releases, ERSPAN transported mirrored traffic through GRE tunnels that belonged to only default VRF.

Here, the tunnel interface, where the traffic mirroring is destined, is now in a VRF.

The traffic coming out of the interfaces of a router do not have any grouping. By configuring a specific VRF, you can now identify the incoming traffic group.

Configuration

Use the following command to configure a specific VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 2
RP/0/RP0/CPU0:router(config)# tunnel vrf red
```

For more information on enabling the tunnel mode in GRE, see Configuring GRE Tunnels.

Configuration example

The following example shows a tunnel interface configured with endpoints in a non-default VRF (**vrf: red**):

```
Router#show run int tunnel-ip 2
Thu Feb  3 06:18:28.075 UTC
interface tunnel-ip2
 ipv4 address 102.1.1.100 255.255.255.0
 tunnel tos 32
 tunnel mode gre ipv4
 tunnel source 120.1.1.100
 tunnel vrf red
 tunnel destination 120.1.1.1

Router#show monitor-session status
Thu Feb  3 06:18:11.061 UTC
Monitor-session ERSPAN-2
Destination interface tunnel-ip2
================================================================
```

```
Source Interface      Dir   Status
--------------------- ----  ------------------------------------------------------
Te0/0/0/5 (port)      Rx    Operational
```

Verification

The following CLI output shows how to verify, if the configured tunnel VRF is programmed in the session:

```
Router#show monitor-session ERSPAN-2 status internal
Thu Feb  3 06:19:50.014 UTC

Information from SPAN Manager and MA on all nodes:
Monitor-session ERSPAN-2 (ID 0x00000003) (Ethernet)
SPAN Mgr: Destination interface tunnel-ip2 (0x20008024)
          Last error: Success
          Tunnel data:
            Mode: GREoIPv4
            Source IP: 120.1.1.100
            Dest IP: 120.1.1.1
            VRF: red
            VRF TBL ID: 0
            ToS: 32
            TTL: 255
            DFbit: Not set
```

Configuring Flexible CLI for ERSPAN Sessions

Table 6: Feature History Table

Feature Name	Release Information	Description
Configuring Flexible CLI for ERSPAN Sessions	Release 7.5.4	With this feature, you can define a set of router configurations in a configuration group, thus minimizing the repetitive configurations. You can use this feature to create group ERSPAN configurations and apply it to multiple interfaces. Flexible CLI for ERSPAN sessions helps you improve the efficiency of your network monitoring and analysis, reduces the risk of errors, and ensures compatibility with a wide range of devices and tools. You can create a configuration group and apply it to the interfaces using the **apply-group** *group name* command.

The flexible CLI (FlexCLI) feature allows administrators to simplify complex configurations, and streamline day-to-day operations. The configurations can be saved as part of the device configuration for later use.

FlexCLI Configuration Groups

FlexCLI configuration groups provide the ability to minimize repetitive configurations by defining a series of configuration statements in a configuration group, and then applying this group to multiple hierarchical levels in the router configuration tree.

FlexCLI configuration groups utilize regular expressions that are checked for a match at multiple submodes of the configuration tree based on where the group is applied within the hierarchy. If a match is found at a

configuration submode, the corresponding configuration defined in the group is inherited within the matched submode.

FlexCLI configuration groups also provide an auto-inheritance feature. Auto-inheritance means that any change done to a CLI configuration group is automatically applied to the configuration in any matched submodes that have an apply-group at that hierarchical level. This allows you to make a configuration change or addition once, and have it applied automatically in multiple locations, depending on where you have applied the FlexCLI configuration group.

For more details, see the *System Management Configuration Guide for Cisco NCS 560 Series Routers*.

FlexCLI for ERSPAN Sessions

With FlexCLI, you can create a single configuration containing all the properties of the ERSPAN session, including the GRE tunnel properties and the list of source interfaces, which can be easily removed and re-added. You should pre-configure the `tunnel-ip` and `monitor-session`, and then create the group.

Restrictions

Note the following restrictions when using flexible configuration groups:

- Flexible CLI configuration groups are not supported in administration configurations and corresponding apply-groups are not supported in administration configurations.
- Use of preconfigured interfaces in configuration groups is not supported.
- Downgrading from an image that supports configuration groups to an image that does not support them is not supported.
- Access lists, quality of service and route policy configurations do not support the use of configuration groups. Configurations such as these are not valid:

```
group g-not-supported
 ipv4 access-list ...
 !
 ipv6 access-list ...
 !
 ethernet-service access-list ...
 !
 class-map ...
 !
 policy-map ...
 !
 route-policy ...
 !
end-group
```

You can, however, reference such configurations, as shown in this example:

```
group g-reference-ok
 router bgp 6500
  neighbor 7::7
   remote-as 65000
   bfd fast-detect
   update-source Loopback300
   graceful-restart disable
   address-family ipv6 unicast
       route-policy test1 in
    route-policy test2 out
    soft-reconfiguration inbound always
   !
```

```
 !
!
interface Bundle-Ether1005
  bandwidth 10000000
  mtu 9188
     service-policy output input_1
  load-interval 30
!
end-group
```

Some regular expressions are not supported within groups. For example, '?', '|' and '$,' are not supported within groups. Also some characters such as /d and /w are not supported.

- The choice operator "|" to express multiple match expressions within a regular expression is not supported. For example, these expressions are not supported:

  `Gig.*|Gig.*\..*`—To match on either Gigabit Ethernet main interfaces or Gigabit Ethernet sub-interfaces.

  `Gig.*0/0/0/[1-5]|Gig.*0/0/0/[10-20]`—To match on either Gig.*0/0/0/[1-5] or Gig.*0/0/0/[10-20].

  `'TenGigE.*|HundredGigE.*`—To match on either TenGigE.* or HundredGigE.* .

- Commands that require a node identifier for the **location** keyword are not supported. For example, this configuration is not supported:

```
lpts pifib hardware police location 0/RP0/CPU0
```

- Overlapping regular expressions within a configuration group for the same configuration are not supported. For example:

```
group G-INTERFACE
interface 'gig.*a.*'
  mtu 1500
!
interface 'gig.*e.* '
  mtu 2000
!
end-group

interface gigabitethernet0/0/0/* ---- where * is 0 to 31
  apply-group G-INTERFACE
```

  This configuration is not permitted because it cannot be determined whether the `interface GigabitEthernet0/0/0/*` configuration inherits `mtu 1500` or `mtu 2000`. Both expressions in the configuration group match GigabitEthernet0/0/0/*.

- Up to eight configuration groups are permitted on one apply-group command.

Configuration

A configuration group includes a series of configuration statements that can be used in multiple hierarchical levels in the router configuration tree. By using regular expressions in a configuration group, you can create generic commands that can be applied in multiple instances.

Configuring Flexible CLI group for ERSPAN sessions involves the following steps:

1. Create an ERSPAN session configuration group.

2. Configure the tunnel interface and specify the configuration statements that you want included in this configuration group.
3. Apply the flexible CLI group configuration to the interface.

Before you begin

Add the GRE tunnel configuration and one-liner configuration for the monitor session to be used in FlexCLI.

Step 1 Configure global ERSPAN session using the following sample command.

Specify a name for the configuration group. The group-name argument can have up to 32 characters and cannot contain any special characters.

Example:

```
Router#configure terminal
Tue Mar  8 10:42:43.916 UTC
Router(config)#group ERSPAN-G1
Router(config-GRP)#monitor-session 'foo' ethernet
Router(config-GRP-mon)#destination interface tunnel-ip 1
Router(config-GRP-mon)#exit
```

Step 2 Configure the tunnel interface using the following sample command:

Specify the configuration statements that you want to include in this configuration group.

Example:

```
Router(config-GRP)#interface 'tunnel-ip1'
Router(config-GRP-if)#ipv4 address 100.1.1.100 255.255.255.0
Router(config-GRP-if)# tunnel vrf red
Router(config-GRP-if)# tunnel mode gre ipv4
Router(config-GRP-if)# tunnel source 140.1.1.100
Router(config-GRP-if)# tunnel destination 140.1.1.77
Router(config-GRP-if)#exit
```

Step 3 Specify the interface to which the group configuration should be applied.

Example:

```
Router(config-GRP)# interface '(Bundle-Ether([1-2]))'
  Router(config-GRP-if)# monitor-session foo ethernet direction rx-only port-level
  !
 !
```

Step 4 Apply the group at global configuration level and interface level..

Example:

```
Router(config)#apply-group ERSPAN-G1
Router(config)#end
```

Use the **no apply-group** command to revert the configuration.

Add the configuration of the configuration group into the router configuration applicable at the location that the group is applied. Groups can be applied in multiple locations, and their effect depends on the location and context.

If the group is applied in global configuration mode, the configuration is inherited by all Ethernet interfaces that do not have this specific configuration.

Verifying FlexCLI Group Configuration

The following command shows the contents of a specific or all configured configuration groups. Here, the group name is ERSPAN-G1.

```
Router# show running-config group ERSPAN-G1

 group ERSPAN-G1
 monitor-session 'foo' ethernet
  destination interface tunnel-ip1
 !
 interface 'tunnel-ip1'
  ipv4 address 100.1.1.100 255.255.255.0
  tunnel mode gre ipv4
  tunnel source 140.1.1.100
  tunnel vrf red
  tunnel destination 140.1.1.77
 !
 interface '(Bundle-Ether([1-2]))'
  monitor-session foo ethernet direction rx-only port-level
  !
 !
end-group
```

```
Router#show running-config
Tue Mar  8 10:46:54.975 UTC
Building configuration...
!! IOS XR Configuration 7.3.4.10I
!! Last configuration change at Tue Mar  8 10:46:46 2022 by root
!
hostname Turin-1
group ERSPAN-G1
 monitor-session 'foo' ethernet
  destination interface tunnel-ip1
 !
 interface 'tunnel-ip1'
  ipv4 address 100.1.1.100 255.255.255.0
  tunnel mode gre ipv4
  tunnel source 140.1.1.100
  tunnel vrf red
  tunnel destination 140.1.1.77
 !
 interface '(Bundle-Ether([1-2]))'
  monitor-session foo ethernet direction rx-only port-level
  !
 !
end-group
apply-group ERSPAN-G1
username root
 group root-lr
 group cisco-support
 secret 10
$6$jtRSp0SbLhtJ9p0.$UiV/zm243yCo0ok94KliDLcORPzbS.WcadYdM45ZDFfTH4shNMh1RKLzaulKnXoha4kyVkJkaCUuUb3qCUCa2/
!
vrf red
 address-family ipv4 unicast
 !
```

```
!

monitor-session foo ethernet
!
interface Bundle-Ether1
 vrf red
 ipv4 address 102.1.1.100 255.255.255.0
!
interface Bundle-Ether2
 vrf red
 ipv4 address 105.1.1.100 255.255.255.0
!
interface Loopback10
 ipv4 address 100.100.100.100 255.255.255.255
!
interface tunnel-ip1
 tunnel source 140.1.1.100
 tunnel vrf red
 tunnel destination 140.1.1.77
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 5.16.23.100 255.255.0.0
!
interface TenGigE0/0/0/0
 shutdown
!
```

The following example shows the inherited configuration wherever a configuration group has been applied.

```
Routershow running-config inheritance
Tue Mar  8 10:46:58.605 UTC
Building configuration...
!! IOS XR Configuration 7.3.4.10I
!! Last configuration change at Tue Mar  8 10:46:46 2022 by root
!
hostname Turin-1
group ERSPAN-G1
 monitor-session 'foo' ethernet
  destination interface tunnel-ip1
 !
 interface 'tunnel-ip1'
  ipv4 address 100.1.1.100 255.255.255.0
  tunnel mode gre ipv4
  tunnel source 140.1.1.100
  tunnel vrf red
  tunnel destination 140.1.1.77
 !
 interface '(Bundle-Ether([1-2]))'
  monitor-session foo ethernet direction rx-only port-level
  !
 !
end-group

monitor-session foo ethernet
 destination interface tunnel-ip1
!
.
.
```

SPAN

SPAN over Pseudo-Wire

Pseudo-wire traffic mirroring (known as PW-SPAN) is an extra functionality on the existing SPAN solutions. The existing SPAN solutions are monitored on a destination interface or through a GRE tunnel or RSPAN. In PW-SPAN, the traffic mirroring destination port is configured to be a pseudo-wire rather than a physical port. Here, the designated traffic on the source port is mirrored over the pseudo-wire to a central location. This allows the centralization of expensive network traffic analysis tools.

Because the pseudo-wire carries only mirrored traffic, this traffic is unidirectional. Incoming traffic from the remote provider edge is not allowed. Typically, a monitor session should be created with a destination pseudo-wire. This monitor session is one of the L2VPN xconnect segments. The other segment of the L2VPN VPWS is a pseudowire.

Note Only port-level source interfaces are supported.

Limitations

The following functionalities are not supported for SPAN over PW:

- Monitor session statistics
- RSPAN
- Partial packet SPAN
- Sampled SPAN
- ERSPAN Tunnel statistics
- A destination port cannot be a source port.

Configuring SPAN over Pseudo-Wire

Use the following steps to configure SPAN over Pseudo-Wire:

Configure SPAN monitor session

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#monitor-session M1
RP/0/RP0/CPU0:router(config-mon)#destination pseudowire
RP/0/RP0/CPU0:router(config-mon)#commit
```

Configure SPAN source

```
RP/0/RP0/CPU0:router#config
Fri Sep  6 03:49:59.312 UTC
RP/0/RP0/CPU0:router(config)#interface Bundle-Ether100
RP/0/RP0/CPU0:router(config-if)#monitor-session M1 ethernet port-level
RP/0/RP0/CPU0:router(config-if-mon)#commit
```

Configure l2vpn xconnect

```
RP/0/RP0/CPU0:router(config)#l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#pw-class span
RP/0/RP0/CPU0:router(config-l2vpn-pwc)#encapsulation mpls
RP/0/RP0/CPU0:router(config-l2vpn-pwc-mpls)#transport-mode ethernet
RP/0/RP0/CPU0:router(config-l2vpn)#xconnect group 1
RP/0/RP0/CPU0:router(config-l2vpn-xc)#p2p 2
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)#monitor-session M1
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)#neighbor ipv4 10.10.10.1 pw-id 2
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)#pw-class span
RP/0/RP0/CPU0:router(config-l2vpn-xc-p2p)#commit
```

Verifying SPAN over Pseudo-Wire

The following examples show how to verify SPAN over Pseudo-Wire.

To check monitor session status:

```
RP/0/RP0/CPU0:router#show run monitor-session M1
monitor-session M1 ethernet
 destination pseudowire

RP/0/RP0/CPU0:router#show monitor-session M1 status
Monitor-session M1
Destination pseudowire
Source Interface      Dir   Status
BE100 (port)          Both  Operational
BE400 (port)          Both  Operational

RP/0/RP0/CPU0:router#show monitor-session M1 status detail
Monitor-session M1
  Destination pseudowire
  Source Interfaces
  -----------------
  Bundle-Ether100
    Direction:  Both
    Port level: True
    ACL match:  Disabled
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Operational
  Bundle-Ether400
    Direction:  Both
    Port level: True
    ACL match:  Disabled
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Operational
```

To check underlying l2vpn xconnect:

```
RP/0/RP0/CPU0:router#show run l2vpn
l2vpn
 pw-class span
  encapsulation mpls
   transport-mode ethernet
  !
  !
  p2p 2
   monitor-session M1
   neighbor ipv4 10.10.10.1 pw-id 2
   pw-class span
   !
  !
  p2p 10
```

```
   monitor-session M2
   neighbor ipv4 10.10.10.1 pw-id 10
    pw-class span
   !
  !
 !
!
RP/0/RP0/CPU0:router#show l2vpn xconnect
Fri Sep  6 03:41:15.691 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                   Segment 1                       Segment 2
Group      Name       ST   Description            ST       Description             ST
------------------------   ----------------------------   ------------------------------
1          2          UP   M1                     UP       10.10.10.1         2      UP

------------------------------------------------------------------------------------------
1          10         UP   M2                     UP       10.10.10.1         10     UP

------------------------------------------------------------------------------------------
```

Traffic Mirroring of Incoming and Outgoing Traffic Separately over Pseudowire

Table 7: Feature History Table

Feature Name	Release	Description
Traffic Mirroring of Incoming and Outgoing Traffic Separately over Pseudowire	Release 7.11.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] You can now distribute the monitoring load by separating the Rx and Tx traffic mirroring over the pseudowire. Earlier, you could mirror the entire traffic without distinguishing between Rx and Tx directions. The separation of traffic direction gives the flexibility of monitoring and analyzing the nature of data being sent and received using independent network traffic analysis tools. The separation also helps in distributing the monitoring load and eases troubleshooting. The feature modifies the **monitor-session** command. The keywords **destination rx** and **destination tx** of the command are extended to monitor session configuration mode. Earlier, this configuration resulted in verification failure.

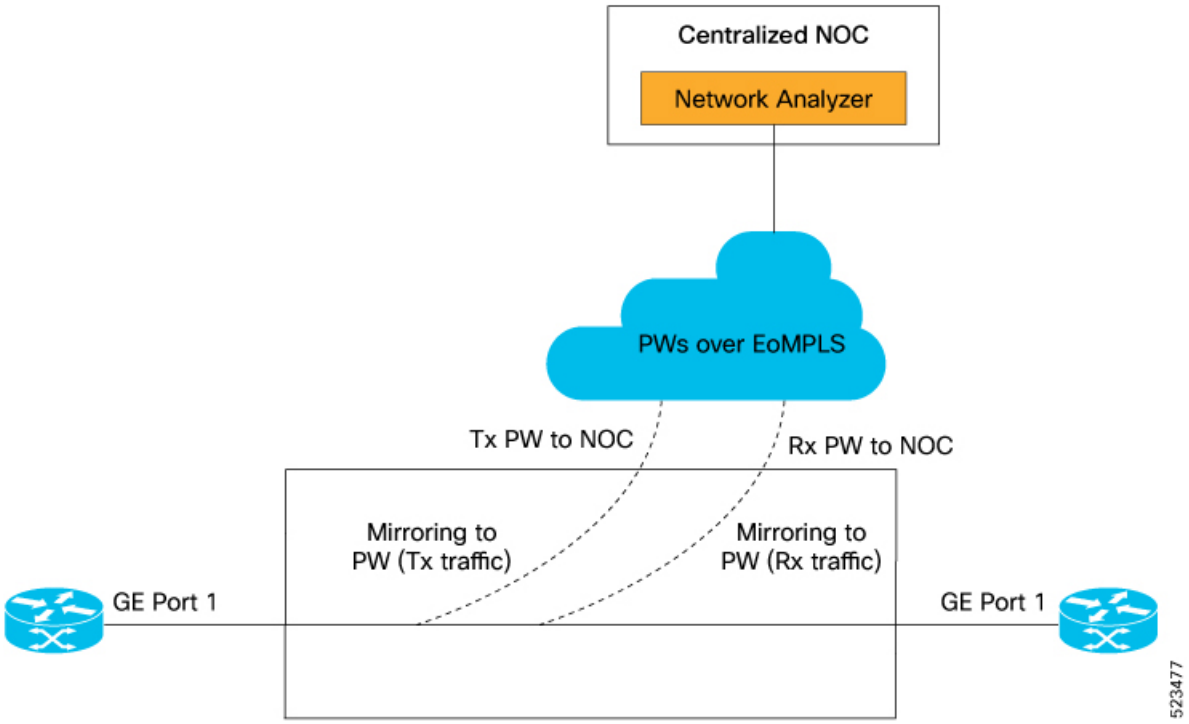
Pseudowire Traffic Mirroring also known as PW-SPAN involves replicating designated traffic from the source port to a central location through the pseudowire. The transmission within the pseudowire follows a unidirectional flow, originating from the source port and terminating at the destination network analyzer. Previously, you could not send Rx and Tx mirrored traffic to separate Rx and Tx PW-SPAN destinations. The entire traffic is mirrored to the destination through pseudowire, which is less effective in monitoring and troubleshooting network issues. Resource allocation of monitoring tools is also not optimized, especially when the monitoring requirement for one direction is different from the other direction.

This feature allows separate Rx and Tx mirror destinations within a single session to optimize resource allocation when the monitoring requirement for one direction is different from the other direction.

Topology

Using this topology, let's understand how incoming and outgoing traffic are mirrored separately over pseudowire.

Figure 3: Mirroring Topology



- This topology uses pseudowires provisioned over EoMPLS.
- Two pseudowires, Rx PW and Tx PW, mirror incoming (Rx) and outgoing (Tx) traffic separately to a centralized Network Operations Center (NOC).
- The network analyzer hosted in the NOC receives the separately mirrored traffic for analysis.

You can provision pseudowires using L2VPN point-to-point cross-connect. The SPAN session supports configuring the session ID and traffic direction to allow multiple mirror destinations within the same SPAN session. After you configure traffic mirroring, traffic is duplicated from the selected pseudowires to the specified destination port without affecting the normal traffic forwarding in the network.

The destination port or monitoring tool captures mirrored traffic from the specified pseudowires, facilitating pseudowire traffic monitoring, analysis, and troubleshooting. The segregation of Rx and Tx monitoring enhances the ability to identify and isolate differences or performance problems. By identifying the root cause network problems can be resolved with greater efficiency and effectiveness.

Configure Traffic Mirroring of Incoming and Outgoing Traffic Separately over Pseudowire

Perform the following tasks to configure Rx and Tx pseudowire destinations:

- Create a pseudowire monitor session to replicate Ethernet traffic.
- Configure the destination for Rx and Tx traffic.
- Create an L2VPN cross-connect corresponding to the monitor session and define point-to-point forwarding details for Rx and Tx.
- Define bundle-ether interfaces for Rx and Tx directions.

```
Router(config)#monitor-session pw-span2 ethernet
Router(config-mon)#destination rx pseudowire
Router(config-mon)#destination tx pseudowire
Router(config-mon)#exit

Router(config)#l2vpn
Router(config-l2vpn)#xconnect group pw-span2
Router(config-l2vpn-xc)#p2p rx2
Router(config-l2vpn-xc-p2p)#monitor-session pw-span2 rx
Router(config-l2vpn-xc-p2p)#neighbor ipv4 100.2.1.11 pw-id 21
Router(config-l2vpn-xc-p2p-pw)#mpls static label local 1421 remote 1521
Router(config-l2vpn-xc-p2p-pw)#pw-class pw
Router(config-l2vpn-xc-p2p-pw)#exit
Router(config-l2vpn-xc-p2p)#exit
Router(config-l2vpn-xc)#p2p tx2
Router(config-l2vpn-xc-p2p)#monitor-session pw-span2 tx
Router(config-l2vpn-xc-p2p)#neighbor ipv4 100.1.1.22 pw-id 22
Router(config-l2vpn-xc-p2p-pw)#mpls static label local 1422 remote 1522
Router(config-l2vpn-xc-p2p-pw)#pw-class pw
Router(config-l2vpn-xc-p2p-pw)#exit
Router(config-l2vpn-xc-p2p)#exit
Router(config-l2vpn-xc)#exit
Router(config-l2vpn)#exit

Router(config)#interface Bundle-Ether1
Router(config-if)#ipv4 address 20.1.1.1 255.255.255.252
Router(config-if)#ipv6 address abc::20:1:1:1/126
Router(config-if)#lacp mode active
Router(config-if)#lacp period short

Router(config-if)#monitor-session pw-span2
Router(config-if-mon)#exit
Router(config-if)#exit

Router(config)#interface Bundle-Ether101
Router(config-if)#ipv4 address 20.1.4.1 255.255.255.252
Router(config-if)#ipv6 address abc::20:1:4:1/126
Router(config-if)#lacp mode active
Router(config-if)#lacp period short

Router(config-if)#monitor-session pw-span2
Router(config-if-mon)#exit
Router(config-if)#exit
Router(config-if)#load-interval 30
Router(config)#exit
```

Running Configuration

The following example shows the running configuration.

```
Router#sh run monitor-session pw-span2
Wed Sep 23 11:06:28.607 UTC
monitor-session pw-span2 ethernet
 destination rx pseudowire
 destination tx pseudowire
!

Router#sh run l2vpn xconnect group pw-span2
!l2vpn
l2vpn
 xconnect group pw-span2
  p2p rx2
   monitor-session pw-span2 rx
   neighbor ipv4 100.2.1.11 pw-id 21
    mpls static label local 1421 remote 1521
```

```
    pw-class pw
   !
  !
  p2p tx2
   monitor-session pw-span2 tx
   neighbor ipv4 100.1.1.22 pw-id 22
    mpls static label local 1422 remote 1522
    pw-class pw
   !
  !
 !
!

Router#sh run interface bundle-ether 1
interface Bundle-Ether1
 ipv4 address 20.1.1.1 255.255.255.252
 ipv6 address abc::20:1:1:1/126
 lacp mode active
 lacp period short
 monitor-session pw-span2
 !
!

Router#sh run interface bundle-ether 101
interface Bundle-Ether101
 ipv4 address 20.1.4.1 255.255.255.252
 ipv6 address abc::20:1:4:1/126
 lacp mode active
 lacp period short
 monitor-session pw-span2
 !
 load-interval 30
!
```

Verification

Verify that both Rx and Tx traffic is operational.

```
show monitor-session status
Monitor-session pw-span2
rx destination pseudowire
tx destination pseudowire
================================================================================
Source Interface      Dir   Status
--------------------- ----  ------------------------------------------------
BE1                   both    Operational
BE101                 both    Operational
```

SPAN to File

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
SPAN Mirror First	Release 7.5.2	With your knowledge of expected packet header size, you can now mirror only the first N bytes of a packet where N can have possible values from 1 through 10000. This allows only the packet headers to be mirrored and not the user payload, ensuring the privacy and security of user data. It also reduces the load on network resources by processing only a few bytes to identify issues in the network. With the introduction of this feature, you can use the `mirror first` option in the global configuration mode of the `monitor-session` command.
SPAN to File - PCAPng File Format	Release 7.3.1	PCAPng is the next generation of packet capture format that contains a dump of data packets captured over a network and stored in a standard format. The PCAPng file contains different types of information blocks, such as the section header, interface description, enhanced packet, simple packet, name resolution, and interface statistics. These blocks can be used to rebuild the captured packets into recognizable data. The PCAPng file format: • Provides the capability to enhance and extend the existing capabilities of data storage over time • Allows you to merge or append data to an existing file. • Enables to read data independently from network, hardware, and operating system of the machine that made the capture.

SPAN to File is an extension of the pre-existing SPAN feature that allows network packets to be mirrored to a file instead of an interface. This helps in the analysis of the packets at a later stage. The file format is PCAP, which helps that data to be used by tools, such as tcpdump or Wireshark.

SPAN to File feature:

- A maximum of 1000 source ports are supported across the system. Individual platforms may support lower numbers. The SPAN session may be any of these currently supported classes: Ethernet, IPv4, IPv6, MPLS-IPv4, and MPLS-IPv6.
- Provides a buffer range of 1000-1000000 KB. The default buffer size is set to 1000 KB.
- Provides support for SPAN source.
  - Each source port can be monitored in only one traffic mirroring session.
  - Each source port can be configured with a direction (ingress, egress, or both) to monitor local traffic mirroring.
- Only supported on the Cisco NCS550x and Cisco NCS55Ax line cards.

When a file is configured as a destination for a SPAN session, a buffer is created on each node to which the network packets are logged. The buffer is for all packets on the node regardless of which interface they are from, that is, multiple interfaces may be providing packets for the same buffer. The buffers are deleted when the session configuration is removed. The file is written by each node to a location on the active RP which contains the node ID of the node on which the buffer was located.

If multiple interfaces are attached to a session, then interfaces on the same node are expected to have their packets sent to the same file. Bundle interfaces can be attached to a session with a file destination, which is similar to attaching individual interfaces.

Limitations

SPAN to File has the following limitations:

- Supports only port-level
- VLAN interface as source port is not supported
- Bundle members as source interfaces are not supported
- Filtering based on Egress ACL is not supported
- Source port statistics is not supported
- Not supported on Cisco NC57 line cards.

Action Commands for SPAN to File

Action commands are added to start and stop network packet collection. The commands may only be run on sessions where the destination is a file. The action command auto-completes names of globally configured SPAN to File sessions. See the table below for more information on action commands.

Table 9: Action Commands for SPAN to File

Action	Command	Description
Start	`monitor-session <name> packet-collection start`	Issue this command to start writing packets for the specified session to the configured buffer. Once the span is configured and operational, the packets are punted to CPU and dropped by CPU until the `monitor-session <name> packet-collection start` command is executed.

Action	Command	Description
Stop	`monitor-session <name> packet-collection stop [ discard-data | write directory <dir> filename <filename> ]`	Issue this command to stop writing packets to the configured buffer. If the `discard-data` option is specified, the buffer is simply cleared, whereas if the `write` option is specified, the buffer is written to disk before clearing. If the buffer is to be written, it is done so in .pcap format to this location: `/<directory>/<node_id>/<filename>.pcap`. If the user adds a .pcap extension when specifying the filename, this is removed so that the extension is not added twice.

Configuring SPAN to File

Use the following command to configure SPAN to File:

```
monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]
    destination file [size <kbytes>] [buffer-type linear]
```

The `monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]` part of the command creates a monitor-session with the specified name and class and is a pre-existing chain point from the current SPAN feature. The `destination file [size <kbytes>] [buffer-type linear]` part of the command adds a new "file" option to the existing "destination".

`destination file` has the following configuration options:

- Buffer size.
- Two types of buffer:
  - Circular: Once the buffer is full, the start is overwritten.
  - Linear: Once the buffer is full, no further packets are logged.

Note The default buffer-type is circular. Only linear buffer is explicitly configurable. Changing any of the parameters (buffer size or type) recreates the session, and clears any buffers of packets.

All configuration options which are applied to an attachment currently supported for other SPAN types should also be supported by SPAN to file. This may include:

- ACLs
- Write only first X bytes of packet.
- Mirror interval from 512 to 16k.

Note These options are implemented by the platform when punting the packet.

Once a session has been created, then interfaces may be attached to it using the following configuration:

```
interface GigabitEthernet 0/0/0/0
    monitor-session <name> [ethernet|ipv4|ipv6|mpls-ipv4|mpls-ipv6]
```

The attachment configuration is unchanged by SPAN to File feature.

Configuration Examples

To configure a `mon1` monitor session, use the following commands:

```
monitor-session mon1 ethernet
          destination file size 230000
         !
```

In the above example, omitting the `buffer-type` option results in default circular buffer.

To configure a `mon2` monitor session, use the following commands:

```
monitor-session mon2 ethernet
          destination file size 1000 buffer-type linear
         !
```

To attach monitor session to a physical or bundle interface, use the following commands:

```
interface Bundle-Ether1
monitor-session ms7 ethernet
!
```

To configure a `mon3` monitor session with the mirror first option, use the following command:

```
monitor-session mon3 ethernet
mirror first 101
!
```

Running Configuration

```
!! IOS XR Configuration 7.1.1.124I
!! Last configuration change at Tue Nov 26 19:29:05 2019 by root
!
hostname OC
logging console informational
!
monitor-session mon1 ethernet
 destination file size 230000 buffer-type circular
!
monitor-session mon2 ethernet
 destination file size 1000 buffer-type linear

!
interface Bundle-Ether1
monitor-session ms7 ethernet
end
```

Verification

To verify packet collection status:

```
RP/0/RP0/CPU0:router#show monitor-session status
Monitor-session mon1
Destination File - Packet collecting
=============================================
Source Interface      Dir   Status
--------------------- ----  ------------------
Hu0/9/0/2             Rx    Operational

Monitor-session mon2
```

```
Destination File - Packet collecting
=======================================
Source Interface      Dir   Status
--------------------- ----  --------------
BE2.1                 Rx    Operational
```

If packet collection is not active, the following line is displayed:

```
Monitor-session mon2
Destination File - Not collecting
```

Packet Capturing Using 7-Tuples ACL

Table 10: Feature History Table

Feature Name	Release Information	Description
Packet Capturing Using 7-Tuples ACL	Release 7.5.4	With this release, you can perform packet capturing with 7-tuple access control lists (ACL). This capability allows you to define seven specific attributes in the ACL and apply it to an interface using the **monitor-session** command. The 7-tuple parameters include source and destination IP addresses, source and destination port numbers, and so on. When the 7-tuples are configured in the ACL, only the matching packets are captured and mirrored. The administrators can examine the captured packets and identify issues such as network congestion and security threats. This analysis helps in diagnosing and resolving network problems, enhancing network performance, and ensuring robust security measures.

Packet capturing functionality enables the network administrators to capture and analyze packets that pass through a router. By defining the seven parameters in the ACL, known as the 7-tuples, data packets can be matched and captured. Only packets that satisfy any or all of the seven parameters are mirrored. The captured packets can be analyzed locally or can be saved and exported for offline analysis.

The following parameters can be included in a 7-tuple ACL:

- Source IP Address (`source ip prefix`)
- Destination IP Address (`dest ip prefx`)
- Protocol (`protocol`, for example, TCP, UDP)
- Differentiated services code point `DSCP`
- Source Port (`source port`)
- Destination Port (dest port)
- Multiple TCP flags

By leveraging this level of granularity, you can fine-tune the packet capturing process to focus on the data relevant to your monitoring objectives.

Configuration Example

You can define the ACL with the seven tuples and apply it to the interface. Use the following sample configuration:

```
Router#configure
Router(config)#monitor-session FOO ethernet
Router(config-mon)#destination interface TenGigE0/6/0/4/1
Router(config-mon)#exit
/* SPAN Source Interface */
Router(config)#interface TenGigE0/6/0/9/2
Router(config-if)#ipv4 address 10.0.0.6 255.0.0.0
Router(config-if)#monitor-session FOO ethernet 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
Router(config-if)#exit
/* SPAN Destination Interface */
Router(config)#interface TenGigE0/6/0/4/1
Router(config-if)#ipv4 address 10.0.0.7 255.0.0.0
```

The following example shows ERSPAN with QoS Configuration:

```
Router#configure
/* GRE Tunnel Interface */
Router(config)#interface Loopback49
Router(config-if)#ipv4 address 172.16.0.1 255.240.0.0
Router(config-if)#exit
Router(config)#interface tunnel-ip100
Router(config-if)#ipv4 address 192.168.0.1 255.255.0.0
Router(config-if)#tunnel mode gre ipv4
Router(config-if)#tunnel source 49.49.49.49
Router(config-if)#tunnel destination 10.0.0.2
Router(config-if)#exit
/* ERSPAN Monitor Session with GRE tunnel as the Destination Interface, and with QoS
configuration */
Router(config)#monitor-session FOO ethernet
Router(config-mon)#destination interface tunnel-ip100
Router(config-mon)#traffic-class 5
Router(config-mon)#discard-class 1
Router(config-mon)#exit
/* ERSPAN Source Interface */
Router(config)#interface TenGigE0/6/0/4/0
Router(config-if)#description connected to TGEN 9/5
Router(config-if)#ipv4 address 10.0.0.1 255.0.0.0
Router(config-if)#monitor-session FOO ethernet 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
Router(config-if)#exit
/* ERSPAN Destination ip-tunnel00’s underlying interface, with egress policy-map shape-foo
 attached */
Router(config)#interface TenGigE0/6/0/9/0
Router(config-if)#service-policy output shape-foo
Router(config-if)#ipv4 address 10.0.0.3 255.0.0.0
Router(config-if)#commit
```

Verification

Use **show monitor-session status** command to get the details of the monitor session.

```
Router# show monitor-session status
```

Displays information about the monitor session.

Traffic Mirroring with DSCP

Differentiated Service Code Point (DSCP) value of Differentiated Services (DS) field in IP packet is used to classify the traffic in the network. DS field formerly known as Type of Service (ToS).You can set the DSCP value in the six most significant bits of the differentiated services (DS) field of the IP header, thereby giving 2^6 = 64 different values (0 to 63). These six bits affect the Per Hop Behavior (PHB) and hence affects how a packet is moved forward. The default value of DSCP is zero (0). DSCP was defined under RFC 2474.

Following the principle of traffic classification, DSCP places a particular packet into a limited number of traffic classes. Similarly, the router is also informed about the DSCP values and the router can prioritize thepacket in traffic flow.

Refer the table to know more about the service class names defined in RFC 2474.

Table 11: 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	Broadcastvideo
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-timeinteractive
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	Networkrouting control
56	111 000	0x38	CS7	224	“reserved”

DSCP Marking on Egress GRE Tunnel in ERSPAN

Table 12: Feature History Table

Feature Name	Release Information	Feature Description
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.

Starting Release 7.5.4, you can set or modify DSCP marking on ERSPAN GRE tunnels. ERSPAN uses GRE encapsulation to route SPAN capture traffic.

Restriction

ERSPAN sessions are not possible on sub-interfaces. You need physical interfaces.

Configure DSCP Marking on Egress GRE Tunnel in ERSPAN

Configuration Example

This example shows how you can configure DSCP Marking on Egress GRE tunnel in ERSPAN.

```
Router#configure terminal
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
```

Note You can configure DSCP value on both IPv4 and IPv6 headers.

Running Configuration

```
interface tunnel-ip1
 tunnel tos 96
 tunnel mode gre ipv4
 tunnel source 192.0.2.1
 tunnel destination 192.0.2.254
!
```

Verification

You can use the following commands to verify that tos value is configured:

```
Router#show run interface tunnel-ip 1
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
```

DSCP Bitmask to Filter Ingress SPAN Traffic

Table 13: Feature History Table

Feature Name	Release Information	Feature Description
DSCP Bitmask to Filter Ingress SPAN 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 SPAN. 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 IP header. This feature introduces the following changes: • **CLI:** 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).

Starting Release 7.5.4, You can configure an ACL rule with DSCP bitmask on the SPAN to mirror specific traffic flows.

Without ACL rule, SPAN mirrors all the traffic on the incoming port. When ACL is configured with DSCP and DSCP mask on the SPAN, SPAN mirrors the traffic whose DSCP value lies within the combination of DSCP value and the specified mask.

A DSCP value is mapped to a single traffic class as per the defined value in RFC2474. Masking the DSCP value in ACL rule allows to mirror multiple traffic flows. DSCP value and mask operate similar to IPv4 address and mask.

Configure DSCP Bitmask to Filter Ingress SPAN Traffic

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

Configuration Example for IPv4

This example shows how you can configure DSCP bitmask on ingress SPAN for IPv4 traffic.

```
/*configure the ACL*/
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

/* Perform the following configurations to attach the created ACL to an interface*/
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0

/* Monitor the ingress ACL applied and DSCP masked IPv4 traffic on SPAN*/
```

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

Running Configuration

```
Router(config)# show running-config ipv4 access-list
ipv4 access-list acl1
 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
!

interface HundredGigE0/0/0/6
 ipv4 address 192.0.2.51 255.255.255.0
 monitor-session TEST ethernet direction rx-only port-level  acl ipv4 acl1
!
!
```

Configuration Example for IPv6

This example shows how you can configure DSCP bitmask on ingress SPAN for IPv6 traffic.

```
/*configure the ACL*/
Router# config
Router(config)# ipv6 access-list acl1
Router(config-ipv6-acl)# 10 permit ipv6 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit

/* Perform the following configurations to attach the created ACL to an interface*/
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32

/* Monitor the ingress ACL applied and DSCP masked IPv4 traffic on ERPSAN*/
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
Router(config-if)# commit
```

Running Configuration

```
Router(config)# show running-config ipv6 access-list
ipv6 access-list acl1
 10 permit ipv6 acl1 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
!
interface HundredGigE0/0/10/3
 ipv6 address 2001:db8::1/32
 monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
!
!
```

File Mirroring

Prior to Cisco IOS XR Software Release 7.2.1, the router did not support file mirroring from active RP to standby RP. Administrators had to manually perform the task or use EEM scripts to sync files across active RP and standby RP. Starting with Cisco IOS XR Software Release 7.2.1, file mirroring feature enables the router to copy files or directories automatically from `/harddisk:/mirror` location in active RP to `/harddisk:/mirror` location in standby RP or RSP without user intervention or EEM scripts.

Two new CLIs have been introduced for the file mirroring feature:

- **mirror enable**

The `/harddisk:/mirror` directory is created by default, but file mirroring functionality is only enabled by executing the `mirror enable` command from configuration terminal. Status of the mirrored files can be viewed with `show mirror status` command.

- **`mirror enable checksum`**

  The `mirror enable checksum` command enables MD5 checksum across active to standby RP to check integrity of the files. This command is optional.

Limitations

The following limitations apply to file mirroring:

- Supported only on Dual RP systems.
- Supports syncing only from active to standby RP. If files are copied into standby `/harddisk:/mirror` location, it won't be synced to active RP.
- A slight delay is observed in `show mirror` command output when mirror checksum configuration is enabled.
- Not supported on multichassis systems.

Configure File Mirroring

File mirroring has to be enabled explicitly on the router. It is not enabled by default.

```
RP/0/RSP0/CPU0:router#show run mirror

Thu Jun 25 10:12:17.303 UTC
mirror enable
mirror checksum
```

Following is an example of copying running configuration to `harddisk:/mirror` location:

```
RP/0/RSP0/CPU0:router#copy running-config harddisk:/mirror/run_config
Wed Jul  8 10:25:51.064 PDT
Destination file name (control-c to abort): [/mirror/run_config]?
Building configuration..
32691 lines built in 2 seconds (16345)lines/sec
[OK]
```

Verification

To verify the syncing of file copied to mirror directory, use the `show mirror` command.

```
RP/0/RSP0/CPU0:router#show mirror
Wed Jul  8 10:31:21.644 PDT
% Mirror rsync is using checksum, this show command may take several minutes if you have
many files. Use Ctrl+C to abort
MIRROR DIR: /harddisk:/mirror/
% Last sync of this dir ended at Wed Jul  8 10:31:11 2020
Location   |Mirrored |MD5 Checksum                      |Modification Time
-------------------------------------------------------------------------
run_config |yes      |76fc1b906bec4fe08ecda0c93f6c7815 |Wed Jul  8 10:25:56 2020
```

If checksum is disabled, `show mirror` command displays the following output:

```
RP/0/RSP0/CPU0:router#show mirror
Wed Jul 8 10:39:09.646 PDT
```

```
MIRROR DIR: /harddisk:/mirror/
% Last sync of this dir ended at Wed Jul  8 10:31:11 2020
Location   |Mirrored |Modification Time
-----------------------------------------
run_config |yes         |Wed Jul  8 10:25:56 2020
```

If there is a mismatch during the syncing process, use `show mirror mismatch` command to verify.

```
RP/0/RP0/CPU0:router# show mirror mismatch
Wed Jul  8 10:31:21.644 PDT
 MIRROR DIR: /harddisk:/mirror/
 % Last sync of this dir ended at Wed Jul  8 10:31:11 2020
 Location  |Mismatch Reason     |Action Needed
-----------------------------------------------
 test.txt  |newly created item. |send to standby
```

Mirroring Forward-Drop Packets

Table 14: Feature History Table

Feature Name	Release Information	Description
Mirroring Forward-Drop Packets	Release 7.5.4	Mirroring forward-drop packets feature copies or mirrors the packets that are dropped during the forwarding process at the router ingress to a configured destination. These mirrored packets can be captured and analyzed using network monitoring tools. The analysis of dropped packets helps you understand the types of traffic that are blocked, analyze potential security threats, troubleshoot, and optimize network performance. This feature introduces the following changes: • **CLI: forward-drop rx** • **YANG Data Model:**New XPath for Cisco-IOS-XR-um-monitor-session-cfg.yang (see GitHub, YANG Data Models Navigator)

In a network, packets are forwarded from one device to another until they reach their destination. However, in some cases, routers may drop packets during this forwarding process. These packets are known as forward-drop packets.

The packet drop can happen for several reasons, such as congestion on the network, errors in the packet header or payload, blocking by firewall or access control lists (ACL), and so on. These forward-drop packets are typically discarded before they can reach their intended destination, and may have to be re-transmitted by the source device. This feature supports mirroring of these forward-drop packets at the ingress (Rx direction) to another destination. When a global forward-drop session is configured for the router, the forward-drop packets at the ingress are mirrored or copied to the configured destination. You can configure the mirror destination as a file (for SPAN-to-file sessions) or an IPv4 GRE tunnel ID (for ERSPAN).

Mirroring forward-drop packets to a suitable destination for analysis can help in the following:

- Network visibility: By mirroring and analyzing forward-drop packets, network administrators gain better visibility into the types of traffic that are blocked by the firewalls and access control lists (ACL).

- Threat detection: As the original dropped packet is forwarded without any change, it helps in identifying the source of potential security threats.
- Troubleshooting: Analyzing forward-drop packets helps in troubleshooting network issues that may be causing the packet drop. This helps in taking proactive measures to avoid escalation of the issue.

Guidelines and Restrictions

- Only one global forward-drop session can be configured on a router.
- When traffic-class is configured under monitor-session for forward-drop, the type of service (ToS) byte of the outgoing ERSPAN packet is overwritten with the configured traffic-class value.
- In-band traffic destined to router management interface cannot be captured using this functionality.

Configuring Forward-Drop

Perform the following tasks on the router to configure a global session for mirroring forward-drop packets:

1. Configure the tunnel mode.
2. Configure the tunnel source.
3. Configure the tunnel destination.
4. Configure a traffic mirroring session.
5. Associate a destination interface with the traffic mirroring session.
6. Run **forward-drop rx** command to start mirroring forward-drop packets.

This example shows how to configure a global traffic mirroring session for forward-drop packets.

```
Router(config)# interface tunnel-ip 2
Router(config-if)# tunnel mode gre ipv4
Router(config-if)# tunnel source 20.20.20.20
Router(config-if)# tunnel destination 192.1.1.3
Router(config-if)!
Router(config)# monitor-session mon2 ethernet
Router(config)#destination interface tunnel-ip2
Router(config)#forward-drop rx
Router(config)#!
```

Running Configuration

This section shows forward-drop running configuration.

```
RP/0/RSP0/CPU0:router#sh running-config
interface tunnel-ip 2
tunnel mode gre ipv4
tunnel source 20.20.20.20
tunnel destination 192.1.1.3
!
monitor-session mon2 ethernet
destination interface tunnel-ip2
forward-drop rx
!
```

Verification

Verify the forward-drop packets are mirrored using the **show monitor-session** command.

```
Router#show monitor-session mon2 status detail
Mon Aug 15 19:14:31.975 UTC
Monitor-session mon2
   Destination interface tunnel-ip2
   All forwarding drops:
      Direction: Rx
Source Interfaces
-----------------
```

Troubleshooting Traffic Mirroring

When you encounter any issue with traffic mirroring, begin troubleshooting by checking the output of the **show monitor-session status** command. This command displays the recorded state of all sessions and source interfaces:

```
# show monitor-session status
Monitor-session 5
rx destination interface tunnel-ip5
tx destination is not specified
================================================================================
Source Interface  Dir  Status
--------------------- ---- --------------------------------------------------
Te0/0/0/23 (port) Rx   Operational
```

In the preceding example, the line marked as `<Session status>` can indicate one of these configuration errors:

Session Status	Explanation
Session is not configured globally	The session does not exist in global configuration. Review the command output and ensure that a session with a correct name configured.
Destination interface <intf> (<down-state>)	The destination interface is not in Up state in the Interface Mar can verify the state using the **show interfaces** command. Chec configuration to determine what might be keeping the interface fr up (for example, a sub-interface needs to have an appropriate enc configured).

The <Source interface status> can report these messages:

Source Interface Status	Explanation
Operational	Everything appears to be working correctly in traffic mirroring follow up with the platform teams in the first instance, if mirro operating as expected.
Not operational (Session is not configured globally)	The session does not exist in global configuration. Check the s command output to ensure that a session with the right name ha configured.

Source Interface Status	Explanation
Not operational (destination not known)	The session exists, but it either does not have a destination interface s or the destination interface named for the session does not exist. For e if the destination is a sub-interface that has not been created.
Not operational (source same as destination)	The session exists, but the destination and source are the same inte traffic mirroring does not work.
Not operational (destination not active)	The destination interface or pseudowire is not in the Up state. See corresponding *Session status* error messages for suggested resoluti
Not operational (source state <down-state>)	The source interface is not in the Up state. You can verify the state the **show interfaces** command. Check the configuration to see wha be keeping the interface from coming up (for example, a sub-interfa to have an appropriate encapsulation configured).
Error: see detailed output for explanation	Traffic mirroring has encountered an error. Run the **show monitor status detail** command to display more information.

The **show monitor-session status detail** command displays full details of the configuration parameters and any errors encountered. For example:

RP/0/RP0/CPU0:router **show monitor-session status detail**

```
Monitor-session sess1
 Destination interface is not configured
 Source Interfaces
 -----------------
 TenGigE0/0/0/1
  Direction: Both
  ACL match: Disabled
  Portion:  Full packet
  Status:  Not operational (destination interface not known)
 TenGigE0/0/0/2
  Direction: Both
  ACL match: Disabled
  Portion:  First 100 bytes
  Status: Not operational (destination interface not known). Error: 'Viking SPAN PD' detected
 the 'warning' condition 'PRM connection
          creation failure'.
Monitor-session foo
 Destination next-hop TenGigE 0/0/0/0
 Source Interfaces
 -----------------
 TenGigE 0/1/0/0.100:
  Direction: Both
  Status:  Operating
 TenGigE 0/2/0/0.200:
  Direction: Tx
  Status:  Error: <blah>

Monitor session bar
 No destination configured
 Source Interfaces
 -----------------
 TenGigE 0/3/0/0.100:
  Direction: Rx
```

```
  Status:  Not operational(no destination)
```

Here are additional trace and debug commands:

```
RP/0/RP0/CPU0:router# show monitor-session platform trace ?

 all   Turn on all the trace
 errors Display errors
 events Display interesting events

RP/0/RP0/CPU0:router# show monitor-session trace ?

 process Filter debug by process

RP/0/RP0/CPU0:router# debug monitor-session platform ?

 all   Turn on all the debugs
 errors VKG SPAN EA errors
 event  VKG SPAN EA event
 info  VKG SPAN EA info

RP/0/RP0/CPU0:router# debug monitor-session process all

RP/0/RP0/CPU0:router# debug monitor-session process ea

RP/0/RP0/CPU0:router# debug monitor-session process ma

RP/0/RP0/CPU0:router# show monitor-session process mgr

 detail  Display detailed output
 errors  Display only attachments which have errors
 internal Display internal monitor-session information
 |     Output Modifiers

RP/0/RP0/CPU0:router# show monitor-session status

RP/0/RP0/CPU0:router# show monitor-session status errors

RP/0/RP0/CPU0:router# show monitor-session status internal
```