ACL-based traffic mirroring

This chapter introduces ACL-based traffic mirroring, a feature for selectively monitoring network traffic by using ACL configurations. It covers benefits like improved security and efficient resource use, details configuration guidelines and restrictions, and provides step-by-step procedures for setting up IPv4, IPv6, and Layer 3 ACLs.

ACL-based traffic mirroring

ACL-based traffic mirroring is a feature that allows you to:

- mirror traffic based on the configuration of the global interface ACL, and
- monitor particular types of traffic that match certain characteristics, such as source or destination IP addresses, protocols, or port numbers.

Benefits of ACL-based traffic mirroring

- Selective monitoring: Allows you to focus on specific traffic flows that are of interest, thereby reducing the amount of data that needs to be processed and analyzed.
- Improved security: Enables the monitoring of suspicious or critical traffic patterns, helping to detect and respond to potential security threats more effectively.
- Efficient resource usage: Mirrors only selected traffic and uses network resources such as bandwidth and processing power more efficiently, avoiding the overhead of capturing all traffic.

Configuration guidelines for ACL-based traffic mirroring

These configuration guidelines apply to ACL-based traffic mirroring:

Traffic mirroring on source interface

- Configure ACLs on the source interface to avoid default mirroring of traffic.
- Configure the ACLs on the bundle interface and not on bundle members, if a bundle interface is a source interface.

Restrictions for ACL-based traffic mirroring

These restrictions apply to ACL-based traffic mirroring:

- You must remove and re-apply monitor-sessions on all interfaces after modifying the access control list (ACL).
- SPAN ACL does not support User Defined Fields (UDF).
- Deny action in SPAN ACL is ignored, and no packet drops from SPAN ACL. Deny ACEs will be internally converted to permit ACEs. Packets will also be mirrored.
- There is no implicit deny-all entry in SPAN ACL.
- IPV6 ACL is required for mirroring IPv6 packets and IPv4 ACL is required for IPv4 packets. This follows the same structure as security ACL with IPv4 and IPv6 mirror options.

How ACL-based traffic mirroring works

These stages describe how ACL-based traffic mirroring works.

1. The router creates an ACL.
2. This ACL defines the traffic to be mirrored and specifies the packets to be mirrored.
3. The keywords defined in the ACL designates that the packet is mirrored to the destination port.
4. The rules defined in the ACL determine the behavior for traffic.

When the system..	But..	Then..
configures the **acl** command on the source mirroring port	the ACL configuration command does not use the **capture** keyword	the router does not mirror the traffic.
uses ACL configuration with the **capture** keyword	you have not configured the **acl** command on the source port	the router mirrors the traffic, but does not apply access list configuration.

Configure ACLs for traffic mirroring

Use this procedure to configure IPv4 or IPv6 ACLs for traffic mirroring.

Procedure

Step 1 Create SPAN IPv4 ACL for traffic mirroring.

Example:

```
Router(config)# ipv4 access-list v4-monitor-acl
Router(config-ipv4-acl)# 10 permit udp 20.1.1.0 0.0.0.255 eq 10 any
Router(config-ipv4-acl)# 20 permit udp 30.1.1.0 0.0.0.255 eq 20 any
Router(config-ipv4-acl)# exit
Router(config)# commit
```

The router creates an ACL named **v4-monitor-acl** and applies the **permit** action for the traffic.

Note
If you specify **deny** action, the router drops the traffic for that interface. Mirroring happens only if you add the **icmp-off** keyword to the ACE as shown. You can use the **icmp-off** keyword only for security or hybrid ACLs.

```
ipv4 access-list acl1
10 deny ipv4 any 2.1.0.0/16 capture icmp-off
20 permit ipv4 any any
!
```

Step 2 Create SPAN IPv6 ACL for traffic mirroring.

Example:

```
Router(config)# ipv6 access-list v6-monitor-acl
Router(config-ipv6-acl)# 10 permit ipv6 host 120:1:1::1 host 130:1:1::1
Router(config-ipv6-acl)# exit
```

The router creates an ACL named **v6-monitor-acl** and applies the **permit** action for the traffic.

Step 3 Apply the traffic monitoring to SPAN source interface.

Example:

```
Router(config)# interface HundredGigE0/0/0/12
Router(config-if)# monitor-session mon1 ethernet direction rx-only
Router(config-if)# acl ipv4 v4-monitor-acl
Router(config-if)# acl ipv4 v6-monitor-acl!
!
```

For **v4-monitor-acl** and **v6-monitor-acl** ACLs, the router applies traffic mirroring for **HundredGigE0/0/0/12** interface.

Note
To enable traffic mirroring, include the **capture** keyword for security or hybrid ACLs.

Step 4 Verify the ACL configuration on your router.

Example:

```
Router# show access-lists ipv4 v4span1 hardware ingress span interface HundredGigE0/0/0/12
location 0/3/cpu0
```

```
ipv4 access-list v4-monitor-acl
10 permit ipv4 host 51.0.0.0 host 101.0.0.0
20 permit ipv4 host 51.0.0.1 host 101.0.0.1
30 permit ipv4 host 51.0.0.2 any
40 permit ipv4 any host 101.0.0.3
50 permit ipv4 51.0.1.0 0.0.0.255 101.0.1.0 0.0.0.255
60 permit ipv4 51.0.2.0 0.0.0.255 101.0.2.0 0.0.0.255 precedence critical
```

Configure layer 3 ACL-based traffic mirroring

Use these steps to configure traffic mirroring for layer 3 ACLs.

Procedure

Step 1 Start a monitor session.

Example:

```
Router# configure
Router(config)# monitor-session ms1
```

Step 2 Define a destination.

Example:

```
Router(config-mon)# destination tunnel-ip 1
Router(config-mon)# commit
```

Step 3 Attach an interface to the monitor session for an acl and specify the direction for which you want to mirror the traffic.

Example:

```
Router# configure
Router(config)# interface HundredGigE/2/0/11
Router(config-if)# ipv4 access-group span ingress
Router(config-if)# monitor-session ms1 ethernet direction rx-only acl
Router(config-if-mon)# commit
```

Step 4 Use the **capture** keyword to start mirroring traffic for the ACL.

Example:

```
Router# configure
Router(config)# ipv4 access-list span
Router(config-ipv4-acl)# 5 permit ipv4 any any dscp 5 capture
Router(config-ipv4-acl)# 10 permit ipv4 any any
Router(config-ipv4-acl)# commit
```

Attach a source interface

Use these steps to attach a source interface to a monitor session for an ACL.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Router# configure
```

Step 2 Enter interface configuration mode for the specified source interface in **interface** *type number*. 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.

Example:

```
Router(config)# interface HundredGigE 0/1/0/10/0/1/0
```

Step 3 Control access to an interface in **ipv4 access-group** *acl-name* {**ingress** | **egress**}.

Example:

```
Router(config-if)# ipv4 access-group acl1 ingress
```

Step 4 Attach a monitor session to the source interface and enter the monitor session configuration mode.

Example:

```
Router(config-if)# monitor-session mon1 ethernet direction rx-only port-level acl
Router(config-if-mon)#
```

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

Step 5 Specify that the traffic mirrored is according to the defined ACL.

Example:

```
Router(config-if-mon)# acl
```

Note
f an ACL is configured by name, it overrides any ACL that may be configured on the interface.

Step 6 Exit the monitor session configuration mode and return to interface configuration mode.

Example:

```
Router(config-if-mon)# exit
Router(config-if)#
```

Step 7 Save configuration changes.

Example:

```
RP/0/RP0/CPU0(config-if)# end
or
RP/0/RP0/CPU0(config-if)# commit
```

When you execute the **end** command, the system prompts you to commit changes.

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

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

- **no** - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- **cancel** - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- **commit** - Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 8 Display information about the monitor session.

Example:

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

Multiple SPAN ACL sessions for MPLS

Multiple SPAN ACL sessions for MPLS is a feature that

- monitors the MPLS traffic by configuring multiple SPAN ACL sessions for MPLS, and
- mirrors ingress MPLS traffic through the **monitor-session** *session-name* **ethernet direction rx-only port-level** command.

Table 1: Feature History Table

Feature Name	Release Information	Description
Multiple SPAN ACL sessions for MPLS	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on Cisco 8011-4G24Y4H-I routers.

Feature Name	Release Information	Description
Multiple SPAN ACL sessions for MPLS	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature verifies the overall network performance simultaneously from various network locations and ensures a better network visibility, network resource efficiency, and flexibility. This feature allows to configure multiple SPAN ACL sessions for MPLS on Layer 3 interfaces configured on the Label-Switched Paths (LSPs) to monitor the MPLS traffic based on the labels and the EXP bit. This MPLS SPAN ACL configuration is supported only in the ingress direction. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH This feature introduces these changes: **CLI:** • **acl mpls** • **mpls access-list** **YANG Data Model:** `Cisco-IOS-XR-um-mpls-acl-cfg.yang` (see Github, YANG Data Models Navigator).

Starting from Cisco IOS XR Release 24.4.1, you can monitor the MPLS traffic by configuring multiple SPAN ACL sessions for MPLS. With this feature, the ingressing MPLS traffic is mirrored. This is achieved with the **monitor-session** *session-name* **ethernet direction rx-only port-level** configuration.

This feature is supported on both the Physical and Bundle main and subinterfaces.

Benefits of using multiple MPLS SPAN ACL sessions

We recommend using multiple SPAN ACL sessions for MPLS because this approach:

- Improves flexibility of the associated user interface.

- Avoids redundancy.
- Provides backward compatibility.
- Minimises configuration size on the disk.
- Reduces process memory in both the shared plane and local plane for scale configurations.

Configuration guidelines for multiple MPLS SPAN ACL sessions

Follow these guidelines when configuring multiple SPAN ACL sessions for MPLS:

- Configure multiple ACL sessions for MPLS exclusively in the ingress (Rx) direction.
- Configure up to four SPAN sessions.
- Do not use the *Deny* action as it is not supported.
- Use only GRE tunnel interfaces as the destination interfaces.
- Specify the monitor sessions for the configured interfaces.
- Use the SPAN session ID to distinguish between multiple SPAN sessions under the same source interface.

Configure multiple SPAN ACL sessions for MPLS

Use these steps to configure multiple SPAN ACL sessions for MPLS:

Procedure

Step 1 Define multiple SPAN ACLs for the incoming (Rx) traffic or the MPLS packets captured. In this example, multiple SPAN ACLs, mp1 and mp2, are defined for mirroring MPLS traffic.

Example:

```
Router(config)# mpls access-list mp1
Router(config-mpls-acl)# 10 permit label1 2000 label2 3000 label3 4000 exp1 5 exp2 5
exp3 7
Router(config-mpls-acl)# exit
Router(config)# mpls access-list mp2
Router(config-mpls-acl)# 10 permit label3 9000 exp3 5
Router(config-mpls-acl)# exit
Router(config)# commit
```

Step 2 Configure a monitor session on the specified destination interface for the incoming (Rx) traffic.

Example:

```
Router#config
Router(config)#interface tunnel-ip41
Router(config-if)#tunnel source 11.11.11.11
Router(config-if)#tunnel destination 22.22.22.22
Router(config-if)#ipv4 address 41.41.41.2 255.255.255.0
Router(config-if)#tunnel mode gre ipv4
Router(config-if)#commit
Router(config-if)#exit
!
```

```
Router(config)#monitor-session S1 ethernet destination interface tunnel-ipv41
Router(config-if)#commit
!
```

Step 3 Attach monitor session to source interface. This configuration attaches the MPLS SPAN ACL sessions to the specified source interface. Use the **direction rx-only** keyword so that only the ingress traffic is mirrored.

Example:

```
Router(config)# interface tenGigE 0/0/0/14
Router(config-if)# monitor-session S1 ethernet direction rx-only port-level
Router(config-if-mon)# acl mpls mp1
!!
```

Step 4 Execute this command to view the running configuration.

Example:

```
Router# show running-config interface tenGigE 0/0/0/14
Mon Apr  1 13:16:47.430 UTC
interface TenGigE0/0/0/14
 ipv4 address 1.1.1.1 255.255.255.0
 ipv6 address 1111::1:1/96
 monitor-session S1 ethernet direction rx-only port-level
  acl mpls mp1
 !
Router#
```

Step 5 Verify the monitor session and details of the session.

Example:

```
Router# show monitor-session status
Mon Apr 1 13:16:40.408 UTC
Monitor-session S1
Destination interface tunnel-ip41
================================================================================
Source Interface Dir Status
---------------------- ---- -------------------------------------------------
Te0/0/0/14 (port) Rx Operational

Router# show monitor-session status detail
Mon Apr 1 13:19:11.124 UTC
Monitor-session S1
Destination interface tunnel-ip41
Source Interfaces
-----------------
TenGigE0/0/0/14
Direction: Rx-only
Port level: True
ACL match: Disabled
IPv4 ACL: Disabled
IPv6 ACL: Disabled
MPLS ACL: Enabled (mp1)
Portion: Full packet
Interval: Mirror all packets
Mirror drops: Disabled
Status: Operational
RP/0/RP0/CPU0:ios#
```