Local SPAN

This chapter details a traffic mirroring feature that allows users to monitor network traffic on a single router or switch. It explains how Local SPAN copies traffic from source interfaces or VLANs to a destination port on the same device for analysis.

Local SPAN

Local SPAN is a traffic mirroring feature and the most basic form of traffic mirroring that

- mirrors both source and destination interfaces on the same router, and
- simplifies the router setup and reduces the need for additional hardware.

Table 1: Feature History Table

Feature Name	Release Information	Description
Local SPAN	Release 25.2.1	Introduced in this release on: Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 88-LC1-36EH • 88-LC1-12TH24FH-E

Feature Name	Release Information	Description
Local SPAN	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) Local SPAN allows you to monitor network traffic on a single switch by copying traffic from one or more source ports or VLANs to a destination port for analysis. This process occurs entirely within the same device, ensuring that both source and destination ports are located on it. You can monitor and analyze traffic without affecting the normal operation of the network. This feature is now supported on: • 8011-4G24Y4H-I

Configuration guidelines for local SPAN

The local SPAN feature supports multiple capabilities. These are the key guidelines:

- You can only configure this feature for ingress traffic.
- Configures the destination interface only as Layer 2 or Layer 3 physical main interface.
- Configures these interfaces as sources for a local SPAN session:
  - L3 physical main and sub-interface, bundle main, and bundle sub-interface.
  - L2 ethernet interfaces: Ethernet Flow Point (EFP) and trunk.
  - BVI interface.
- Mirrors IPv4, IPv6, IP-in-IP and MPLS traffic.
- Supports extended Access Control Lists (ACLs) to reduce mirrored traffic throughput.
- Supports traffic shaping on the destination interface.
- Supports session statistics. There is one counter for all types of traffic, that is, IPv4, IPv6, and MPLS.
- Supports up to four local SPAN sessions, shared between:
  - ERSPAN
  - Local SPAN, and
  - SPAN to File features.
- Supports up to 1000 source interfaces.

Restrictions for local SPAN

Generic restrictions for local SPAN

The generic restrictions for local SPAN include:

- Egress mirroring isn't supported.
- The physical interface used as destination can't be a bundle member link.
- GRE tunnels are not supported as source or destination interfaces.
- Per-source interface mirroring statistics isn't supported. However, SPAN session statistics are supported. The session statistics contain the total number of packets mirrored by the session.
- A destination interface can't be a mirrored source interface and vice versa.
- NetFlow or sFlow configuration is not supported on interfaces that already have a local SPAN session configured.
- The dropped packets at NPU cannot be captured by regular SPAN session. For capturing dropped packets at NPU, use the mirror forward-drop packets feature.

ACL restrictions for local SPAN

The ACL restrictions for local SPAN include:

- ACLs for Local SPAN are applied only in ingress direction.
- If the ACL keyword is present in monitor-session configuration for an interface but no ACL is applied to that interface, traffic packets are not mirrored.
- ACL for MPLS traffic isn't supported.

Configure local SPAN

Use these steps to configure local SPAN.

Procedure

Step 1 Create a local SPAN session.

Example:

```
Router#configure
Router(config)#monitor-session mon1 ethernet
Router(config-mon)#destination interface HundredGigE0/1/0/0
Router(config-mon)#commit
Router(config-mon)#end
Router#
```

Step 2 Attach the SPAN session to an interface.

Example:

```
Router(config-mon)#interface HundredGigE0/1/0/2
Router(config-if)# monitor-session mon1 ethernet direction rx-only
Router(config-if-mon)# no shut
Router(config-if)#!
Router(config-if)#
Router(config-if)#interface Bundle-Ether1
Router(config-if)# monitor-session mon1 ethernet direction rx-only
Router(config-if-mon)# no shutdown
Router(config-if)#!
Router(config-if)#


Router:monitor(config-if)#interface HundredGigE0/1/0/14.100
Router:monitor(config-subif)# monitor-session mon1 ethernet direction rx-only
Router:monitor(config-if-mon)# no shut
Router:monitor(config-subif)#!
Router:monitor(config-subif)#
Router:monitor(config-subif)#interface Bundle-Ether1.1
Router:monitor(config-subif)# monitor-session mon1 ethernet direction rx-only
Router:monitor(config-if-mon)# no shut
Router:monitor(config-subif)#!
Router:monitor(config-subif)#commit
```

Step 3 Verify the configuration.

Example:

```
Router#show monitor-session status
Monitor-session mon1
Destination interface HundredGigE0/1/0/0
========================================
Source Interface Dir Status
---------------------- ---- ----------------
Hu0/1/0/2 Rx Operational
Hu0/1/0/14.100 Rx Operational
BE1 Rx Operational
BE1.1 Rx Operational
```

Step 4 Execute the **show monitor-session status internal** command for session statistics.

Example:

```
Router#show monitor-session status internal
Thu Aug 13 20:05:23.478 UTC
Information from SPAN Manager and MA on all nodes:
Monitor-session mon1 (ID 0x00000001) (Ethernet)
SPAN Mgr: Destination interface HundredGigE0/1/0/0 (0x00800190)
Last error: Success
0/1/CPU0: Destination interface HundredGigE0/1/0/0 (0x00800190)
0/RP0/CPU0: Destination interface HundredGigE0/1/0/0 (0x00800190)
Information from SPAN EA on all nodes:
Monitor-session 0x00000001 (Ethernet)
0/1/CPU0: Name 'mon1', destination interface HundredGigE0/1/0/0 (0x00800190)
Platform, 0/1/CPU0:
Monitor Session ID: 1
Monitor Session Packets: 32
Monitor Session Bytes: 4024
0/2/CPU0: Name 'mon1', destination interface HundredGigE0/1/0/0 (0x00800190)
Platform, 0/2/CPU0:
Monitor Session ID: 1
```

```
Monitor Session Packets: 0
Monitor Session Bytes: 0
```

Local SPAN with ACLs

Local SPAN with an Access Control List (ACL) is a traffic mirroring feature that:

- filters and mirrors ingress traffic
- considers only Access Control Entries (ACEs) with capture keyword for traffic mirroring
- captures both permit and deny packets if the ACE contains the **capture** keyword, and
- allows one IPv4 ingress ACL and one IPv6 ingress ACL per interface.

Benefits of local SPAN with ACL

These are the benefits of local SPAN with ACL:

- **Traffic Filtering**: Local SPAN with ACL allows precise filtering of ingress traffic, ensuring that only relevant data is mirrored based on specific criteria.
- **Selective Mirroring**: By using the **capture** keyword in ACEs, you can selectively mirror both permitted and denied packets, providing flexibility in monitoring.
- **Efficient Monitoring**: Specifying one IPv4 and one IPv6 ingress ACL per interface streamlines monitoring processes and reduces unnecessary data capture.
- **Enhanced Network Security**: Filtering and mirroring ingress traffic can help identify and analyze potential security threats or anomalies in network traffic.

Configure local SPAN with IPv4 ACLs

Use these steps to configure local SPAN using IPv4 ACLs.

Procedure

Step 1 Configure IPv4 ACLs for traffic mirroring.

Example:

```
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 25.0.0.0 0.0.0.255 any capture
Router(config-ipv4-acl)# 20 permit ipv4 20.0.0.0 0.0.0.255 any
Router(config-ipv4-acl)# 30 permit ipv4 131.1.1.0 0.0.0.255 any capture
Router(config-ipv4-acl)# 40 permit ipv4 191.1.1.0 0.0.0.255 any capture
```

Step 2 Apply the traffic monitoring to an interface.

Example:

```
Router(config)# interface HundredGigE0/1/0/2
Router(config-if)# ipv4 address 131.1.1.2 255.255.255.0
Router(config-if)# monitor-session mon1 ethernet direction rx-only port-level
Router(config-if-mon)# acl
Router(config-if-mon)# ipv4 access-group acl1 ingress
```

Step 3 Verify the configuration.

Example:

```
Router#show running-config ipv4 access-list acl1
Thu Aug 13 20:22:54.388 UTC
ipv4 access-list acl1
10 permit ipv4 22.0.0.0 0.0.0.255 any capture
20 permit ipv4 20.0.0.0 0.0.0.255 any
30 permit ipv4 131.1.1.0 0.0.0.255 any capture
40 deny ipv4 181.1.1.0 0.0.0.255 any capture
!
```

Configure local SPAN with IPv6 ACLs

Use these steps to configure local SPAN using IPv6 ACLs.

Procedure

Step 1 Configure IPv6 ACLs for traffic mirroring.

Example:

```
Router(config)# ipv6 access-list acl2
Router(config-ipv6-acl)# 10 permit ipv6 10:1:1::2/64 any capture
Router(config-ipv6-acl)# 20 permit ipv6 10:1:1::3/64 any
Router(config-ipv6-acl)# 30 permit ipv6 10:1:1::4/64 any capture
```

Step 2 Apply the traffic monitoring to an interface.

Example:

```
Router(config)# interface HundredGigE0/1/0/3
Router(config-if)# ipv6 address 10:1:1::5/64
Router(config-if)# monitor-session mon2 ethernet direction rx-only port-level
Router(config-if-mon)# acl
Router(config-if-mon)# ipv6 access-group acl2 ingress
```

Step 3 Verify the configuration.

Example:

```
Router#show running-config ipv6 access-list acl2
Thu Aug 14 20:22:54.388 UTC
ipv6 access-list acl2
10 permit ipv6 10:1:1::2/64 any capture
20 permit ipv6 10:1:1::3/64 any
30 permit ipv6 10:1:1::4/64 any capture
!
```

Local SPAN rate limit

Local SPAN rate limit is a traffic mirroring feature that

- takes place at the session level, not at source interface level
- configures rate limiting when you configure a traffic class in local SPAN session
- uses traffic class to shape traffic on an egress interface, and
- applies a Quality of Service (QoS) policy to the egress interface over which the router send the mirrored traffic.

Example

This example provides details on how to configure the local SPAN rate limit. In this example, the class, TC5, matches with the class that you configured in the monitor session.

```
Router# monitor-session mon2 ethernet
destination interface HundredGigE0/1/0/19
traffic-class 5
class-map match-any TC5
match traffic-class 5
end-class-map
policy-map shape-foo
class TC5 /* This has to match the class that was configured on monitor session */
shape average percent 15
class class-default
interface HundredGigE0/1/0/19 /* This is the egress interface over which mirrored packets
are sent */
service-policy output shape-foo
```