



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 6.3.1	The local SPAN feature was introduced.

- [Introduction to Traffic Mirroring, on page 1](#)
- [Traffic Mirroring Types, on page 2](#)
- [Restrictions for Traffic Mirroring, on page 3](#)
- [Configuring Local Traffic Mirroring, on page 3](#)
- [Additional Information on Traffic Mirroring, on page 4](#)

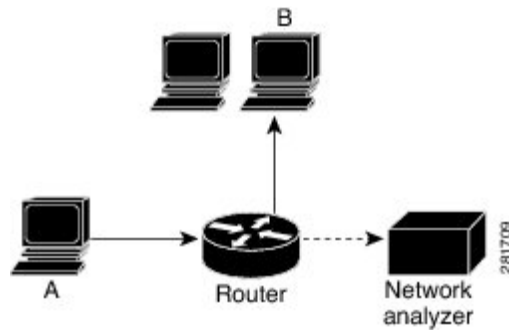
Introduction to Traffic Mirroring

Switched Port Analyzer (SPAN), which is also called port mirroring, or traffic mirroring 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. However, traffic from one source port can be copied to only one destination port. Traffic mirroring does not affect the flow of traffic on the source ports, and allows the mirrored traffic to be sent to a destination port.

For example, you need to attach a traffic analyzer to the router if you want to capture Ethernet traffic that is sent by host A to host B. Traffic between host A and host B is also seen on the destination port.

Figure 1: Traffic Mirroring Operation



When local traffic mirroring is enabled, the traffic analyzer is attached directly to the port of the same router that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port. The other sections of this document describe how you can fine tune this feature.

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 or Layer 3 traffic mirroring:** Both Layer 2 and Layer 3 source ports can be mirrored.
- **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 mirror 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 if the packets in the traffic are permitted or denied. 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.

- **SPAN to File:** 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 simplifies the analysis of the packets at a later stage.



Warning

Be cautious when you apply this feature to files located on interfaces with high traffic.

- **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 Embedded Event Manager (EEM) scripts.

Restrictions for Traffic Mirroring

- A maximum of 100 source ports/L2 subinterfaces per session are supported.
- Egress mirroring is supported on best effort basis. All the changes made to the source packets may not be reflected in the mirrored packets at the destination port.
- A maximum of up to four sessions are supported, based on the source interface directions.

Configuring Local Traffic Mirroring

The following task describes how to configure local traffic mirroring with physical ports used as the source port.



Note

For physical ports, you must configure the **port-level** option of the **monitor-session test direction rx-only port-level** command.

```
Router# configure
Router(config)# monitor-session mon1
Router(config-mon)# destination interface HundredGigE0/1/0/15
Router(config-mon)# exit
Router(config)# interface HundredGigE 0/1/0/1
Router(config-if)# monitor-session mon1 port-level direction rx-only
Router(config-if)# commit
```

The following task describes how to configure local traffic mirroring with L2 sub-interface used as the source port.

```
Router(config)# interface tenGigE 0/0/0/0.1 12transport
Router(config-subif)# encapsulation dot1q 1000
Router(config-subif)# monitor-session test direction rx-only
Router(config-if-mon)# commit
```

Verification

To verify the status information about configured traffic mirroring sessions, use the **show monitor-session status** command in EXEC mode.

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

```
Router# show monitor-session status
Monitor-session ms1
Destination interface HundredGigE0/0/1/2
=====
Source Interface      Dir      Status
-----
Hu0/0/1/3.100         Rx       Operational
Gi0/0/0/5 (port)      Both     Operational
Hu0/0/1/3 (port)      Both     Operational

Router# show monitor-session status detail
Monitor-session ms1
Destination interface HundredGigE0/0/1/2
Source Interfaces
-----
HundredGigE0/0/1/3.100
  Direction: Rx-only
  Port level: False
  ACL match: Disabled
  Portion: Full packet
  Interval: Mirror all packets
  Status: Operational
GigabitEthernet0/0/0/5
  Direction: Both
  Port level: True
  ACL match: Disabled
  Portion: Full packet
  Interval: Mirror all packets
  Status: Operational
HundredGigE0/0/1/3
  Direction: Both
  Port level: True
  ACL match: Disabled
  Portion: Full packet
  Interval: Mirror all packets
  Status: Operational

Router# show monitor-session status error
Monitor-session ms1
Destination interface HundredGigE0/0/1/2
=====
Source Interface      Dir      Status
-----
```

Additional Information on Traffic Mirroring

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 ports.

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 routers support a maximum of up to 800 source ports.

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 NCS 5000 Series Routers support a maximum of up to 100 source ports.

A source port has these characteristics:

- Physical ports are supported. It can be any data port type, such as 100 Gigabit Ethernet or 10 Gigabit Ethernet.
- L2 sub-interfaces can be configured 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 for local traffic mirroring.

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 monitor sessions.

Maximum number of monitor sessions supported can vary from 2 to 4, based on the directions (rx|tx|both) that you 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 Cisco IOS XR Software Release 7.8.1, up to three monitor sessions are supported on the NCS 5500 router. However, if you configure SPAN and CFM on the router, the maximum number of monitor sessions becomes one, as both functions use the same mirror profiles.

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 in native mode. From 7.4.1 release, 24 sessions in total are supported in 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 100 source ports.

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 cannot be a source port.
- A destination port must reside on the same router as the source port for local traffic mirroring.
- 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. It can be a Layer 2 or Layer 3 transport interface.
- At any 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.