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).

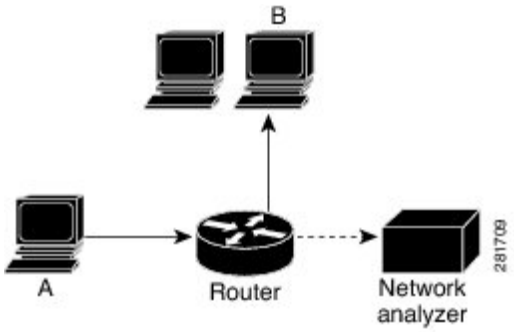
Overview of Traffic Mirroring

Traffic mirroring, which is 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, and allows the mirrored traffic to be sent to a destination interface or sub-interface.

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. All other ports see the traffic between hosts A and B.

Figure 1: Traffic Mirroring Operation



When local traffic mirroring is enabled, the traffic analyzer is attached directly 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. The other sections of this document describe how you can fine tune this feature.

ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) mirrors traffic on one or more source ports and delivers the mirrored traffic to destination port on another switch or management server.

ERSPAN enables network operators to troubleshoot issues in the network in real-time using automated tools that auto-configures ERSPAN parameters on the network devices to send specific flows to management servers for in-depth analysis.

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 analyzer.

Supported Capabilities

The following capabilities are supported:

- Layer 3 interfaces, such as physical, and bundle interfaces or sub-interface, can be source interfaces.
- ERSPAN with GRE IPv4 has tunnel destinations.
- ERPSAN supports only RX direction
- One destination interface is allowed per monitor session.
- Only port mode or ACL permit packets are part of mirroring features.
- Full packet capture is supported.
- MPLS protocols are supported only with IPv4 unicast routing.
- To limit the amount of bandwidth used for SPAN, a static policer is applied before sending out the SPAN-replicated packet. There will be one policer for all the SPAN packets on RX source. Initially, the policing rate is set to 1Gbps per Network Processor Unit (NPU).

Restrictions

The following are the ERSPAN and SPAN ACL restrictions:

- The maximum number of user-defined fields (UDF) supported in configurations is 8.
- The maximum number of UDF configurations that can be add to access control entries (ACE) is 8.
- The maximum number of bytes involved in a UDF lookup is 16 bytes.
- Remove and re-apply monitor-sessions on all interfaces after modifying the access control list (ACL) and UDF
- Only port mode or ACL permit packets will be part of mirroring features.
- The UDF offset depth that can be configured is 64 bytes, beginning from the start of Layer 2 frame.
- GRE features do not support ERSPAN generic routing encapsulation (GRE) encapsulated packets.
- Tunnel statistics are updated in the ingress of ERSPAN packets. When these encapsulated packets are dropped in egress, the tunnel statistics is still updated.
- Only ERSPAN TYPE II header is supported. The value of the index and session-ID fields are always 0.
- Sequence bit is set in the GRE header and the value of sequence number is always 0 for ERSPAN packets
- When you use the same ACEs defined in both the IPv4 and IPv6 ACLs, the router doesn't perform ERSPAN mirroring for the ACLs with the lowest priority set as 2 ms.

ERPAN with UDF

ERSPAN with UDF feature enables the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. This feature helps you to analyze and isolate packet drops in the network.

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.
- Monitor Session A designation for a collection of SPAN configurations consisting of many source interfaces and a set of destinations.
- 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 traffic mirroring configurations consisting of a single destination and, potentially, many source interfaces.

Characteristics of the 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. Your router can support any number of source ports (up to a maximum number of 800).

A source port has these characteristics:

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

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

- Each source port can be monitored in only one traffic mirroring session.
- It cannot be a destination port.
- Interfaces over which mirrored traffic may be routed must not be configured as a source port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor for local traffic mirroring. Remote traffic mirroring is supported in the ingress direction only. For bundles, the monitored direction applies to all physical ports in the group.

In the figure above, the network analyzer is attached to a port that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port.

Characteristics of the 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 is 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:

- A single Cisco NCS 5500 Series Router can have a maximum of eight monitor sessions.
- 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.

Characteristics of the Destination Port

Each session must have a destination port 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.
- A destination port for local mirroring can be any Ethernet physical port, EFP, and GRE tunnel interface, but not a bundle interface. It can be a Layer 2 or Layer 3 transport interface.
- A destination port can be a trunk (main) interface or a subinterface.
- 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.

Note

1. Source traffic mirroring ports (can be ingress or egress traffic ports).
2. Destination traffic mirroring port.

Configure Traffic Mirroring

```
 /* Configure remote  traffic mirroring. */

Router# configure
Router(config)# monitor-session session-name mpls-ipv4
Router(config)# destination interface tunnel-ip
Router(config)# exit
Router(config)# interface HundredGigE 0/1/0/1
Router(config-if)# monitor-session mon1 mpls-ipv4 direction rx-only
Router(config-if)# end

/* Attach the configurable source interface. */
Router# configure
Router(config)# interface HundredGigE 0/1/0/1
Router(config-if)# monitor-session mon1 mpls-ipv4 direction rx-only
Router(config-if-mon)# acl acl1
Router(config-if-mon)# end

/* Configure UDF-based ACL for traffic mirroring.*/
Router# configure
Router(config)# udf udf3 header outer 14 0 length
Router(config-if)# ipv4 access-list acl1
Router(config-ipv4-acl)#10 permit ipv4 any any udf udf1 0x1234 0xffff udf3 0x56 0xff
Router(config-ipv4-acl)# exit
Router(config)# interface HundredGigE 0/2/0/2
Router(config-if)# monitor-session mon1 mpls-ipv4 direction rx-only
Router(config-if-mon)# acl acl1
Router(config-if-mon)# commit
```

Running Configuration

```
/* Configure remote  traffic mirroring. */

configure
monitor-session session-name mpls-ipv
 destination interface tunnel-ip
exit
interface HundredGigE 0/1/0/1
monitor-session mon1 mpls-ipv4 direction rx-only

!

/* Attach configurable source interface. */
 interface HundredGigE 0/1/0/1
  monitor-session mon1 mpls-ipv4 direction rx-only
  acl acl1
!

/* Configure UDF-based ACL for traffic mirroring. */
udf udf3 header outer 14 0 length
  ipv4 access-list acl1
  10 permit ipv4 any any udf udf1 0x1234 0xffff udf3 0x56 0xff
  exit
  interface HundredGigE 0/2/0/2
   monitor-session mon1 mpls-ipv4 direction rx-only
  acl acl1
!
```

Verification

```
/* The following output displays the statistics of traffic mirroring sessions. */
/* Note that all source interfaces and the replicated packet statistics for each interface.
  */

Router# show monitor-session counters

Sat May 20 06:09:11.505 UTC
Monitor-session test1 (MPLS-IPv4)
  TenGigE0/7/0/6/9.2
    Rx replicated: 56197 packets, 43440281 octets
    Tx replicated: 0 packets, 0 octets
    Non-replicated: 0 packets, 0 octets
  TenGigE0/7/0/6/9.3
    Rx replicated: 56134 packets, 43391582 octets
    Tx replicated: 0 packets, 0 octets
    Non-replicated: 0 packets, 0 octets
  TenGigE0/7/0/6/9.4
    Rx replicated: 56126 packets, 43385398 octets
    Tx replicated: 0 packets, 0 octets


/* The following output displays the configured traffic mirroring sessions. */
/* In this output, the list of source and destinations interfaces, their status, and other
 pertinent details are displayed. */

Router# show monitor-session status

Sat May 20 06:48:29.133 UTC
Monitor-session mon1 (MPLS-IPv4)
```

```
Destination interface tunnel-ip2
=========================================
Source Interface      Dir   Status
--------------------- ----  --------------
Te0/6/0/1/9           Rx    Operational
Te0/7/0/6/9.1         Rx    Operational
Te0/7/0/6/9.2         Rx    Operational
Te0/7/0/6/9.3         Rx    Operational
Te0/7/0/6/9.4         Rx    Operational
Te0/7/0/6/9.5         Rx    Operational
Te0/7/0/6/9.6         Rx    Operational
Te0/7/0/6/9.7         Rx    Operational
Te0/7/0/6/9.8         Rx    Operational
Te0/7/0/6/9.9         Rx    Operational

/* The following output diaplays the configured traffic mirroring sessions in detail for
the specofoed interface. */

Router#  show monitor-session mon1 status detail
Sat May 20 11:26:03.482 UTC
Monitor-session test3 (MPLS-IPv4)
  Destination interface tunnel-ip3
  Source Interfaces
  -----------------
  TenGigE0/7/0/6/9.200
    Direction:  Rx-only
    Port level: False
    ACL match:  Enabled (acl101200)
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Operational
  TenGigE0/7/0/6/9.199
    Direction:  Rx-only
    Port level: False
    ACL match:  Enabled (acl101200)
    Portion:    Full packet
    Interval:   Mirror all packets
    Status:     Operational
  TenGigE0/7/0/6/9.198
    Direction:  Rx-only
    Port level: False
    ACL match:  Enabled (acl101200)



/* The following output displays the configured traffic mirroring sessions for the specifed
 interface. */

Router# show monitor-session source interface tenGigE 0/7/0/6/9 status internal
Sat May 20 06:13:52.934 UTC
Interface TenGigE0/7/0/6/9 (0x03800370)
SPAN MA:
  monitor-session test1 (MPLS-IPv4) (configured globally)
  destination interface tunnel-ip2 (0x08000084)
  replication direction: Rx-only
  port level: False
  ACL enabled (acl1)
  mirroring first 0 bytes
  interval: Mirror all packets
  state: up
  interface capsulation exists
  last PFI error: Success
SPAN EA, location 0/7/CPU0:
  monitor-session (MPLS-IPv4)
```

```
destination interface tunnel-ip2 (0x08000084)
replication direction: Rx-only
port level: False
ACL enabled (acl1)
mirroring first 0 bytes
interval: Mirror all packets
last platform error: Success.
```