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 4.3.0	This feature was introduced on the Cisco CRS Router.

Introduction to 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 Layer 3 network traffic passing in, or out of, a set of Ethernet interfaces. You can then pass this traffic to a network analyzer for analysis.

Traffic mirroring copies traffic from one or more Layer 3 interfaces or sub-interfaces 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 switching of traffic on the source interfaces or sub-interfaces, and allows the mirrored traffic to be sent to a destination next-hop address .

Traffic mirroring was introduced on switches because of a fundamental difference between switches and hubs. When a hub receives a packet on one port, the hub sends out a copy of that packet from all ports except from the one at which the hub received the packet. In the case of switches, after a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch receives. After this forwarding table is built, the switch forwards traffic that is destined for a MAC address directly to the corresponding port.

Layer 2 SPAN is not supported on the Cisco CRS Router.

The difference from Layer 2 SPAN is that the destination for mirrored packets is specified as a next-hop IP address rather than an explicit interface, and only Layer 3 packets are mirrored. In the Cisco IOS XR Software Release 4.3.0, it is assumed that the next-hop IP address should be looked up in the default VRF routing table.

Implementing Traffic Mirroring on the Cisco ASR 9000 Series RouterCisco CRS Router

Traffic Mirroring Terminology

- Ingress Traffic — Traffic that comes into the router.

- Egress Traffic — Traffic that goes out of the router.

- Source (SPAN) interface — An ingress interface that is monitored using the SPAN feature.

- Destination (SPAN) Nexthop — An egress Nexthop address where a network analyzer is connected.

- Monitor Session A designation for a collection of SPAN configurations consisting of many source interfaces and a set of destinations. In the Cisco IOS XR Software Release 4.3.0, only one destination is supported per monitor session.

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, Gigabit Ethernet, 10-Gigabit Ethernet, or EFPs.

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

- Each source port can be monitored in only one traffic mirroring session.

- Interfaces over which mirrored traffic may be routed must not be configured as a source port.

- ACL-based traffic mirroring. Traffic is mirrored based on the configuration of the global interface ACL. This is optional on the Cisco CRS Router.

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 destination. Some optional operations such as ACL filtering can be performed on the mirrored traffic streams. 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. The result is that the traffic that comes out of the destination is a combination of the traffic from one or more source ports, and the traffic from each source port may or may not have ACLs applied to it.

Monitor sessions have these characteristics:

- A single Cisco CRS Router can have a maximum of eight monitor sessions.

- A single monitor session can have only one destination .

- A single destination can belong to only one monitor session.

- A single Cisco CRS Router can have a maximum of 800 source ports.

- 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

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

A destination has these characteristics:

1	Source traffic mirroring ports (can be ingress or	2	Destination traffic mirroring port
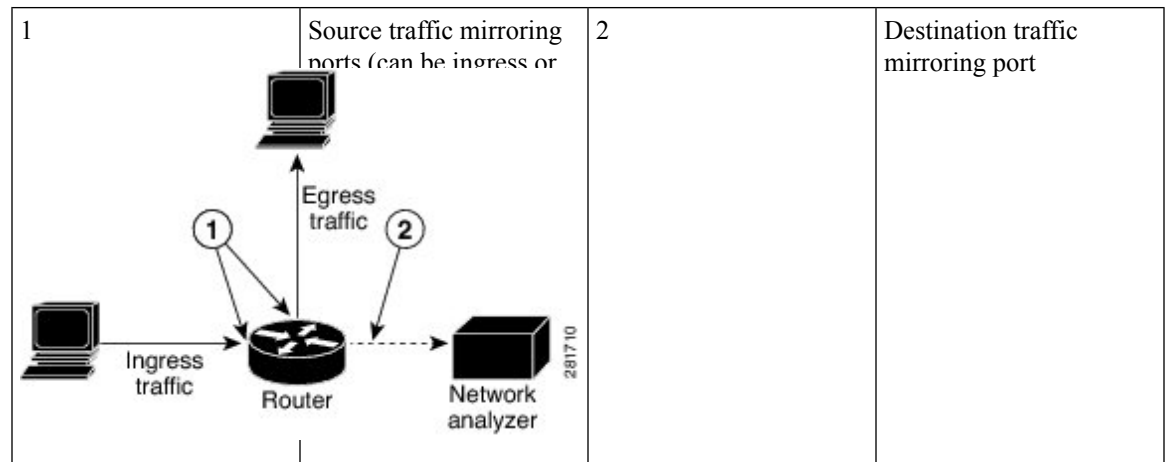
Restrictions for Traffic Mirroring

A maximum of eight monitoring sessions are supported. You can configure 800 source ports on a single monitoring session or an aggregate of 800 source ports over eight monitoring sessions.

These forms of traffic mirroring are not supported:

- Mirroring traffic to a GRE tunnel (also known as Encapsulated Remote Switched Port Analyzer [ER-SPAN] in Cisco IOS Software).

- If the destination of traffic mirroring is an nV satellite port and ICL is configured with a bundle interface, then replicated packets are not forwarded to the destination.

- MPLS traffic or tunnel traffic.

- Layer 2 traffic mirroring.

- VRF at destination ports.

- Mirroring for POS interfaces.

- Mirroring of egress traffic.

Configuring Traffic Mirroring

These tasks describe how to configure traffic mirroring:

How to Configure Layer-3 Traffic Mirroring

SUMMARY STEPS

1. **configure**
2. **monitor-session** *session-name* **[ipv4|ipv6]**
3. **destination** `next-hop` *ip address*
4. **exit**
5. **interface** *source-interface*
6. **monitor-session** *session-name* **{ipv4|ipv6}** **[direction {rx-only| tx-only}]**
7. **end** or **commit**
8. **show monitor-session [session-name] status**

DETAILED STEPS

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

Step 2	**monitor-session** *session-name* **[ipv4|ipv6]**
	
	 Example:
	
	 `RP/0/RP0/CPU0:router(config)# monitor-session mon1`
	 `RP/0/RP0/CPU0:router(config-mon)#`
		Defines a monitor session and enters monitor session configuration mode. The monitor-session name is a printable string that can be at most 79 characters in length.
		
		 Note • This command triggers entry in to the monitor-session sub-mode and creates the session. The session is non-operable until a destination is configured for the session. The destination can be either an IPv4 or IPv6 address.

Step 3	**destination** `next-hop` *ip address*
	
	 Example:
	
	 `RP/0/RP0/CPU0:router(config-mon)# destination`
	 `next-hop ipv4 254.23.24.5`
		Configures the destination for the current monitor-session to be a next-hop IP address (whose type matches that of the monitor-session).
		
		 Note • This may only be specified for ipv4 and ipv6 monitor-sessions. A monitor session can be either for IPv4 or for IPv6. It cannot support both together.

	Command or Action	Purpose

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** *source-interface*
	
	Example:
	
	`RP/0/RP0/CPU0:router(config)# interface`
	`gigabitethernet0/0/0/11.10`
		Enters interface configuration mode for the specified 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* **{ipv4|ipv6}** [**direction** {**rx-only| tx-only**}]
	
	Example:
	
	`RP/0/RP0/CPU0:router(config-if)# monitor-session`
	`mon1`
		Specifies the monitor session to be used on this interface. Use the **direction** keyword to specify that only ingress or egress traffic is mirrored. To support both IPv4 and IPv6 mirroring, separate monitor sessions defined for IPv4 and IPv6 must be attached to the interface.
		
		The interface name can be the name of any Ethernet interface. The monitor-session name is a printable string at most 79 characters in length.
		
		Note • If no type is given, ethernet is assumed. Only Rx 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.

	Command or Action	Purpose
Step 8	**show monitor-session [session-name] status** **Example:** `RP/0/RP0/CPU0:router# show monitor-session`	Displays information about the traffic mirroring session.

How to Configure ACL-Based Traffic Mirroring

Before you begin

The global interface ACL should be configured using one of these commands with the **capture** keyword:

- **ipv4 access-list**

- **ipv6 access-list**

- **ethernet-services access-list**

    For more information, refer to the *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router* or the *Cisco IOS XR Virtual Private Network Command Reference for the Cisco CRS Router*.

SUMMARY STEPS

1. **configure**
2. **monitor-session** *session-name* **[ipv4|ipv6]**
3. **destination** `next-hop` *ip address*
4. **exit**
5. **interface** *source-interface*
6. **ethernet-services access-group** *access-list-name* [**ingress** | **egress**]
7. **monitor-session** *session-name* [ipv4|ipv6] [direction {rx-only|tx-only}]
8. **acl**
9. **end** or **commit**
10. **show monitor-session [session-name] status** [**detail**] [**error**]

DETAILED STEPS

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

Step 2	**monitor-session** *session-name* **[ipv4|ipv6]**
	
	Example:
	
	`RP/0/RP0/CPU0:router(config)# monitor-session mon1`
	`RP/0/RP0/CPU0:router(config-mon)#`
		Defines a monitor session and enters monitor session configuration mode. The monitor-session name is a printable string that can be at most 79 characters in length.

	Command or Action	Purpose
		Note • This command triggers entry in to the monitor-session sub-mode and creates the session. The session is non-operable until a destination is configured for the session. The destination can be either an IPv4 or IPv6 address.
Step 3	**destination** next-hop *ip address* **Example:** RP/0/RP0/CPU0:router(config-mon)# destination next-hop ipv4 254.23.24.5	Configures the destination for the current monitor-session to be a next-hop IP address (whose type matches that of the monitor-session). **Note** • This may only be specified for ipv4 and ipv6 monitor-sessions. A monitor session can be either for IPv4 or for IPv6. It cannot support both together.
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** *source-interface* **Example:** RP/0/RP0/CPU0:router(config)# interface gigabitethernet0/0/0/11	Enters interface configuration mode for the specified 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	**ethernet-services access-group** *access-list-name* [**ingress** | **egress**] **Example:** RP/0/RP0/CPU0:router(config-if)# ethernet-services access-group acl1 ingress	Associates the access list definition with the interface being mirrored.
Step 7	**monitor-session** *session-name* [ipv4|ipv6] [direction {rx-only|tx-only}] **Example:** RP/0/RP0/CPU0:router(config-if)# monitor-session mon1 direction rx-only	Specifies the monitor session to be used on this interface.
Step 8	**acl** **Example:** RP/0/RP0/CPU0:router(config-if-mon)# acl	Specifies that the traffic mirrored is according to the defined global interface ACL.
Step 9	**end** or **commit**	Saves configuration changes.

Command or Action	Purpose

Example:
 	
`RP/0/RP0/CPU0:router(config-if)# end`
 	
or
 	
`RP/0/RP0/CPU0:router(config-if)# commit`
	• 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 10 **show monitor-session [session-name] status [detail] [error]** **Example:** `RP/0/RP0/CPU0:router# show monitor-session`	Displays information about the monitor session.

Troubleshooting ACL-Based Traffic Mirroring

Take note of these configuration issues:

- Even when the **acl** command is configured on the source mirroring port, if the ACL configuration command does not use the **capture** keyword, no traffic gets mirrored.

- If the ACL configuration uses the **capture** keyword, but the **acl** command is not configured on the source port, traffic is mirrored, but no access list configuration is applied.

This example shows both the **capture** keyword in the ACL definition and the **acl** command configured on the interface:

```
monitor-session tm_example
!
ethernet-services access-list tm_filter
 10 deny 0000.1234.5678 0000.abcd.abcd any capture
!
interface GigabitEthernet0/2/0/0
 monitor-session tm_example direction rx-only
 acl
!
 l2transport
 !
```

```
 ethernet-services access-group tm_filter ingress
end
```

Traffic Mirroring Configuration Examples

This section contains examples of how to configure traffic mirroring:

Viewing Monitor Session Status: Example

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

```
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 >
```

Monitor Session Statistics: Example

Use the **show monitor-session** command with the **counters** keyword to show the statistics/counters (received/transmitted/dropped) of different source ports. For each monitor session, this command displays a list of all source interfaces and the replicated packet statistics for that interface.

The full set of statistics displayed for each interface is:

• RX replicated packets and octets

• TX replicated packets and octets

• Non-replicated packet and octets

```
 RP/0/RP00/CPU0:router# show monitor-session counters

Monitor-session ms1
 GigabitEthernet0/2/0/19.10
  Rx replicated: 1000 packets, 68000 octets
  Tx replicated: 1000 packets, 68000 octets
  Non-replicated: 0 packets, 0 octets
```

Use the **clear monitor-session counters** command to clear any collected statistics. By default this command clears all stored statistics; however, an optional interface filter can be supplied.

```
RP/0/RP00/CPU0:router# clear monitor-session counters
```

Layer 3 ACL-Based Traffic Mirroring: Example

This example shows how to configure Layer 3 ACL-based traffic mirroring:

```
RP/0/RP00/CPU0:router# configure
RP/0/RP00/CPU0:router(config)# monitor-session ms1
RP/0/RP00/CPU0:router(config-mon)# destinationnext-hop 10.1.1.0
RP/0/RP00/CPU0:router(config-mon)# commit

RP/0/RP00/CPU0:router# configure
RP/0/RP00/CPU0:router(config)# interface gig0/2/0/11
RP/0/RP00/CPU0:router(config-if)# ipv4 access-group span ingress
RP/0/RP00/CPU0:router(config-if)# monitor-session ms1
RP/0/RP00/CPU0:router(config-if-mon)# commit

RP/0/RP00/CPU0:router# configure
RP/0/RP00/CPU0:router(config)# ipv4 access-list span
RP/0/RP00/CPU0:router(config-ipv4-acl)# 5 permit ipv4 any any dscp 5 capture
RP/0/RP00/CPU0:router(config-ipv4-acl)# 10 permit ipv4 any any
RP/0/RP00/CPU0:router(config-ipv4-acl)# commit
```

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:

```
Monitor-session sess1
<Session status>
=========================================================================
Source Interface   Dir  Status
-------------------- ---- --------------------------------------------------
Gi0/0/0/0      Both <Source interface status>
Gi0/0/0/2      Both <Source interface status>
```

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. Check **show run** command output to ensure that a session with a correct name has been configured.
Destination next-hop IPv4/IPv6 address <addr> is not configured	The IPv4 or IPv6 address that has been configured as the destination does not exist.
Destination next-hop IPv4 address <addr> not reachable	The IPv4 or IPv6 address that has been configured as the destination is not reachable or is not in the Up state. You can verify the status of the destination using the **show monitor-session status detail** command**.**

The <Source interface status> can report these messages:

Source Interface Status	Explanation
Operational	Everything appears to be working correctly in traffic mirroring PI. Please follow up with the platform teams in the first instance, if mirroring is not operating as expected.
Not operational (Session is not configured globally)	The session does not exist in global configuration. Check the **show run** command output to ensure that a session with the right name has been configured.
Not operational (destination not known)	The session exists, but it either does not have a destination interface specified, or the destination interface named for the session does not exist (for example, if the destination is a sub-interface that has not been created).
Not operational (destination not active)	The destination interface or pseudowire is not in the Up state. See the corresponding *Session status* error messages for suggested resolution.
Not operational (source state <down-state>)	The source interface is not in the Up state. You can verify the state using the **show interfaces** command. Check the configuration to see what might be keeping the interface from coming up (for example, a sub-interface needs to have an appropriate encapsulation configured).
Error: see detailed output for explanation	Traffic mirroring has encountered an error. Run the **show monitor-session status detail** command to display more information.

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

RP/0/RP0**show monitor-session status detail**

Here are additional trace and debug commands:

```
RP/0/RP00/CPU0:router# show monitor-session platform trace ?

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

RP/0/RP00/CPU0:router# show monitor-session trace ?

 process Filter debug by process

RP/0/RP00/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/RP00/CPU0:router# debug monitor-session platform all

RP/0/RP00/CPU0:router# debug monitor-session platform event

RP/0/RP00/CPU0:router# debug monitor-session platform info

RP/0/RP00/CPU0:router# show monitor-session status ?

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

RP/0/RP00/CPU0:router# show monitor-session status

RP/0/RP00/CPU0:router# show monitor-session status errors
```