CHAPTER 27

Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Cisco ME 3400E Ethernet Access switch.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

Understanding SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

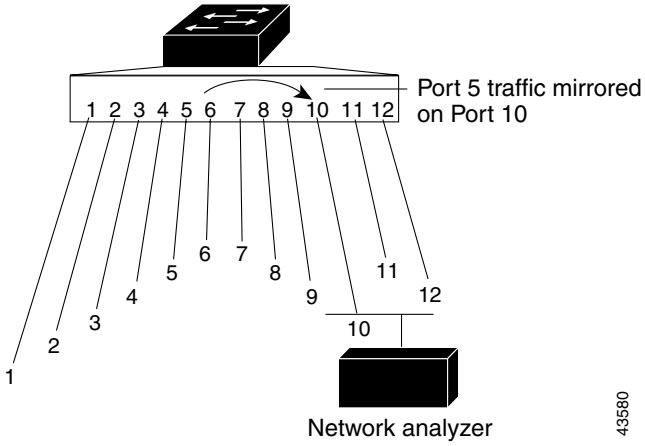
You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

-
-
-
- , page 27-8

Local SPAN

all traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

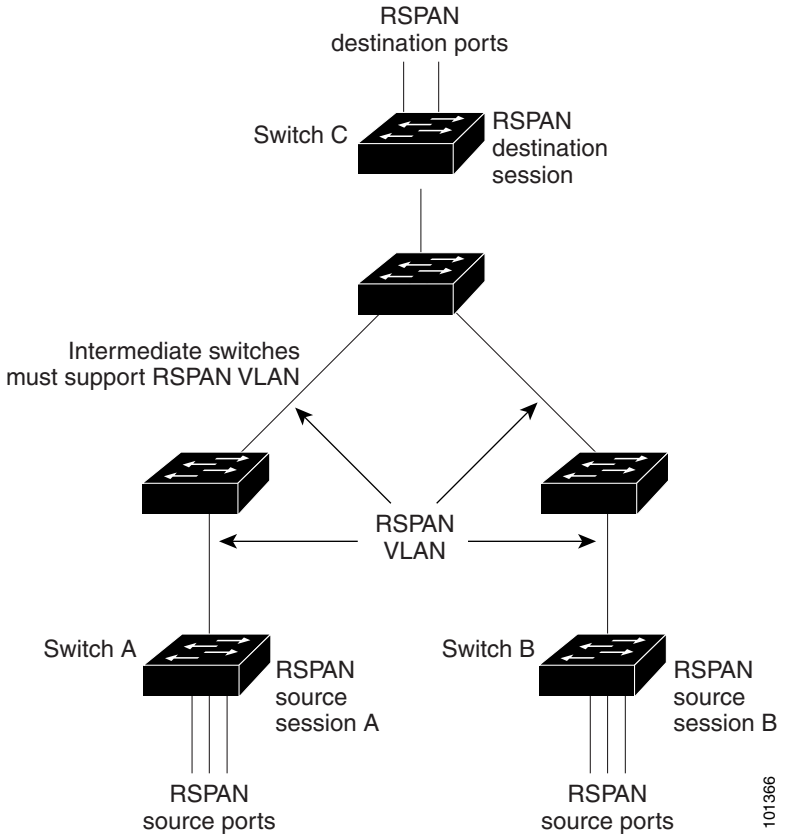
Figure 27-1 Example of Local SPAN Configuration on a Single Switch



Remote SPAN

A and Switch B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Switch C in the figure.

Example of RSPAN Configuration



SPAN and RSPAN Concepts and Terminology

SPAN Sessions

"RSPAN VLAN" section on page 27-7).

Traffic monitoring in a SPAN session has these restrictions:

Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.

The switch supports up to two source sessions (local SPAN and RSPAN source sessions). You can run both a local SPAN and an RSPAN source session in the same switch. The switch supports a total of 66 source and RSPAN destination sessions.

You can have multiple destination ports in a SPAN session, but no more than 64 destination ports.

You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. When the metro IP access image in running on the switch, both switched and routed ports can be configured as SPAN sources and destinations.

SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, can result in dropped or lost packets.

When RSPAN is enabled, each packet being monitored is transmitted twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.

You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.

The switch does not support a combination of local SPAN and RSPAN in a single session. That is, an RSPAN source session cannot have a local destination port, an RSPAN destination session cannot have a local source port, and an RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch.

Monitored Traffic

- Receive (Rx) SPAN—The goal of receive (or ingress) SPAN is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input access control lists (ACLs), ingress QoS policing, VLAN ACLs and egress QoS policing.

encapsulation replicate

Source Ports

monitored port

It can be any port type—for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, user network interface (UNI), network node interface (NNI), enhanced network interface (ENI) and so forth.

For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.

It can be a routed port, an access port, or a trunk port.

It cannot be a destination port.

Source ports can be in the same or different VLANs.

You can monitor multiple source ports in a single session.

Source VLANs

-
-
-
-
-
-

VLAN Filtering

-
-
-
-
-

Destination Port

monitoring port

-
-
-
-
-
-
-
-
-
-
-
-
-

encapsulation dot1q

encapsulation replicate

RSPAN VLAN

-
-
-

remote-span

–

rspan-vlan

–

no uni-vlan

SPAN and RSPAN Interaction with Other Features

-
-
-
-
-

inactive suspended

Configuring SPAN and RSPAN

-
-
-

Default SPAN and RSPAN Configuration

Table 27-1 Default SPAN and RSPAN Configuration

Feature	Default Setting
	both

SPAN Configuration Guidelines

-
-
-
-
-
- {*session_number* | | | } global configuration command to delete configured SPAN parameters.

  For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged or IEEE 802.1Q—if the or keywords are specified. If the keywords are not specified, the packets are sent in native form. For RSPAN destination ports, outgoing packets are not tagged.

  You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.

  You can limit SPAN traffic to specific VLANs by using the **filter vlan**

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports:

	Command	Purpose
Step 1	**configure terminal**	
Step 2		

	Command	Purpose
Step 3	*interface-id* | *vlan-id* [**,** **-**] [| **rx** **tx**	**port-channel** *port-channel-number* . *Valid port-channel numbers are 1 to 48.* *vlan-id* *session_number*
Step 4	*session_number* *interface-id*	*session_number* **Note** *interface-id* **Note** *session_number*
Step 5		

Step 6	**show monitor session** **show running-config**	
Step 7	**copy running-config startup-config**	

no monitor session

no monitor session

source interface vlan **no**
monitor session **destination interface**
encapsulation replicate **no**

```
Switch(config)# no monitor session 1
                monitor session 1 source interface gigabitethernet0/1
                monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
                end
```

```
                no monitor session 1 source interface gigabitethernet0/1
                end
```

```
                no monitor session 1 source interface gigabitethernet0/1 rx
```

```
                no monitor session 2
                monitor session 2 source vlan 1 - 3 rx
                monitor session 2 destination interface gigabitethernet0/2
                monitor session 2 source vlan 10
                end
```

Creating a Local SPAN Session and Configuring Ingress Traffic

Note

configure terminal	
no monitor session all local remote	
monitor session source interface vlan , - both rx tx	
monitor session destination interface encapsulation dot1q | replicate} ingress dot1q | untagged] vlan	**, -** **encapsulation dot1q** **encapsulation replicate** **ingress** **dot1q—** **untagged—** **vlan** *vlan-id* **dot1q untagged**
end	
show monitor session *session_number* **show running-config**	
copy running-config startup-config	

no monitor session

no monitor session

source interface vlan **no**
monitor session **destination interface**

no

```
replicate ingress dot1q vlan 6
end
```

Specifying VLANs to Filter

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

	Command	Purpose
Step 8		

```
monitor session 2 filter vlan 1 - 5 , 9
monitor session 2 destination interface gigabitethernet0/1
end
```

-

Configuring a VLAN as an RSPAN VLAN


```
                vlan 901
Switch(config-vlan)#
Switch(config-vlan)#
```


```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```


	Command	Purpose
Step 9		
Step 10		

```
Switch(config)#
Switch(config)#
Switch(config)#
```

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		**Note** **Note** • •
Step 5		
Step 6		
Step 7		

Specifying VLANs to Filter

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		

Displaying SPAN and RSPAN Status