



CHAPTER 49

Configuring SPAN, RSPAN and the Mini Protocol Analyzer

This chapter describes how to configure Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), and the Mini Protocol Analyzer on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How SPAN and RSPAN Work, page 49-1](#)
- [Understanding How the Mini Protocol Analyzer Works, page 49-4](#)
- [SPAN, RSPAN and Mini Protocol Analyzer Session Limits, page 49-5](#)
- [Configuring SPAN on the Switch, page 49-6](#)
- [Configuring RSPAN on the Switch, page 49-10](#)
- [Configuring the Mini Protocol Analyzer on the Switch, page 49-19](#)



Note

To configure SPAN, RSPAN or the Mini Protocol Analyzer from a network management station (NMS), refer to the NMS documentation (see the [“Using CiscoWorks2000” section on page 47-6](#)).

Understanding How SPAN and RSPAN Work

These sections describe the concepts and terminology that are associated with SPAN and RSPAN configuration:

- [SPAN Session, page 49-2](#)
- [Destination Port, page 49-2](#)
- [Source Port, page 49-2](#)
- [Ingress SPAN, page 49-3](#)
- [Egress SPAN, page 49-3](#)
- [VSPAN, page 49-3](#)

- [Trunk VLAN Filtering, page 49-4](#)
- [SPAN Traffic, page 49-4](#)

SPAN Session

A SPAN session is an association of destination ports with a set of source ports, configured with the parameters that specify the monitored network traffic. You can configure multiple SPAN sessions in a switched network. The SPAN sessions do not interfere with the normal operation of the switches. You can enable or disable the SPAN sessions with the command-line interface (CLI) or SNMP commands. When enabled, a SPAN session might become active or inactive based on various events or actions, and this would be indicated by a syslog message. The “Status” field in the **show span** and **show rspan** commands displays the operational status of a SPAN or RSPAN session.

A SPAN or RSPAN destination session remains inactive after system power up until the destination ports are operational. An RSPAN source session remains inactive until any of the source ports are operational or the RSPAN VLAN becomes active.

Destination Port

A destination port (also called a *monitor port*) is an access port where SPAN sends the packets for analysis. After a port becomes an active destination port, it does not forward any traffic except that required for the SPAN session. By default, an active destination port disables the incoming traffic (from the network to the switching bus), unless you specifically enable the port. If the incoming traffic is enabled for the destination port, it is switched in the native VLAN of the destination port. The destination port does not participate in spanning tree while the SPAN session is active. See the caution statement in the “[Configuring SPAN from the CLI](#)” section on page 49-8 for information on how to prevent loops in your network topology.

Multiple destination ports can be specified in each local SPAN session but a destination port cannot be a destination port for multiple SPAN sessions. An access port that is configured as a destination port cannot be configured as a source port. EtherChannel ports cannot be SPAN destination ports.

If the trunking mode of a SPAN destination port is “on” or “nonegotiate” during the SPAN session configuration, the SPAN packets that are forwarded by the destination port have the encapsulation as specified by the trunk type; however, the destination port stops trunking, and the **show trunk** command reflects the trunking status for the port prior to the SPAN session configuration.

Source Port

A source port is an access port that is monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both. You can monitor one or more source ports in a single SPAN session with the user-specified traffic types (ingress, egress, or both) applicable for all the source ports.

You can configure the source ports in any VLAN. You can configure the VLANs as the source ports (*src_vlans*), which means that all the ports in the specified VLANs are the source ports for the SPAN session.

The source ports are administrative (*Admin Source*), operational (*Oper Source*), or both. The administrative source ports are the source ports or the source VLANs that are specified during the SPAN session configuration. The operational source ports are the source ports that are monitored by the destination port. For example, when the source VLANs are used as the administrative source, the operational source is all the ports in all the specified VLANs.

The operational sources are always the active ports. If a port is not in the spanning tree, it is not an operational source. All physical ports in an EtherChannel source are included in the operational sources if the logical port is included in the spanning tree.

The destination port, if it belongs to any of the administrative source VLANs, is excluded from the operational source.

You can configure a port as a source port in multiple active SPAN sessions, but you cannot configure an active source port as a destination port for any SPAN session.

If a SPAN session is inactive, the “oper source” field is not updated until the session becomes active.

The trunk ports can be configured as the source ports and can be mixed with the nontrunk source ports; however, the encapsulation of the packets that are forwarded by the destination port are determined by the trunk settings of the destination port during the SPAN session configuration.

Ingress SPAN

Ingress SPAN copies the network traffic that is received by the source ports for analysis at the destination ports.

Egress SPAN

Egress SPAN copies the network traffic that is transmitted from the source ports for analysis at the destination ports.

VSPAN

VLAN-based SPAN (VSPAN) is analysis of the network traffic in one or more VLANs. You can configure VSPAN as ingress SPAN, egress SPAN, or both. All the ports in the source VLANs become the operational source ports for the VSPAN session. The destination ports, if they belong to any of the administrative source VLANs, are excluded from the operational source. If you add or remove the ports from the administrative source VLANs, the operational sources are modified accordingly.

Use the following guidelines for VSPAN sessions:

- The trunk ports are included as the source ports for the VSPAN sessions, but only the VLANs that are in the Admin source list are monitored if these VLANs are active for the trunk.
- For the VSPAN sessions with both ingress and egress SPAN configured, the system operates as follows based upon the type of supervisor engine that you have:
 - WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-SUP720, WS-SUP32-GE-3B, —Two packets are forwarded by the SPAN destination port if the packets get switched on the same VLAN.
 - WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE—Only one packet is forwarded by the SPAN destination port.
- An inband port is not included as Oper source for the VSPAN sessions.

- When a VLAN is cleared, it is removed from the source list for the VSPAN sessions.
- A VSPAN session is disabled if the Admin source VLANs list is empty.
- The inactive VLANs are not allowed for the VSPAN configuration.
- A VSPAN session is made inactive if any of the source VLANs become the RSPAN VLANs.

Trunk VLAN Filtering

Trunk VLAN filtering is analysis of network traffic on a selected set of VLANs on the trunk source ports. You can combine trunk VLAN filtering with the other source ports that belong to any of the selected VLANs, and you can also use trunk VLAN filtering for RSPAN. Based on the traffic type (ingress, egress, or both), SPAN sends a copy of the network traffic in the selected VLANs to the destination ports.

Use trunk VLAN filtering only with the trunk source ports. If you combine trunk VLAN filtering with the other source ports that belong to the VLANs that are not included in the selected list of filter VLANs, SPAN includes only the ports that belong to one or more of the selected VLANs in the operational sources.

When a VLAN is cleared, it is removed from the VLAN filter list. A SPAN session is disabled if the VLAN filter list becomes empty.

Trunk VLAN filtering is not applicable to the VSPAN sessions.

SPAN Traffic

All network traffic, including the multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN (RSPAN does not support monitoring of BPDU packets or Layer 2 protocol packets such as CDP, DTP, and VTP). Multicast packet monitoring is enabled by default.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination ports. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination port d1. If a packet enters the switch through a1 and gets switched to a2, both the incoming and outgoing packets are sent to destination port d1. Both packets would be the same (if a Layer 3 rewrite occurs, the packets are different). For the RSPAN sessions with the sources that are distributed in multiple switches, the destination ports might forward multiple copies of the same packet.

Understanding How the Mini Protocol Analyzer Works

The Mini Protocol Analyzer copies network traffic from a source port (see the [“Source Port” section on page 49-2](#) for an explanation of a source port). A Mini Protocol Analyzer session differs from a SPAN session in that the copied source port traffic from a Mini Protocol Analyzer session travels over the switch backplane where it is written to an output file. By default, the output file is stored on the flash memory of the switch. No destination port is required for the Mini Protocol Analyzer.

Once the file is created, you open and view the file using the Ethereal Network Protocol Analyzer. The Ethereal Network Protocol Analyzer is open source software and is available from <http://www.ethereal.com>.

You specify a single port as the source port. The source port can be either an access port or a trunk port. You cannot specify a VLAN as a source port. The Mini Protocol Analyzer also captures double tagged frames on dot1qtunnel, PAgP and LACP channel ports.

The functional differences between the Mini Protocol Analyzer and SPAN are as follows:

- The Mini Protocol Analyzer does not use a SPAN destination port, which frees up an extra port for network traffic.
- The Mini Protocol Analyzer does not require an external traffic analyzer such as a remote monitor.
- You do not require physical access to the switch to attach a network analyzer. You can access and download the output file from the Flash memory.

Mini Protocol Analyzer Session

A Mini Protocol Analyzer session is an association of a source port with the output file to which the source port traffic is mirrored. You can filter the type of traffic that is monitored by the following criteria:

- Source IP address
- Destination IP address
- Source MAC address
- Destination MAC address

By default, all traffic is captured. If you specify any combination of source and destination filters, only the traffic that matches those source and destination filters will be captured. The source and destination filters are applied on a Boolean logical OR basis—if traffic meets any of the criteria specified in any of the filters, it will be captured.

If you specify a filter based on the packet size, the packets that are larger than the specified size are captured and truncated to the specified size. You can specify a maximum of 16 filters for a Mini Protocol Analyzer session. Enter the **set packet-capture snap-length** command to specify the length to which the packets are truncated. The packet length is not counted against the maximum number of filters.

You can specify the filtering criteria either before or after you begin the Mini Protocol Analyzer session. If you specify the filtering criteria before you start the Mini Protocol Analyzer session, only the traffic that meets the filtering criteria is captured and sent to the output file. You can also filter the captured traffic after the Mini Protocol Analyzer session completes by using the Filter function of the Ethereal Network Protocol Analyzer.

You enable or disable a Mini Protocol Analyzer session using CLI or SNMP commands.

A Mini Protocol Analyzer session becomes active when both of the following criteria are met:

- After the source port becomes operational.
- After you enter the **set packet-capture start** command.

SPAN, RSPAN and Mini Protocol Analyzer Session Limits

You can configure (and store in NVRAM) a maximum of 30 SPAN sessions or 29 SPAN sessions and (store in the Flash memory) one Mini Protocol Analyzer session in a Catalyst 6500 series switch.

See [Table 49-1](#) for the supported combinations of SPAN, RSPAN, and Mini Protocol Analyzer sessions. You can configure multiple ports or VLANs as sources for each SPAN session, and you can configure a single source port for each Mini Protocol Analyzer session.

Table 49-1 SPAN RSPAN and Mini Protocol Analyzer Session Limits

SPAN, RSPAN, and Mini Protocol Analyzer Sessions	Catalyst 6500 Series Switches
rx or both SPAN sessions	2 ¹
tx SPAN sessions	4
Mini Protocol Analyzer sessions	1
tx, rx, or both RSPAN source sessions	1 ²
RSPAN destinations	24
Total SPAN sessions	30 ³

1. Each RSPAN source session or Mini Protocol Analyzer session reduces the limit for **rx** or **both** SPAN sessions by one.
2. Supervisor Engine 720 supports two RSPAN source sessions.
3. 2 **rx** or **both** SPAN sessions + 4 **tx** SPAN sessions + 24 RSPAN destination sessions = 30 total SPAN sessions. A Mini Protocol Analyzer session counts as one **rx** or **both** SPAN session.

Configuring SPAN on the Switch

These sections describe how to configure SPAN:

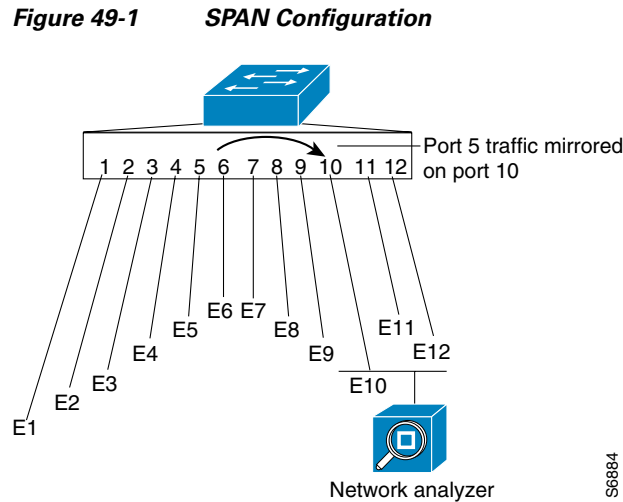
- [SPAN Hardware Requirements, page 49-6](#)
- [Understanding How SPAN Works, page 49-6](#)
- [SPAN Configuration Guidelines, page 49-7](#)
- [Configuring SPAN from the CLI, page 49-8](#)

SPAN Hardware Requirements

All Catalyst 6500 series switch supervisor engines support SPAN.

Understanding How SPAN Works

SPAN selects the network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN mirrors the traffic from one or more source ports on any VLAN, from one or more VLANs, or from the sc0 console interface to the destination ports for analysis (see [Figure 49-1](#)). In [Figure 49-1](#), all traffic on Ethernet port 5 (the source port) is mirrored to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to it.



For SPAN configuration, the source ports and the destination ports must be on the same switch.

SPAN does not affect the switching of network traffic on the source ports; a copy of the packets that are received or transmitted by the source ports is sent to the destination ports.

SPAN Configuration Guidelines

This section describes the guidelines for configuring SPAN:

- Use a network analyzer to monitor ports.
- For the SPAN source ports, SPAN is not supported with the ATM ports; it works with the Ethernet 10/100/1000-Mbps ports and 10-Gbps ports.
- When enabled, SPAN uses any previously entered configuration. If you have not entered any configuration commands, SPAN uses the default parameters.
- If you specify multiple SPAN source ports, the ports can belong to the different VLANs.
- See the “[SPAN, RSPAN and Mini Protocol Analyzer Session Limits](#)” section on page 49-5.
- The RSPAN sessions can coexist with the SPAN sessions within the SPAN/RSPAN limits that are described in the “[SPAN, RSPAN and Mini Protocol Analyzer Session Limits](#)” section on page 49-5.
- The optional **inpkts** keyword is disabled by default. Use the **inpkts** keyword with the optional **enable** keyword to allow the SPAN destination ports to receive the normal incoming traffic. Enter the optional **disable** keyword to prevent the SPAN destination ports from receiving the normal incoming traffic.
- When you enable the optional **inpkts** keyword, a warning message notifies you that the destination port does not support the Spanning Tree Protocol (STP) and may cause loops if you enable this option.
- Learning is enabled by default. Use the **inpkts** keyword with the optional **learning** keyword to enable or disable learning for a specific port.
- You can specify a Multilayer Switch Module (MSM) port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.
- When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.

- If any of the VLANs on the SPAN source port(s) are blocked by spanning tree, you may see extra packets that are transmitted on the destination port(s) that were not actually transmitted out the source port(s). The extra packets are sent through the switch fabric to the source port and are blocked by spanning tree at the source port.

**Caution**

In software releases before software release 8.4(1), if you used the **set span** command without the **create** keyword, and you had only one session configured, the session was overwritten. If two SPAN sessions were already configured, you received an error message. If a matching destination port existed, the particular session was overwritten (with or without specifying the **create** keyword). If you specified the **create** keyword and there was no matching destination port, the session was created.

In software release 8.4(1) and later releases, the **create** keyword has been removed from the **set span** command. When you enable a SPAN session without the **create** keyword, and another session is available, the first session is not overwritten.

Configuring SPAN from the CLI

To configure SPAN, you specify the source, the destination ports, the direction of the traffic through the source that you want to mirror to the destination ports, and if the destination port can receive the packets.

To configure a SPAN port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the SPAN source and destination ports.	set span { <i>src_mod/src_ports</i> <i>src_vlans</i> sc0 } { <i>dest_mod/dest_port</i> } [rx tx both] [session <i>session_number</i>] [inpkts { enable disable }] [learning { enable disable }] [multicast { enable disable }] [filter <i>vlans...</i>]
Step 2	Verify the SPAN configuration.	show span

**Caution**

If the SPAN destination port is connected to another device and you enable reception of the incoming packets (using the **inpkts enable** keywords), the SPAN destination port receives the traffic for whatever VLAN to which the SPAN destination ports belong. The SPAN destination port does *not* participate in spanning tree for that VLAN. Use caution when using the **inpkts** keyword to avoid creating network loops with the SPAN destination port or assigning the SPAN destination port to an unused VLAN.

This example shows how to configure SPAN so that both the transmit and receive traffic from port 1/1 (the SPAN source) is mirrored on port 2/1 (the SPAN destination):

```
Console> (enable) set span 1/1 2/1
```

```
Destination      : Port 2/1
Admin Source     : Port 1/1
Oper Source      : Port 1/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1

Destination      : Port 2/1
Admin Source     : VLAN 522
Oper Source      : Port 3/1-2
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/12 as the SPAN destination. Only the transmit traffic is monitored. The normal incoming packets on the SPAN destination port are allowed.

```
Console> (enable) set span 522 2/12 tx inpkts enable

Destination      : Port 2/12
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction       : transmit
Incoming Packets: enabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create

Destination      : Port 2/1
Admin Source     : port 3/1
Oper Source      : Port 3/1
Direction       : transmit/receive
Incoming Packets: disabled

Destination      : Port 2/2
Admin Source     : port 3/2
Oper Source      : Port 3/2
Direction       : transmit
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Console> (enable)
```

To disable SPAN, perform this task in privileged mode:

Task	Command
Disable SPAN on the switch.	set span disable [<i>dest_mod</i> / <i>dest_port</i> <i>all</i>]

This example shows how to disable SPAN on the switch:

```
Console> (enable) set span disable 2/1
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled port 2/1 to monitor transmit traffic of VLAN 522
Console> (enable)
```

Configuring RSPAN on the Switch

These sections describe how to configure RSPAN:

- [RSPAN Hardware Requirements](#), page 49-10
- [Understanding How RSPAN Works](#), page 49-10
- [RSPAN Configuration Guidelines](#), page 49-11
- [Configuring RSPAN](#), page 49-12
- [RSPAN Configuration Examples](#), page 49-15

RSPAN Hardware Requirements

The RSPAN supervisor engine requirements are as follows:

- For source switches—The Catalyst 6500 series switch with any of the following:
 - Supervisor Engine 1A and Policy Feature Card (PFC): WS-X6K-SUP1A-PFC
 - Supervisor Engine 1A, PFC, and Multilayer Switch Feature Card (MSFC): WS-X6K-SUP1A-MSFC
 - Supervisor Engine 1A, PFC, and MSFC2: WS-X6K-S1A-MSFC2
 - Supervisor Engine 2 and PFC2: WS-X6K-S2-PFC2
 - Supervisor Engine 1A, PFC, and MSFC2: WS-X6K-S1A-MSFC2
 - Supervisor Engine 720 with the following onboard components: Policy Feature Card 3A (PFC3A/PFC3B/PFC3BXL), Multilayer Switch Feature Card 3 (MSFC3), and integrated 720-Gbps switch fabric: WS-SUP720
 - Supervisor Engine 32, PFC3B/PFC3BXL, and MSFC2A: WS-SUP32-GE-3B
- For destination or intermediate switches—Any Cisco switch supporting RSPAN VLAN

No third party or other Cisco switches can be placed in the end-to-end path for RSPAN traffic.

Understanding How RSPAN Works



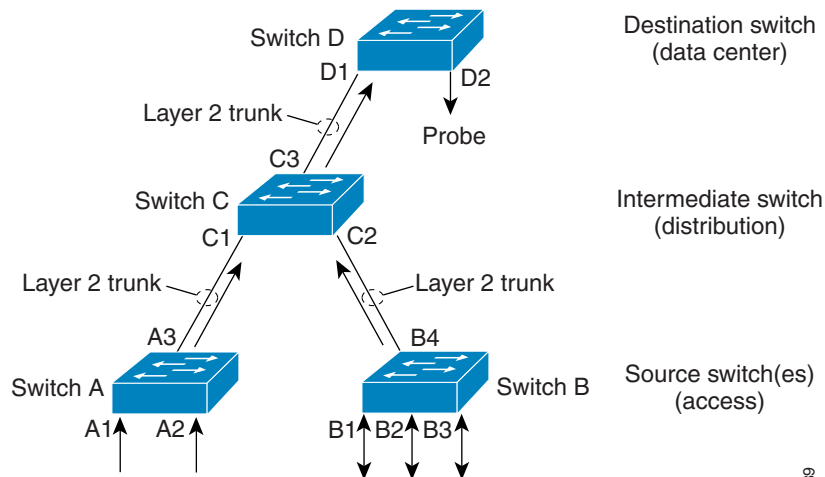
Note

See the [“Understanding How SPAN and RSPAN Work”](#) section on page 49-1 for the concepts and terminology that apply to both the SPAN and RSPAN configurations.

RSPAN has all the features of SPAN (see the [“Understanding How SPAN Works”](#) section on page 49-6), plus support for the source ports and the destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network (see [Figure 49-2](#)).

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 SPAN traffic from the sources, which cannot be in the RSPAN VLAN, is switched to the RSPAN VLAN and is forwarded to the destination ports that are configured in the RSPAN VLAN. The traffic type for the sources (ingress, egress, or both) in an RSPAN session can be different in the different source switches but is the same for all the sources in each source switch for each RSPAN session. Do not configure any ports in an RSPAN VLAN except those that are selected to carry the RSPAN traffic. Learning is disabled on the RSPAN VLAN.

Figure 49-2 RSPAN Configuration



RSPAN Configuration Guidelines

This section describes the guidelines for configuring RSPAN:



Tip

As RSPAN VLANs have special properties, we recommend that you reserve a few VLANs across your network for use as RSPAN VLANs. Do not assign an access port to these VLANs.



Tip

You can apply an output access control list (ACL) to the RSPAN traffic to selectively filter the specific flows. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.

- All the items in the “[SPAN Configuration Guidelines](#)” section on page 49-7 apply to RSPAN.
- The RSPAN sessions can coexist with the SPAN sessions within the SPAN/RSPAN limits that are described in the “[SPAN, RSPAN and Mini Protocol Analyzer Session Limits](#)” section on page 49-5.
- For the RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches.
- For RSPAN, trunking is required if you have a source switch with all the source ports in one VLAN (VLAN 2 for example) and it is connected to the destination switch through an uplink port that is also in VLAN 2. With RSPAN, the traffic is forwarded to the remote switches in the RSPAN VLAN. The RSPAN VLAN is configured only on trunk ports and not on access ports.
- The learning option applies to the RSPAN destination ports only.
- RSPAN does not support monitoring the BPDU packets or Layer 2 protocol packets such as Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP).
- To optimize the bandwidth utilization in the connecting links, you can configure the quality of service (QoS) parameters for the RSPAN VLAN in each of the participating source, intermediate, or destination switches.

- Each Catalyst 6500 series switch can source a maximum of one RSPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for the local ingress or bidirectional SPAN sessions is reduced to one. There are no limits on the number of RSPAN sessions that are carried across the network within the RSPAN session limits (see the “[SPAN, RSPAN and Mini Protocol Analyzer Session Limits](#)” section on page 49-5).
- The RSPAN VLANs cannot be included as the sources for the port-based RSPAN sessions when the source trunk ports have active RSPAN VLANs. Additionally, the RSPAN VLANs cannot be the sources in the VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN if these conditions are met:
 - The same RSPAN VLAN is used for an RSPAN session in all the switches.
 - All participating switches have the appropriate hardware and software.
 - No access port (including the sc0 interface) is configured in the RSPAN VLAN.
- If you enable VTP and VTP pruning, the RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of the RSPAN traffic across the network.
- If you enable the GARP VLAN Registration Protocol (GVRP) and the GVRP requests conflict with the existing RSPAN VLANs, you might observe unwanted traffic in the RSPAN sessions.
- You can use the RSPAN VLANs in Inter-Switch Link (ISL) to dot1q mapping. However, ensure that the special properties of RSPAN VLANs are supported in all the switches to avoid the unwanted traffic in these VLANs.

Configuring RSPAN

The first step in configuring an RSPAN session is to select an RSPAN VLAN for the RSPAN session that *does not* exist in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

Once the RSPAN VLAN is created, you configure the source and destination switches by entering the **set rspan** command.

To configure the RSPAN VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure the RSPAN VLANs.	set vlan <i>vlan</i> [rspan]
Step 2	Verify the RSPAN VLAN configuration.	show vlan

This example shows how to set VLAN 500 as an RSPAN VLAN and verify the configuration:

```

Console> (enable) set vlan 500 rspan
vlan 500 configuration successful
Console> (enable)
Console> (enable) show vlan
.
display truncated
.
VLAN DynCreated RSPAN
-----
1 static disabled
2 static disabled
3 static disabled
99 static disabled
500 static enabled
Console> (enable)

```

To configure the RSPAN source ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure the RSPAN source ports. Use this command on each of the source switches that participate in RSPAN.	set rspan source { <i>src_mod/src_ports...</i> <i>vlangs...</i> sc0 } { <i>rspan_vlan</i> } [rx tx both] session <i>session_number</i> [multicast { enable disable }] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify ports 4/1 and 4/2 as the ingress source ports for RSPAN VLAN 500:

```

Console> (enable) set rspan source 4/1-2 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : Port 4/1-2
Oper Source     : None
Direction      : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)

```

To configure the RSPAN source VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure the RSPAN source VLANs. All the ports in the source VLAN become the operational source ports.	set rspan source { <i>src_mod/src_ports...</i> <i>vlangs...</i> sc0 } { <i>rspan_vlan</i> } [rx tx both] session <i>session_number</i> [multicast { enable disable }] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify VLAN 200 as a source VLAN for RSPAN VLAN 500 (selecting the optional **rx** keyword makes all the ports in the VLAN ingress ports):

```
Console> (enable) set rspan source 200 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : VLAN 200
Oper Source     : None
Direction      : receive
Incoming Packets: -
Learning       : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

To configure the RSPAN destination ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure the RSPAN destination ports. Use this command on each of the destination switches that participate in RSPAN.	set rspan destination <i>mod/port</i> { <i>rspan_vlan</i> } session <i>session_number</i> [inpkts { enable disable }] [learning { enable disable }] [create]
Step 2	Verify the RSPAN configuration.	show rspan

```
Console> (enable) set rspan destination 3/1 500
Rspan Type      : Destination
Destination     : Port 3/1
Rspan Vlan      : 500
Admin Source    : -
Oper Source     : -
Direction      : -
Incoming Packets: disabled
Learning       : enabled
Multicast       : -
Filter          : -
Console> (enable)
```

To disable RSPAN, perform this task in privileged mode:

	Task	Command
	Disable RSPAN on the switch.	set rspan disable source [<i>rspan_vlan</i> all] set rspan disable destination [<i>mod/port</i> all]

This example shows how to disable all the enabled source sessions:

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

This example shows how to disable one source session by *rspan_vlan* number:

```
Console> (enable) set rspan disable source 903  
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.  
Console> (enable)
```

This example shows how to disable all the enabled destination sessions:

```
Console> (enable) set rspan disable destination all  
This command will disable all remote span destination session(s).  
Do you want to continue (y/n) [n]? y  
Disabled monitoring of remote span traffic for all rspan destination ports.  
Console> (enable)
```

This example shows how to disable one destination session by *mod/port*:

```
Console> (enable) set rspan disable destination 4/1  
Disabled monitoring of remote span traffic on port 4/1.  
Console> (enable)
```

RSPAN Configuration Examples

These sections describe how to configure RSPAN:

- [Configuring a Single RSPAN Session, page 49-15](#)
- [Modifying an Active RSPAN Session, page 49-16](#)
- [Adding the RSPAN Source Ports in Intermediate Switches, page 49-17](#)
- [Configuring Multiple RSPAN Sessions, page 49-17](#)
- [Adding Multiple Network Analyzers to an RSPAN Session, page 49-19](#)

Configuring a Single RSPAN Session

This example shows how to configure a single RSPAN session. [Figure 49-3](#) shows an RSPAN configuration; see [Table 49-2](#) for the commands to configure this RSPAN session. [Table 49-2](#) assumes that you have already set up RSPAN VLAN 901 for this session on all the switches using the **set vlan *vlan* rspan** command. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain. Note that in the configuration example shown in [Table 49-2](#), the RSPAN session may be disabled in Switch A or B or both without modifying the configuration in Switch C or Switch D.

Figure 49-3 Single RSPAN Session

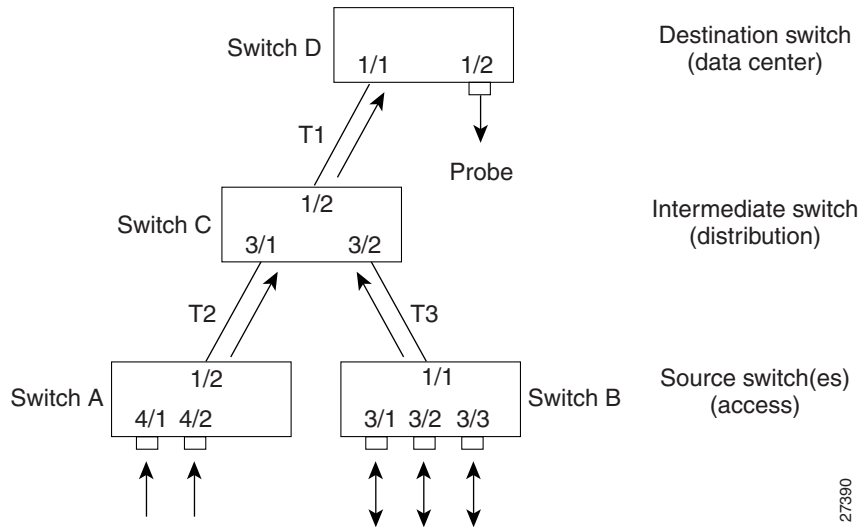


Table 49-2 Configuring a Single RSPAN Session

Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	set rspan source 4/1-2 901 rx
B (source)	3/1, 3/2, 3/3	901	Bidirectional	set rspan source 3/1-3 901
C (intermediate)	–	901	–	No RSPAN CLI command needed
D (destination)	1/2	901	–	set rspan destination 1/2 901

Modifying an Active RSPAN Session

This example shows how to modify an active RSPAN session. Use [Figure 49-3](#) for reference; see [Table 49-3](#) for the commands to disable an RSPAN session and to add or remove the source ports from an RSPAN session.

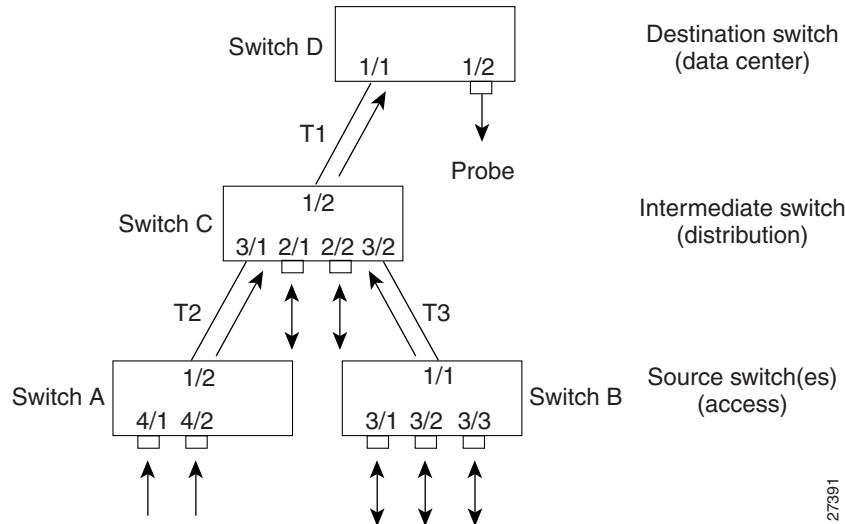
Table 49-3 Making Modifications to an Active RSPAN Session

Switch	Action	RSPAN CLI Commands
A (source)	Disable the RSPAN session.	set rspan disable source 901
B (source)	Remove source port 3/2 from the RSPAN session.	set rspan source 3/1, 3/3 901
B (source)	Add back source port 3/2 to the RSPAN session.	set rspan source 3/1-3 901

Adding the RSPAN Source Ports in Intermediate Switches

This example shows how to add the RSPAN source ports in the intermediate switches. Figure 49-4 shows an RSPAN configuration; see Table 49-4 for the commands to configure this RSPAN session. Ports 2/1-2 in Switch C can be configured for the same RSPAN session.

Figure 49-4 Adding the RSPAN Source Ports in Intermediate Switches



27391

Table 49-4 Adding the RSPAN Source Ports in Intermediate Switches

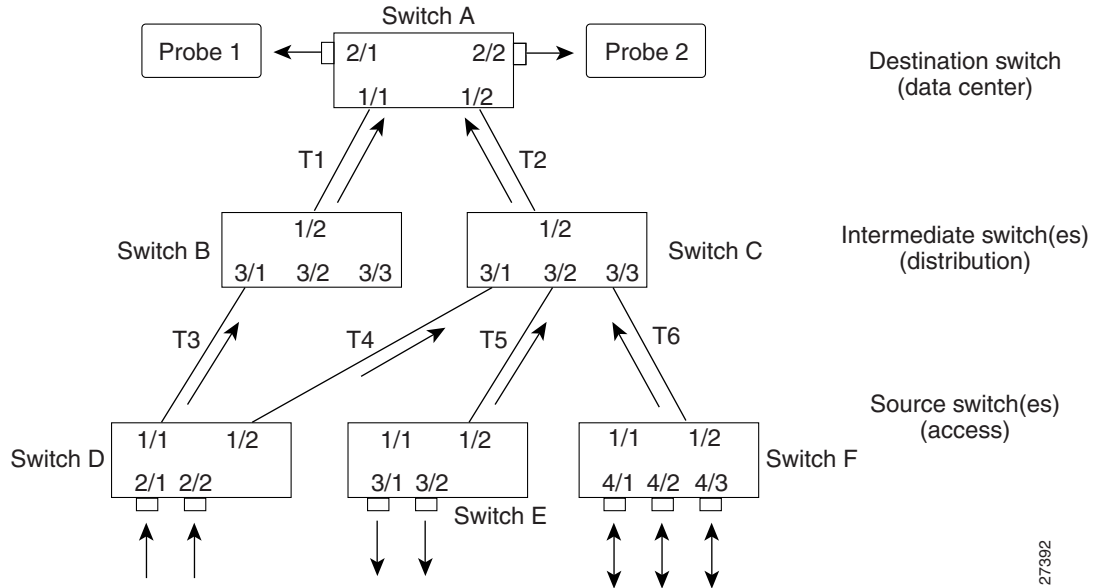
Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	set rspan source 4/1-2 901 rx
B (source)	3/1, 3/2, 3/3	901	Bidirectional	set rspan source 3/1-3 901
C (intermediate)	–	901	–	No RSPAN CLI command needed
C (source)	2/1, 2/2	901	Bidirectional	set rspan source 2/1-2 901
D (destination)	1/2	901	–	set rspan destination 1/2 901

Configuring Multiple RSPAN Sessions

This example shows how to configure multiple RSPAN sessions. Figure 49-5 shows an RSPAN configuration; see Table 49-5 for the configuration commands to configure this RSPAN session. This example is a typical scenario where the monitoring probes would be placed in the data center and the source ports in the access switches (other ports in any of the switches can also be configured for RSPAN). If there is no change in the route for the SPAN traffic, the destination switch and the intermediate switches need to be configured only once.

In Figure 49-5, two RSPAN sessions are used with RSPAN VLANs 901 (for probe 1) and 902 (for probe 2). The direction of traffic over trunks T1 through T6 is shown only for understanding; the direction of the trunks depends on the STP states of the trunks for the RSPAN VLAN(s). You need to configure the RSPAN VLANs in each of the switches for the RSPAN sessions. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in that VTP domain. With VTP disabled, create the RSPAN VLANs in each switch.

Figure 49-5 Configuring Multiple RSPAN Sessions



27392

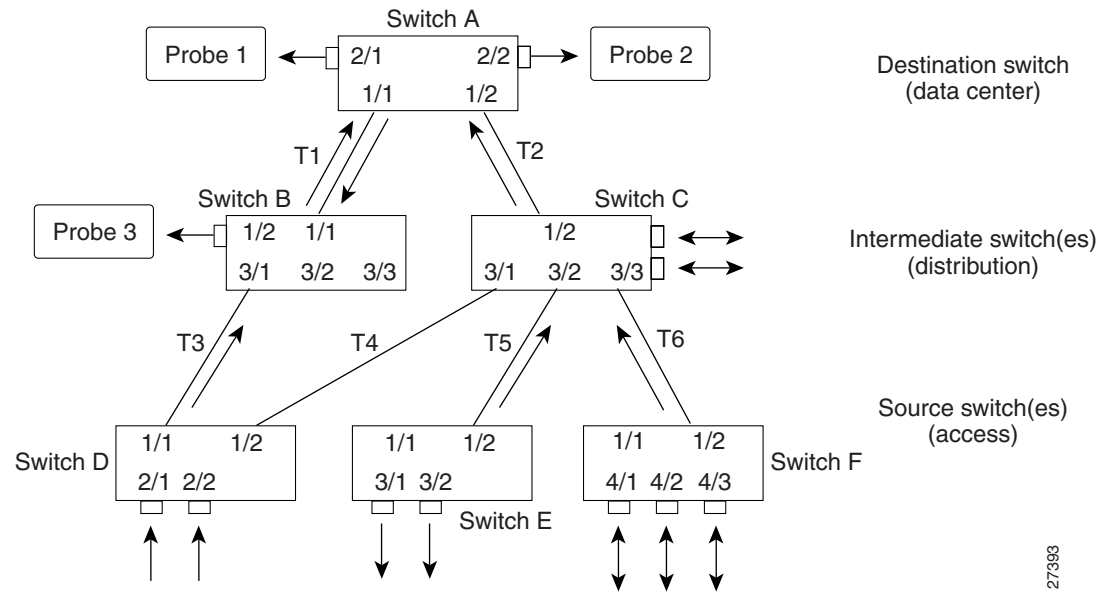
Table 49-5 Configuring Multiple RSPAN Sessions

Switch	Port	RSPAN VLAN(s)	Direction	RSPAN CLI Commands
A (destination)	2/1	901	–	set rspan destination 2/1 901
A (destination)	2/2	902	–	set rspan destination 2/2 902
B (intermediate)	–	901, 902	–	No RSPAN CLI command needed
C (intermediate)	–	901, 902	–	No RSPAN CLI command needed
D (source)	2/1-2	901	Ingress	set rspan source 2/1-2 901 rx
E (source)	3/1-2	901	Egress	set rspan source 3/1-2 901 tx
F (source)	4/1-3	902	Both	set rspan source 4/1-3 902

Adding Multiple Network Analyzers to an RSPAN Session

You can attach multiple network analyzers (probes) to the same RSPAN session. For example, in [Figure 49-6](#), you can add probe 3 in Switch B to monitor RSPAN VLAN 901 using the `set rspan destination 1/2 901` command. Similarly, you could add the source ports to Switch C.

Figure 49-6 Adding Multiple Probes to an RSPAN Session



27383

Configuring the Mini Protocol Analyzer on the Switch

These sections describe how to configure the Mini Protocol Analyzer on the switch:

- [Mini Protocol Analyzer Hardware Requirements](#), page 49-19
- [Understanding How the Mini Protocol Analyzer Works](#), page 49-19
- [Mini Protocol Analyzer Configuration Guidelines](#), page 49-20
- [Configuring the Mini Protocol Analyzer from the CLI](#), page 49-21

Mini Protocol Analyzer Hardware Requirements

Supervisor Engine 720 and Supervisor Engine 32 support the Mini Protocol Analyzer.

Understanding How the Mini Protocol Analyzer Works

A Mini Protocol Analyzer session mirrors the traffic from a single source port. The source port can be either an access port or a trunk port.

The Mini Protocol Analyzer does not affect the switching of network traffic on the source port. A copy of the packets that are received and transmitted by the source port is sent over the backplane where the copies are stored as a file in the Flash memory of the switch. The file can be stored in the following places:

- For the Supervisor Engine 720: bootflash (default), disk0, or disk1
- For the Supervisor Engine 32: bootdisk (default) or disk0

When a Mini Protocol Analyzer session starts (when you enter the **set packet-capture start** command), the session monitors the source port traffic and stores it on the flash memory until one of the following conditions occur:

- You enter the **set packet-capture stop** command to end the Mini Protocol Analyzer session.
- The number of packets as specified by the **set packet-capture limit** command is reached. A system message is displayed and the Mini Protocol Analyzer session ends.
- The flash device runs out of memory. A system message is displayed and the Mini Protocol Analyzer session ends.

Mini Protocol Analyzer Configuration Guidelines

This section describes the guidelines for configuring the Mini Protocol Analyzer:

- Ensure that your flash memory has enough space to store the output file from the Mini Protocol Analyzer session, or specify filters that limit the size of the output file.
- You use Ethernet 10/100/1000-Mbps ports and 10-Gbps ports as Mini Protocol Analyzer source ports. You cannot use ATM ports, MSFC ports, or service module ports as Mini Protocol Analyzer source ports.
- When enabled, the Mini Protocol Analyzer uses any previously entered configuration. If you have not entered any configuration commands, the Mini Protocol Analyzer uses the default parameters.
- Only one Mini Protocol Analyzer session is allowed on the switch at one time. See the [“SPAN, RSPAN and Mini Protocol Analyzer Session Limits” section on page 49-5](#) for switch-wide limitations regarding SPAN, RSPAN, and the Mini Protocol Analyzer. One Mini Protocol Analyzer session counts as one SPAN session.
- A maximum of 16 filters can be run on the traffic that is being monitored in a Mini Protocol Analyzer session. The **set packet-capture snap-length** command, which specifies the length to which packets are truncated, is not counted against the maximum number of filters. Entering the **clear packet-capture filter** or **clear packet-capture all** command removes all filters.
- If you have saved a file on the flash memory from one Mini Protocol Analyzer session and you start another Mini Protocol Analyzer session with the same output filename, the existing information from the previous Mini Protocol Analyzer session is overwritten. Multiple output files can be stored on the flash memory if the output filenames are different.
- The file system in the flash memory is locked and cannot be modified or accessed while the Mini Protocol Analyzer session is running.
- Because the Mini Protocol Analyzer sends the copied traffic from the source port over the backplane, the performance of your switch might be affected if the source port is processing a large amount of traffic.

- If your switch performance is adversely affected by the amount of traffic that is being processed during a Mini Protocol Analyzer session, the CPU of the switch can become overloaded and cause the copied packets to drop or the control packets, such as the Bridge Protocol Data Units (BPDUs), to drop. If the switch becomes extremely overloaded, you cannot stop the Mini Protocol Analyzer session.
- High Availability (HA) is supported with the Mini Protocol Analyzer. However, if you perform a soft or hard reboot of the switch and a Mini Protocol Analyzer session is in progress, the Mini Protocol Analyzer session will not continue after the reboot until you enter the **set packet-capture start** command.
- You cannot view the copied traffic from a Mini Protocol Analyzer session on the system console. You can only save the copied traffic to a file on the switch's flash memory and view the file using the Ethernet Network Protocol Analyzer.
- You cannot capture Ethernet Out-of-Band Channel (EOBC) traffic with the Mini Protocol Analyzer.
- If any VLAN on the Mini Protocol Analyzer source port is blocked by spanning tree, you might see extra packets that are saved on the flash memory that were not actually transmitted out the source port. The extra packets are sent through the switch fabric to the flash memory and are blocked by spanning tree at the source port.

Configuring the Mini Protocol Analyzer from the CLI

To configure the Mini Protocol Analyzer, you specify the source port and, optionally, the name of the output file to which the copied packets will be written.

To monitor a source port using the Mini Protocol Analyzer, perform this task in privileged mode:

	Task	Command
Step 1	Configure the source port for the Mini Protocol Analyzer session.	set packet-capture <i>mod/port</i>
Step 2	(Optional) Specify the location and filename of the output file for the Mini Protocol Analyzer session. Note The default filename is bootflash:eth_yymmdd-hhmmss where yymmdd-hhmmss is the year, month, day, hour, minute, and second when the Mini Protocol Analyzer session was started.	set packet-capture dump-file <i>device:filename</i>
Step 3	(Optional) Specify the filtering criteria for the source or destination IP or MAC addresses.	set packet-capture filter { source destination } { ip mac }
Step 4	(Optional) Specify the direction of the traffic to be captured as either receive (rx), transmit (tx), or both . rx is the default.	set packet-capture direction { rx tx both }
Step 5	(Optional) Specify the length to which the packets that are captured by the Mini Protocol Analyzer session are truncated. Note The range is 0 to 10258 bytes.	set packet-capture snap-length <i>packet-length</i>

	Task	Command
Step 6	(Optional) Specify the total number of packets that are captured by the Mini Protocol Analyzer session. Note The range is 0 to 32,000 packets. The default is 1,000 packets.	set packet-capture limit <i>packet-number</i>
Step 7	Verify the Mini Protocol Analyzer configuration.	show packet-capture
Step 8	Start the Mini Protocol Analyzer session.	set packet-capture start

This example shows how to configure the Mini Protocol Analyzer so that all traffic that is sent and received from port 5/1 is copied to a file on the bootflash memory called port_5_1_stats:

```
Console> (enable) set packet-capture 5/1
Capturing port set to 5/1.
Console> (enable) set packet-capture dump-file bootflash:port_5_1_stats
Packet capture dump file name set to bootflash:port_5_1_stats.
```

The date and time when the Mini Protocol Analyzer session is started will be appended to the output filename. For example, if the Mini Protocol Analyzer session was started July 28, 2008 at 4:54:08 p.m. Greenwich Mean Time (GMT), the filename for the previous example would be port_5_1_stats_080728-165408.

This example shows how to specify that only traffic that has either a destination address of 10.1.1.2 or a destination address of 10.1.1.3 will be captured:

```
Console> (enable) set packet-capture filter destination ip 10.1.1.2
Successfully added the filter string.
Console> (enable) set packet-capture filter destination ip 10.1.1.3
Successfully added the filter string.
```

This example shows how to specify the direction of the traffic to be captured:

```
Console> (enable) set packet-capture direction tx
Packets from transmit (tx) direction will be captured.
```

This example shows how to specify that all packets will be captured but packets that have a length of 5,000 bytes or larger will be truncated to 5,000 bytes:

```
Console> (enable) set packet-capture snap-length 5000
Packets captured will be truncated to 5000 bytes.
```

This example shows how to specify that 500 packets will be captured during the Mini Protocol Analyzer session. After 500 packets have been captured, the Mini Protocol Analyzer session will end.

```
Console> (enable) set packet-capture limit 500
Packet capture number set to 500.
```

This example shows how to verify the configuration of the Mini Protocol Analyzer:

```
Console> (enable) show packet-capture
Packet-capture parameter      Value
-----
Operational Status            Not-running
Dump File Name                 bootflash:port_5_1_stats
Direction                      rx
Filter - Source IP             None
Filter - Destination IP        host 10.1.1.2/32,10.1.1.3/32
Filter - Source MAC address    None
Filter - Destination MAC address None
Number of packets to capture    500
Packet Snap Length             5000
```

```
Source Port          5/1
Bytes Captured      7
```

This example shows how to start the Mini Protocol Analyzer session:

```
Console> (enable) set packet-capture start
Packet capturing can result in protocol packets(STP, UDLD, PAGP, etc.)
getting dropped resulting in network instability. Also, it can affect
system performance or inband connectivity as sc0/sc1 interface packets
can be dropped without warning
Do you want to continue(y/n) [n]? y
Console> (enable) 2006 Jul 28 16:54:08 %SYS-5-SPAN_CFGSTATECHG:local span sessio
n active for session Number 1
2006 Jul 28 16:54:08 %SYS-5-PKTCAP_START:Packet capture session active
2006 Jul 28 16:55:34 %SYS-5-PKTCAP_STOPPKT:Packet capture session ended after ca
pturing 300 packets
2006 Jul 28 16:55:34 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for ses
sion Number 1
CCCCCCCCCCCCCCC
```

