CHAPTER 56

Using the Mini Protocol Analyzer

This chapter describes how to use the Mini Protocol Analyzer on the Cisco 7600 series routers. Release 12.2(33)SRD and later releases support the Mini Protocol Analyzer feature.

Note For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Master Command List, All Releases* at this URL:

This chapter consists of these sections:

Understanding How the Mini Protocol Analyzer Works

The Mini Protocol Analyzer captures network traffic from a SPAN session and stores the captured packets in a local memory buffer. Using the provided filtering options, you can limit the captured packets to:

- Packets from selected VLANs, ACLs, or MAC addresses.
- Packets of a specific EtherType
- Packets of a specified packet size

You can start and stop the capture using immediate commands, or you can schedule the capture to begin at a specified date and time.

The captured data can be displayed on the console, stored to a local file system, or exported to an external server using normal file transfer protocols. The format of the captured file is libpcap, which is supported by many packet analysis and sniffer programs. Details of this format can be found at the following URL:

http://www.tcpdump.org/

By default, only the first 68 bytes of each packet are captured.

Configuring the Mini Protocol Analyzer

To configure a capture session using the Mini Protocol Analyzer, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] monitor session number type capture`	Configures a SPAN session number with packets directed to the processor for capture. Enters capture session configuration mode. The session number range is 1 to 80. The **no** prefix removes the session.
Step 3	`Router(config-mon-capture)# buffer-size buf_size`	(Optional) Sets the size in KB of the capture buffer. The range is 32-65535 KB; the default is 2048 KB.
Step 4	`Router(config-mon-capture)# description session_description`	(Optional) Describes the capture session. The description can be up to 240 characters and cannot contain special characters. If the description contains spaces, it must be enclosed in quotation marks(“”).
Step 5	`Router(config-mon-capture)# rate-limit pps`	(Optional) Sets a limit on the number of packets per second (*pps*) that can be captured. The range is 10-100000 packets per seconds; the default is 10000 packets per second.
Step 6	`Router(config-mon-capture)# source {{interface {single_interface | interface_list | interface_range | mixed_interface_list} | port-channel channel_id}} | {vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}}[rx | tx | both]`	Associates the capture session with source ports or VLANs, and selects the traffic direction to be monitored. The default traffic direction is both.
Step 7	`Router(config-mon-capture)# exit`	Exits the capture session configuration mode.

When configuring a capture session, note the following information:

- Only one capture session is supported; multiple simultaneous capture sessions cannot be configured.
- The **source interface** command argument is either a single interface, or a range of interfaces described by two interface numbers (the lesser one first, separated by a dash), or a comma-separated list of interfaces and ranges.

Note When configuring a source interface list, you must enter a space before and after the comma. When configuring a source interface range, you must enter a space before and after the dash.

- The **source vlan** command argument is either a single VLAN number from 1 through 4094 (except reserved VLANs), or a range of VLANs described by two VLAN numbers (the lesser one first, separated by a dash), or a list of VLANs and ranges.

Note When configuring a source VLAN list, do not enter a space before or after the comma. When configuring a source VLAN range, do not enter a space before or after the dash. Note that this requirement differs from the requirement for source interface lists and ranges.

- Data capture does not begin when the capture session is configured. The capture is started by the **monitor capture start** or **monitor capture schedule** command described in the "Starting and Stopping a Capture" section on page 56-4.
- Although the capture buffer is linear by default, it can be made circular as a run-time option in the **monitor capture start** or **monitor capture schedule** command.
- When no hardware rate limit registers are available, the capture session is disabled.
- The source VLAN cannot be changed if a VLAN filter is configured. Remove any VLAN filters before changing the source VLAN.

Filtering the Packets to be Captured

Several options are provided for filtering the packets to be captured. Filtering by ACL and VLAN is performed in hardware before any rate-limiting is applied; all other filters are executed in software. Software filtering can decrease the capture rate.

To filter the packets to be captured by the Mini Protocol Analyzer, perform this task in capture session configuration mode:

	Command	Purpose
Step 1	`Router(config-mon-capture)# [no] filter access-group {acl_number | acl_name}`	(Optional) Captures only packets from the specified ACL.
Step 2	`Router(config-mon-capture)# [no] filter vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}`	(Optional) Captures only packets from the specified source VLAN or VLANs.
Step 3	`Router(config-mon-capture)# [no] filter ethertype type`	(Optional) Captures only packets of the specified EtherType. The *type* can be specified in decimal, hex, or octal.
Step 4	`Router(config-mon-capture)# [no] filter length min_len [max_len]`	(Optional) Captures only packets whose size is between *min_len* and *max_len,* inclusive. If *max_len* is not specified, only packets of exactly size *min_len* will be captured. The range for *min_len* is 0 to 9216 bytes and the range for *max_len* is 1 to 9216 bytes.
Step 5	`Router(config-mon-capture)# [no] filter mac-address mac_addr`	(Optional) Captures only packets from the specified MAC address.
Step 6	`Router(config-mon-capture)# end`	Exits the configuration mode.

When configuring capture filtering, note the following information:

- The **filter vlan** argument is either a single VLAN number from 1 through 4094 (except reserved VLANs), or a range of VLANs described by two VLAN numbers (the lesser one first, separated by a dash), or a list of VLANs and ranges.

Note When configuring a filter VLAN list, you must enter a space before and after the comma. When configuring a filter VLAN range, you must enter a space before and after the dash. Note that this requirement differs from the requirement for source VLAN lists and ranges described in the preceding section.

- To enter an EtherType as a decimal number, enter the number (1 to 65535) with no leading zero. To enter a hexadecimal number, precede four hexadecimal characters with the prefix 0x. To enter an octal number, enter numeric digits (0 to 7) with a leading zero. For example, the 802.1Q EtherType can be entered in decimal notation as 33024, in hexadecimal as 0x8100, or in octal as 0100400.
- Enter a MAC address as three 2-byte values in dotted hexadecimal format. An example is 0123.4567.89ab.
- The **no** keyword removes the filter.

Note After removing a VLAN filter using the **no** keyword, you must exit configuration mode, reenter the capture configuration mode, and issue the **source vlan** command before making other capture configuration changes.

- When you configure a VLAN filter, the capture source or destination must be a VLAN. When you configure a port filter, the capture source or destination must be a port.

Starting and Stopping a Capture

The commands to start and stop a capture are not stored as configuration settings. These commands are executed from the console in EXEC mode. You can start a capture immediately or you can set a future date and time for the capture to start. The capture ends when one of the following conditions occurs:

- A stop or clear command is entered from the console.
- The capture buffer becomes full, unless it is configured as a circular buffer.
- The optionally specified number of seconds has elapsed.
- The optionally specified number of packets has been captured.

When the capture stops, the SPAN session is ended and no further capture session packets are forwarded to the processor.

When starting a packet capture, you have the option to override some configured settings.

To start, stop, or cancel a capture, perform this task:

	Command	Purpose
Step 1	`Router# monitor capture [buffer size buf_size][length cap_len][linear | circular][filter acl_number | acl_name] {start [for count (packets | seconds)] | schedule at time date}`	Starts a capture with optional run-time configuration changes. The capture can start immediately or it can start at a specified time and date. • The **buffer size** option overrides the configured or default capture buffer size. • The **length** option determines the number of bytes that will be captured from each packet. The range for *cap_len* is 0 to 9216 bytes; the default is 68 bytes. A value of 0 causes the entire packet to be captured. • The **circular** option specifies that the capture buffer will overwrite earlier entries once it fills. The **linear** option specifies that the capture will stop when the buffer fills. The default is **linear**. • The **filter** option applies the specified ACL. • The **for** option specifies that the capture will end after the specified number of seconds has elapsed or the specified number of packets has been captured.
Step 2	`Router# monitor capture stop`	Stops the capture.
Step 3	`Router# monitor capture clear [filter]`	Clears any run-time configuration settings, clears any pending scheduled capture, and clears the capture buffer. The **filter** option clears only the run-time filter settings.

When using these commands, note the following information:

- The format for *time* and *date* is hh:mm:ss dd mmm yyyy. The hour is specified in 24-hour notation, and the month is specified by a three-letter abbreviation. For example, to set a capture starting time of 7:30 pm on October 31, 2006, use the notation 19:30:00 31 oct 2006. The time zone is GMT.
- When you specify a capture filter ACL in the start command, the new ACL will not override any configured ACLs. The new ACL will execute in software.

Displaying and Exporting the Capture Buffer

To display the captured packets or information about the capture session, or to export the captured packets for analysis, perform this task:

	Command	Purpose
Step 1	`Router# show monitor capture`	Displays the capture session configuration.
Step 2	`Router# show monitor capture status`	Displays the capture session state, mode, and packet statistics.
Step 3	`Router# show monitor capture buffer [start [end]] [detail][dump [nowrap [dump_length]] [acl acl_number | acl_name]]`	Displays the capture buffer contents. • The *start* and *end* parameters specify packet number indices in the capture buffer. When a *start* index is specified with no *end* index, only the single packet at the *start* index is displayed. When both the *start* and *end* indices are specified, all packets between these indices are displayed. The range is 1 to 4294967295. • The **detail** option adds expanded and formatted protocol and envelope information for each packet, including the packet arrival time. • The **dump** option displays the hexadecimal contents of the packet. If *nowrap* is specified with *dump_length*, one line of hexadecimal packet content of *dump_length* characters will be displayed for each packet. If *dump_length* is not specified, a line of 72 characters will be displayed. The range of *dump_length* is 14 to 256. • The **acl** option causes the display of only those packets that match the specified ACL.
Step 4	`Router# show monitor capture buffer [start [end]] brief [acl acl_number | acl_name]`	Displays only packet header information.
Step 5	`Router# monitor capture export buffer url`	Copies the contents of the capture buffer to the specified file system or file transfer mechanism.

Mini Protocol Analyzer Configuration, Operation, and Display Examples

This section provides examples for configuring the Mini Protocol Analyzer, for starting and stopping a capture session, and for displaying the results of a capture session.

General Configuration Examples

This example shows how to minimally configure the Mini Protocol Analyzer:

```
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# end

Router# show mon cap
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

This example shows how to configure the buffer size, session description, and rate limit:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# buffer-size 4096
Router(config-mon-capture)# description “Capture from ports, no filtering.”
Router(config-mon-capture)# rate-limit 20000
Router(config-mon-capture)# end
Router#
Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x807
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

This example shows how to configure the source as a mixed list of ports:

```
Router(config-mon-capture)# source interface gig 3/1 - 3 , gig 3/5
```

This example shows how to configure the source as a mixed list of VLANs:

```
Router(config-mon-capture)# source vlan 123,234-245
```

Filtering Configuration Examples

This example shows how to configure for capturing packets with the following attributes:

- The packets belong to VLANs 123 or 234 through 245
- The packets are of 802.1Q EtherType (hexadecimal 0x8100, decimal 33024)
- The packet size is exactly 8192 bytes
- The source MAC address is 01:23:45:67:89:ab
- The packets conform to ACL number 99

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# source vlan 123,234-245
Router(config-mon-capture)# filter ethertype 0x8100
Router(config-mon-capture)# filter length 8192
Router(config-mon-capture)# filter mac-address 0123.4567.89ab
Router(config-mon-capture)# filter access-group 99
Router(config-mon-capture)# end

Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x7E07
Capture vlan       : 1019
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68
Sw Filters          :
     ethertype   : 33024
     src mac     : 0123.4567.89ab
  Hw  acl          : 99

Router# show monitor session 1
Session 1
---------
Type                   : Capture Session
Description            : capture from ports
Source VLANs           :
    Both               : 123,234-245
Capture buffer size    : 4096 KB
Capture rate-limit
             value     : 20000
Capture filters        :
     ethertype         : 33024
     src mac           : 0123.4567.89ab
     acl               : 99

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Distributed (default)
```

```
Router#
```

This example shows how to capture packets whose size is less than 128 bytes:

```
Router(config-mon-capture)# filter length 0 128
```

This example shows how to capture packets whose size is more than 256 bytes:

```
Router(config-mon-capture)# filter length 256 9216
```

Operation Examples

This example shows how to start and stop a capture:

```
Router# monitor capture start
Router# monitor capture stop
Router#
```

This example shows how to start a capture to end after 60 seconds:

```
Router# monitor capture start for 60 seconds
Router#
```

This example shows how to start a capture at a future date and time:

```
Router# monitor capture schedule at 11:22:33 30 jun 2008
capture will start at : <11:22:33 UTC Mon Jun 30 2008>  after 32465825 secs
Router#
```

This example shows how to start a capture with options to override the buffer size and to change to a circular buffer:

```
Router# monitor capture buffer size 65535 circular start
Router#
```

This example shows how to export the capture buffer to an external server and a local disk:

```
Router# monitor capture export buffer tftp://server/user/capture_file.cap
Router# monitor capture export buffer disk1:capture_file.cap
```

Display Examples

These examples show how to display configuration information, session status, and capture buffer contents.

Displaying the Configuration

To display the capture session configuration, enter the **show monitor capture** command.

```
Router# show monitor capture
Capture instance [1] :
=====================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
```

```
capture state      : OFF
capture mode       : Linear
capture length     : 68
```

This example shows how to display more details using the **show monitor session** *n* command:

```
Router# show monitor session 1
Session 1
---------
Type                   : Capture Session
Source Ports           :
    Both               : Gi3/1-3,Gi3/5
Capture buffer size    : 32 KB
Capture filters        : None

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Distributed (default)
```

This example shows how to display the full details using the **show monitor session** *n* **detail** command:

```
Router# show monitor session 1 detail
Session 1
---------
Type                   : Capture Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Gi3/1-3,Gi3/5
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
Dest RSPAN VLAN        : None
Source IP Address      : None
Source IP VRF          : None
Source ERSPAN ID       : None
Destination IP Address : None
Destination IP VRF     : None
Destination ERSPAN ID  : None
Origin IP Address      : None
IP QOS PREC            : 0
IP TTL                 : 255
Capture dst_cpu_id     : 1
Capture vlan           : 0
Capture buffer size    : 32 KB
Capture rate-limit
             value     : 10000
Capture filters        : None

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Distributed (default)
```

Displaying the Capture Session Status

To display the capture session status, enter the **show monitor capture status** command.

```
Router# show monitor capture status
capture state      : ON
capture mode       : Linear
Number  of packets
          received : 253
           dropped : 0
          captured : 90
```

Displaying the Capture Buffer Contents

To display the capture session contents, enter the **show monitor capture buffer** command. These examples show the resulting display using several options of this command:

```
Router# show monitor capture buffer
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
 6     IP: s=10.12.0.1 , d=224.0.0.10, len 60


Router# show monitor capture buffer detail
 1      Arrival time : 09:44:30 UTC Fri Nov 17 2006
        Packet Length : 74 , Capture Length : 68
        Ethernet II :  0100.5e00.000a  0008.a4c8.c038  0800
        IP: s=10.12.0.5 , d=224.0.0.10, len 60, proto=88
 2      Arrival time : 09:44:31 UTC Fri Nov 17 2006
        Packet Length : 346 , Capture Length : 68
346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757463031


Router# show monitor capture buffer dump
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
08063810:                       0100 5E00000A            ..^...
08063820: 0008A4C8 C0380800 45C0003C 00000000  ..$H@8..E@.<....
08063830: 0258CD8F 0A0C0005 E000000A 0205EE6A  .XM.....`.....nj
08063840: 00000000 00000000 00000000 00000064  ...............d
08063850: 0001000C 01000100 0000000F 0004      ..............
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757465720415
 3     60    0180.c200.0000  0004.c099.06c5  0026 4242030000000000800000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 0001080006040001001244
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
0806FCB0:                       0100 5E000005            ..^...
0806FCC0: 0015C7D7 AC000800 45C00074 00000000  ..GW,...E@.t....
0806FCD0: 01597D55 07005417 E0000005 0201002C  .Y}U..T.`......,
0806FCE0: 04040404 00000000 00000002 00000010  ................
0806FCF0: 455D8A10 FFFF0000 000A1201 0000      E]............


Router# show monitor capture buffer dump nowrap
 1     74    0100.5e00.000a  0008.a4c8.c038  0800 45C0003C000000
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7574
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060400
```