Cisco IOS Embedded Packet Capture Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

monitor capture through show monitor capture

monitor capture

To enable and configure monitor packet capturing, use the the **monitor capture** privileged EXEC mode command. To disable monitor packet capturing, use the **no** form of this command.

monitor capture [**buffer size** *size*] [**circular**| **linear**] **[dot1q]** [**filter** *acl-num*| *exp-acl-num*| *acl-name*] [**length** *bytes*] {**clear [filter]**| **export buffer** *location*| **schedule at** *hh* **:** *mm* **:** *ss* [*date* [*month year*]]| **start** [**for** *number* {**seconds**| **packets**}]| **stop**}

no monitor capture [**buffer size** *size*] [**circular**| **linear**] **[dot1q]** [**filter** *acl-num*| *exp-acl-num*| *acl-name*] [**length** *bytes*] [**clear [filter]**| **export buffer** *location*| **schedule at** *hh* **:** *mm* **:** *ss* [*date* [*month year*]]]

Syntax Description

buffer size *size*	Specifies the capture buffer size in kilobytes. Range: 32 to 65535. Default: 2048 Kb.
circular | **linear**	Specifies a circular or linear capture buffer. The default is linear.
clear	Clears the capture buffer and sets the number of captured packets to zero.
dot1q	Includes dot1q information in the monitor capturing.
export buffer	Exports to remote location.
filter	Specifies that packets from a specified ACLs only are sent to the capture buffer.
acl-num	IP access list (standard or extended). Range: 1 to 199.
exp-acl-num	IP expanded access list (standard or extended). Range: 1300 to 2699.
acl-name	ACL name.
length *size*	Specifies the capture length of each packet in bytes. Range: 0 to 9216. Default: 68.

location	Location to dump capture buffer. Valid values are as follows: • **dot1q** *location* --Specifies the dot1q capture buffer location. • **bootflash:** --Location to dump buffer. • **disk0:** --Location to dump buffer. • **ftp:** --Location to dump buffer. • **http:** --Location to dump buffer. • **https:** --Location to dump buffer. • **rcp:** --Location to dump buffer. • **scp:** --Location to dump buffer. • **sup-bootdisk:** --Location to dump buffer. • **tftp:** --Location to dump buffer.
schedule at	Schedules the capture at a specific time/date.
hh **:** *mm* **:** *ss*	Time in hours:minutes:seconds. Range: hours: 0 to 23; minutes: 0 to 59; seconds: 0 to 59.
date	(Optional) Date. Range: 1 to 31.
month	(Optional) Month. Range: 1 to 12.
start	Starts capturing the packets to the beginning of the buffer.
for	(Optional) Specifies the length of time in seconds or the number of packets.
number	Stops the capture after the specified number of seconds or packets. Range: 1 to 4294967295.
stop	Moves the capture to the OFF state.

Command Default

Capture buffer is disabled by default.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

The **buffer size** *size* keywords and argument defines the buffer size that is used to store the packet.

The **length** *size* keyword and argument copies the specified number of bytes of data from each packet. The default setting of 68 bytes is adequate for IP, ICMP, TCP, and UDP. If you set the length to 0, the whole packet is copied to the buffer.

The **linear** capture buffer mode specifies that capture stops when the end of the capture buffer is reached. In the **circular** capture buffer mode, the capture will begin to overwrite earlier entries when the capture buffer becomes full. Changing the buffer mode or the buffer length automatically stops the capture.

If the ACL specified is configured, it is used for applying the filter in the software. 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.

If you configure the capture schedule, the capture schedule stops the capture start for the specified future time. This is the same as manually starting a capture at the specified time. If any capture is already running, that capture is stopped and the buffer is cleared.

The format for **time** and **date** is *hh:mm:ss dd mmm yyyy*. The time zone is GMT. 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, 2008, use the notation 19:30:00 31 oct 2008.

If you do not enter the **start** or **stop** keyword, the capture buffer is initialized and set in the OFF state.

If you enter the **no monitor capture** command without entering any keywords or arguments, capture is stopped and the capture buffer is deleted. After entering the **no** form of the monitor capture command, the capture buffer cannot be displayed or exported. If you specify the *length* or **buffer size** with the **no monitor capture** command, the capture is not deleted and the length or buffer size is set to the default values. The **start** and **stop** keywords are not valid with the **no monitor capture** command.

To clear the EXEC configurations or any capture schedules, enter the **clear** keyword. The **clear** keyword clears the capture buffer and sets the number of captured packets to zero.

Examples

This example shows how to configure the capture length initially before starting the capture:

```
Router# monitor capture length 128

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

This example shows how to start a new capture with non-default values:

```
Router# monitor capture length 100 circular start
Router# monitor capture stop
```

Related Commands

Command	Description
show monitor capture	Displays the capture buffer contents.

monitor capture (access list/class map)

To configure a monitor capture specifying an access list or a class map as the core filter for the packet capture, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified access list or class map as the core filter, use the **no** form of this command.

monitor capture *capture-name* {**access-list** *access-list-name* | **class-map** *class-map-name*}

no monitor capture *capture-name* {**access-list** *access-list-name* | **class-map** *class-map-name*}

Syntax Description

capture-name	The name of the capture.
access-list *access-list-name*	Configures an access list with the specified name.
class-map *class-map-name*	Configures a class map with the specified name.

Command Default

A monitor capture with the specified access list or a class map as the core filter for the packet capture is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Configure the access list using the **ip access-list** command or the class map using the **class-map** command before using the **monitor capture** command. You can specify a class map, or an access list, or an explicit inline filter as the core filter. If you have already specified the filter when you entered the **monitor capture match** command, the command replaces the existing filter.

Examples

The following example shows how to define a core system filter using an existing access control list:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

The following example shows how to define a core system filter using an existing class map:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

Related Commands

Command	Description
class-map	Configures a class map.
ip access-list	Configures an access list.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
monitor capture (interface/control plane)	Specifies attachment points with direction.
monitor capture match	Defines an explicit inline core filter.
permit	Sets conditions in a named IP access list.
show monitor capture	Displays packet capture details.

monitor capture (interface/control plane)

To configure monitor capture specifying an attachment point and the packet flow direction, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction, use the **no** form of this command.

monitor capture *capture-name*{**interface** *type number* | **control-plane**} {**in**| **out**| **both**}

no monitor capture *capture-name*{**interface** *type number* | **control-plane**} {**in**| **out**| **both**}

Syntax Description

capture-name	Name of the capture.
interface *type number*	Configures an interface with the specified type and number as an attachment point.
control-plane	Configures a control plane as an attachment point.
in	Specifies the inbound traffic direction.
out	Specifies the outbound traffic direction.
both	Specifies both inbound and outbound traffic directions.

Command Default

The monitor packet capture filter specifying is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Repeat the **monitor capture** command as many times as required to add multiple attachment points.

Examples

The following example shows how to add an attachment point to an interface:

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 0/0/1 in
Device# end
```

The following example shows how to add an attachment point to a control plane:

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

Related Commands

Command	Description
access-list	Configures an access list.
class-map	Configures a class map.
monitor capture match	Defines an explicit in-line core filter.
monitor capture (access list/class map)	Specifies an access list or class map as the core filter during packet capture.
show monitor capture	Displays packet capture details.

monitor capture buffer

To configure a buffer to capture packet data, use the **monitor capture buffer** command in privileged EXEC mode. To stop capturing packet data into the buffer, use the **no** form of this command.

monitor capture buffer *buffer-name* [**clear**| **export** *export-location*| **filter access-list** {*ip-access-list*| *ip-expanded-list*| *access-list-name*}| **limit** {**allow-nth-pak** *nth-packet*| **duration** *seconds*| **packet-count** *total-packets*| **packets-per-sec** *packets*}| [**max-size** *bytes*| **size** *buffer-size*] [**circular**| **linear**]]

no monitor capture buffer *buffer-name*

Cisco ASR 1000 Series Aggregation Services Routers

monitor capture *capture-name* **buffer circular size** *buffer-size*

no monitor capture *capture-name* **buffer circular size** *buffer-size*

Syntax Description

buffer-name	Name of the capture buffer.
clear	(Optional) Clears the contents of capture buffer.
export *export-location*	(Optional) Exports data from capture buffer in packet capture (PCAP) file format to the export location specified: **ftp:**, **http:**, **https:**, **pram:**, **rcp:**, **scp:**, **tftp:**
filter access-list	(Optional) Configures filters to filter the packets stored in the capture buffer by using access control lists (ACLs). The name or type of access lists can be specified as the criteria for configuring the filters.
ip-access-list	(Optional) IP access list number. The range is from 1 to 199.
ip-expanded-list	(Optional) IP expanded access list number. The range is from 1300 to 2699.
access-list-name	(Optional) Name of the access list.
limit	(Optional) Limits the packets captured based on the parameters specified.
allow-nth-pak *nth-packet*	(Optional) Allows every *n*th packet in the captured data through the buffer.
duration *seconds*	(Optional) Specifies the duration for which the data is captured, in seconds. The range is from 1 to 2147483647.

packet-count *total-packets*	(Optional) Specifies the total number of packets captured. The range is from 1 to 2147483647.
packets-per-sec *packets*	(Optional) Specifies the number of packets copied per second. The range is from 1 to 2147483647.
max-size *bytes*	(Optional) Specifies the maximum size of the element in the buffer, in bytes. The range is from 68 to 9500.
size *buffer-size*	(Optional) Specifies the size of the buffer. • The range is from 246 KB to 102400 KB. The default is 1024 KB. **Note** In Cisco IOS XE software, the range is from 1 MB to 100 MB. The default is 1 MB.
circular	(Optional) Specifies that the buffer is of a circular type. The circular type of buffer continues to capture data, even after the buffer is consumed, by overwriting the data captured previously.
linear	(Optional) Specifies that the buffer is of a linear type. The linear type of buffer stops capturing data when the buffer is fully consumed. **Note** In Cisco IOS XE software, the default type of the buffer is linear.
capture-name	Name of the capture.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Use this command to configure the capture buffer. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and data is overwritten.

Use the **limit** keyword to control the rate at which packets are captured.

Examples

The following example shows how to define a capture buffer named pktrace1 that is up to 256 KB long and is of circular type.

```
Device# monitor capture buffer pktrace1 max-size 256 circular
```

The following example shows how to export data from the pktrace1 buffer for analysis:

```
Device# monitor capture buffer pktrace1 export tftp://209.165.201.1/pktrace1
```

Examples

The following example shows how to define a capture buffer that is up to 2 MB long:

```
Device# monitor capture mycap buffer circular size 2
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture point	Defines a monitor capture point and associates it with a capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture clear

To clear the contents of a packet capture buffer, use the **monitor capture clear** command in privileged EXEC mode.

monitor capture *capture-name* **clear**

Syntax Description

capture-name	Name of the capture.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command to empty the capture buffer. Use the **monitor capture clear** command either during capture or after the capture has stopped either because one or more end conditions has been met, or you entered the **monitor capture stop** command. If you enter the **monitor capture clear** command after the capture has stopped, the **monitor capture export** command that is used to store the contents of the captured packets in a file will have no impact because the buffer has no captured packets.

Examples

The following example shows how to clear capture buffer contents:

```
Device> enable
Device# monitor capture mycap clear
Device# end
```

Related Commands

Command	Description
monitor capture export	Stores the captured packets in a file.
monitor capture stop	Stops the capture of packet data at a traffic trace point.
show monitor capture	Displays packet capture details.

monitor capture export

To store captured packets in a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture *capture-name* **export** *filelocation/file-name*

Syntax Description

capture-name	Name of the capture.
export	Stores all the packets in capture buffer to a file of type .PCAP.
file-location/file-name	Destination file location and name.

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture could have stopped because one or more end conditions has been met or you entered the **monitor capture stop** command.

Examples

The following example shows how to export capture buffer contents:

```
Device> enable
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

Related Commands

Command	Description
monitor capture stop	Terminates the packet capture.

monitor capture match

To define an explicit inline core filter, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture-name* **match** {**any** | {**ipv4**| **ipv6**} {*source-prefix/length*| **any**| **host**} *source-ip-address* {{*destination-prefix/length*| **any**| **host**} *destination-ip-address*}| **protocol** {**tcp**| **udp**} {{*source-prefix/length*| **any**| **host**} {{*destination-prefix/length*| **any**| **host**} | [[**eq** | **gt**| **lt** | **neg**] *port-number*] | **range** *start-port-number end-port-number* | [**eq** | **gt**| **lt** | **neg**] *port-number* | **range** *start-port-number end-port-number*}} | **mac** {*source-mac-address* | {**any**| **host**} *source-mac-address*} *source-mac-address-mask* {*destination-mac-address* | {**any**| **host**} *destination-mac-address*} *destination-mac-address-mask*}

no monitor capture *capture-name* **match**

Syntax Description

capture-name	Name of the capture.
any	Specifies all packets.
ipv4	Specifies IPv4 packets.
ipv6	Specifies IPv6 packets.
source-prefix/length	The network prefix and length of the IPv4 or IPv6 source address.
any	Specifies network prefix of any source IPv4 or IPv6 address.
host	Specifies the source host.
source-ip-address	Source IPv4 or IPv6 address.
destination-prefix/length	Destination IPv4 or IPv6 address.
any	Specifies the network prefix and length of any IPv4 or IPv6 destination address.
host	Specifies the destination host.
destination-ip-address	Destination IPv4 or IPv6 address.
protocol	Specifies the protocol.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

eq	(Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched.
gt	(Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched.
lt	(Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched.
neq	(Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched.
port-number	(Optional) The port number associated with the IP address. The range is from 0 to 65535.
range	(Optional) Specifies the range of port numbers.
start-port-number	(Optional) The start of the range of port numbers. The range is from 0 to 65535.
end-port-number	(Optional) The end of the range of port numbers. The range is from 0 to 65535.
mac	Specifies a Layer 2 packet.
source-mac-address	The source MAC address.
any	Specifies the network prefix of any source MAC address.
host	Specifies the MAC source host.
source-mac-address-mask	The source MAC address mask.
destination-mac-address	The destination MAC address.
any	Specifies the network prefix of any destination MAC address.
host	Specifies the MAC source host.
destination-mac-address-mask	The destination MAC address mask.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the **monitor capture** command to specify the core filter as a class map, access list, or explicit inline filter. Any filter has already specified before you enter the **monitor capture match** command is replaced.

Examples

The following example shows how to set various explicit filters:

```
Device> enable
Device# monitor capture mycap match any
Device# monitor capture mycap match mac any any
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap match ipv4 protocol udp 198.51.100.0/24 eq 20001 any
Device# end
```

The following example shows how to set a filter for MAC addresses:

```
Device> enable
Device# monitor capture match mycap mac 0030.9629.9f84 0000.0000.0000 0030.7524.9f84
0000.0000.0000
Device# end
```

The following example shows how to set a filter for IPv4 traffic:

```
Device> enable
Device# monitor capture match mycap ipv4 198.51.100.0/24 198.51.100.1 203.0.113.0/24
203.0.113.254
Device# end
```

Related Commands

Command	Description
monitor capture (access list/class map)	Configures an access list or class map as a core filter.

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

monitor capture *capture-name* **limit** [**duration** *seconds*] [**every** *number*] [**packet-length** *size*][**packets** *number*] [**pps** *number*]

no monitor capture *name* **limit** [**duration**] [**every**] [**packet-length**] [**packets**] [**pps**]

Syntax Description

capture-name	Name of the packet capture.
duration *seconds*	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
every *number*	(Optional) Specifies that, in a series of packets, the packet whose numerical order is denoted by the *number* argument should be captured. The range is from 2 to 100000.
packet-length *bytes*	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the *bytes* argument is stored.
packets *packets-number*	(Optional) Specifies the number of packets to be processed for capture.
pps *pps-number*	(Optional) Specifies the number of packets to be captured per second. The range is from 1 to 1000000.

Command Default

No capture limits are configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

If no duration is specified, the capture does not stop until it is manually interrupted. The entire packet is processed if the **packet-length** *bytes* keyword-argument pair is not specified. All matched packets are captured, if the **every** *number* keyword-argument pair is not specified. All matched packets are captured if the **packets** *packets-number* keyword-argument pair is not specified. The incoming packets are captured at the rate of 1 million packets per second if the **pps** *number* keyword-argument pair is not specified.

Examples

The following example shows how to specify capture limits:

```
Device> enable
Device# monitor capture mycap limit duration 10
Device# monitor capture mycap limit packet-length 128
Device# monitor capture mycap limit packets 100
Device# monitor capture mycap limit pps 1000
Device# monitor capture mycap limit duration 10 packet-length 128 packets 100
Device# end
```

Related Commands

Command	Description
show monitor capture	Displays packet capture details.

monitor capture point

To define a monitor capture point, use the **monitor capture point**command in privileged EXEC mode. To disable the monitor capture point, use the **no** form of this command.

monitor capture point {**ip**| **ipv6**} {**cef** *capture-point-name interface-name interface-type* {**both**| **in**| **out**}| **process-switched** *capture-point-name* {**both**| **from-us**| **in**| **out**}}

no monitor capture point {**ip**| **ipv6**} {**cef** *capture-point-name interface-name interface-type*| **process-switched** *capture-point-name*}

Syntax Description

ip	Configures an IPv4 capture point.
ipv6	Configures an IPv6 capture point.
cef	Specifies that the capture point contains Cisco Express Forwarding (CEF) packets.
capture-point-name	Name of the capture point.
interface-name interface-type	Specifies the interface name and type. For more information, use the question mark (?) online help function.
both	Specifies that the packets are captured in ingress and egress directions.
in	Specifies that the packets are captured in ingress direction.
out	Specifies that the packets are captured in egress direction.
process-switched	Specifies that the capture point contains process switched packets.
from-us	Specifies that the packets are originating locally.

Command Default

Monitor capture points are not defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Two types of capture points can be defined: IPv4 and IPv6. Once defined, use the **monitor capture point associate** command to associate the capture point with a capture buffer. Use the **monitor capture point start** command to start packet capture.

Multiple packet capture points can be activated on a given interface. For example, Border Gateway Protocol (BGP) packets can be captured into one capture buffer and Open Shortest Path First (OSPF) packets into another.

Examples

The following example shows how to define a capture point named ipceffa0/1 with CEF switching path and the Fast Ethernet interface 0/1:

```
Router# monitor capture point ip cef ipceffa0/1 fastEthernet 0/1 both
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point associate	Associates a monitor capture point with a capture buffer.
monitor capture point start	Enables a monitor capture point to start capturing packet data.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point associate

To associate a monitor capture point with a capture buffer, use the **monitor capture point associate**command in privileged EXEC mode.

monitor capture point associate *capture-point-name capture-buffer-name*

Syntax Description

capture-point-name	Name of the capture point to be associated with the capture buffer.
capture-buffer-name	Name of the capture buffer.

Command Default

Monitor capture points are not associated with capture buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **monitor capture point** command to define the capture points. Once the capture points are defined, use the **monitor capture point associate** command to associate a capture point with a capture buffer. This results in all packets captured from the specified capture point to be dumped into the associated capture buffer. A capture point can be associated with only one capture buffer.

Use the **monitor capture point disassociate** command to disassociate the specified capture point from the capture buffer.

Examples

The following example shows how to associate the ipceffa0/1 capture point to the pktrace1 capture buffer:

```
Router# monitor capture point associate ipceffa0/1 pktrace1
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.

Command	Description
monitor capture point	Defines a monitor capture point.
monitor capture point disassociate	Disassociates a monitor capture point from the specified monitor capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point disassociate

To disassociate a monitor capture point from its associations with a capture buffer, use the **monitor capture point disassociate**command in privileged EXEC mode.

monitor capture point disassociate *capture-point-name*

Syntax Description

capture-point-name	Specifies the name of the capture point to be disassociated from the capture buffer.

Command Default

Monitor capture points are not associated with capture buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **monitor capture point associate** command to associate a capture point with a capture buffer. This results in all packets captured from the specified capture point to be dumped into the associated capture buffer. A capture point can be associated with only one capture buffer.

Use the **monitor capture point disassociate** command to disassociate the specified capture point from the capture buffer.

Examples

The following example shows how to disassociate the ipceffa0/1 capture point from its capture buffer:

```
Router# monitor capture point disassociate ipceffa0/1
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines a monitor capture point.

Command	Description
monitor capture point associate	Associates a monitor capture point with a capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point start

To enable a monitor capture point to start capturing packet data, use the **monitor capture point start**command in privileged EXEC mode.

monitor capture point start {*capture-point-name*| **all**}

Syntax Description

capture-point-name	Name of the capture point to start capturing packet data.
all	Configures all capture points to start capturing packet data.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use this command to capture packet data at a traffic trace point into a buffer.

Once the capture point is defined, use the **monitor capture point start** command to enable the packet data capture. To stop capturing the packet data, use the **monitor capture point stop** command.

Examples

The following example shows how to start the packet capture:

```
Router# monitor capture point start ipceffa0/1
Mar 21 11:13:34.023: %BUFCAP-6-ENABLE: Capture Point ipceffa0/1 enabled.
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines a monitor capture point.

Command	Description
monitor capture point stop	Disables the packet capture.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point stop

To disable the packet capture, use the **monitor capture point stop**command in privileged EXEC mode.

monitor capture point stop {*capture-point-name*| **all**}

Syntax Description

capture-point-name	Name of the capture point to stop the packet capture.
all	Configures all capture points to stop the packet capture.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

```
Router# monitor capture point stop ipceffa0/1
Mar 21 11:14:20.152: %BUFCAP-6-DISABLE: Capture Point ipceffa0/1 disabled.
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines monitor capture points.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point tcp

To define a monitor capture point for TCP packets, use the **monitor capture point tcp** command in privileged EXEC mode. To disable the monitor capture point, use the **no** form of this command.

monitor capture point tcp *capture-point-name* {**both** | **in** | **out**} **filter** {**ipv4** | **ipv6**}

no monitor capture point tcp *capture-point-name*

Syntax Description

capture-point-name	Name for the capture point.
both	Specifies that the packets are captured in both ingress and egress directions.
in	Specifies that the packets are captured in the ingress direction.
out	Specifies that the packets are captured in the egress direction.
filter	Specifies the filter for IPv4 TCP packets or IPv6 TCP packets.
ipv4	Specifies the filter to capture IPv4 TCP packets.
ipv6	Specifies the filter to capture IPv6 TCP packets.

Command Default

Monitor capture points for TCP packets are not defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.10S	This command was introduced.

Usage Guidelines

Two types of capture points can be defined: IPv4 and IPv6. Once defined, use the **monitor capture point associate** command to associate the capture point with a capture buffer. Use the **monitor capture point start** command to start packet capture.

Examples

The following example shows how to define the capture point test01 to capture TCP packets in the ingress direction:

```
Device# monitor capture buffer buff01
Device# monitor capture point tcp test01 in filter ipv4
```

```
Device# monitor capture point associate test01 buff01
Device# monitor capture point start test01
```

Examples

The following example shows sample output with capture point test01, buffer buff01, and IPv4 filtering for capturing TCP packets:

```
Device# show monitor capture point test01

Status Information for Capture Point test01
TCP Process
Switch Path: TCP Process, Capture Buffer: buff01
Status : Active

Configuration:
monitor capture point tcp test01 in filter ipv4
```

Related Commands

Command	Description
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point associate	Associates a monitor capture point with a capture buffer.
monitor capture point start	Enables a monitor capture point to start capturing packet data.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point udp

To define a monitor capture point for UDP packets, use the **monitor capture point udp** command in privileged EXEC mode. To disable the monitor capture point, use the **no** form of this command.

monitor capture point udp *capture-point-name* {**both** | **in** | **out**} **filter** {**ipv4** | **ipv6**}

no monitor capture point udp *capture-point-name*

Syntax Description

capture-point-name	Name for the capture point.
both	Specifies that the packets are captured in both ingress and egress directions.
in	Specifies that the packets are captured in the ingress direction.
out	Specifies that the packets are captured in the egress direction.
filter	Specifies the filter for IPv4 UDP packets or IPV6 UDP packets.
ipv4	Specifies the filter to capture IPv4 TCP packets.
ipv6	Specifies the filter to capture IPv6 TCP packets.

Command Default

Monitor capture points for UDP packets are not defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.10S	This command was introduced.

Usage Guidelines

Two types of capture points can be defined: IPv4 and IPv6. Once defined, use the **monitor capture point associate** command to associate the capture point with a capture buffer. Use the **monitor capture point start** command to start packet capture.

Examples

The following example shows how to define the capture point test01 to capture UDP packets in both ingress direction:

```
Device# monitor capture buffer buff01
Device# monitor capture point udp test01 in filter ipv4
```

```
Device# monitor capture point associate test01 buff01
Device# monitor capture point start test01
```

Examples

The following example shows a sample output with capture point test01, buffer point buff01, and IPv4 inbound filter for capturing UDP packets:

```
Device# show monitor capture point test01

Status Information for Capture Point test01
UDP Process
Switch Path: UDP Process, Capture Buffer: buff01
Status : Active

Configuration:
monitor capture point udp test04 in filter ipv4
```

Related Commands

Command	Description
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point associate	Associates a monitor capture point with a capture buffer.
monitor capture point start	Enables a monitor capture point to start capturing packet data.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture *capture-name* **start**

Syntax Description

capture-name	Name of the capture.

Command Default

Data packets are not captured into a buffer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the **monitor capture start** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Examples

The following example shows how to start capture buffer contents:

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap limit packets 100 duration 60
Device# monitor capture mycap start
Device# end
```

Related Commands

Command	Description
monitor capture stop	Stops the packet data capture.
show monitor capture	Displays packet capture details.

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture *capture-name* **stop**

Syntax Description

capture-name	Name of the capture.

Command Default

The packet data capture is ongoing.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the **monitor capture start** command to start the capture of packet data that you started by using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

Examples

The following example shows how to stop capture buffer contents:

```
Device> enable
Device# monitor capture mycap stop
Device# end
```

Related Commands

Command	Description
monitor capture start	Starts the packet data capture.
show monitor capture	Displays packet capture details.

show monitor capture

To display the contents of a monitor capture buffer or a capture point, use the **show monitor capture** command in privileged EXEC mode.

show monitor capture{**buffer** {*capture-buffer-name* [**parameters**]| **all parameters**| **merged** *capture-buffer-name1 capture-buffer-name2*} [**dump**] [**filter** *filter-parameters*]} | **point** {**all** | *capture-point-name*}}

Catalyst 6500 Series and Cisco 7600 Series

show monitor capture[**buffer** [*start-index* [*end-index*]] [**brief** [**acl** {*acl-list*| *exp-acl-list*}] | **detail**][**dump** [**nowrap** *dump-length*]] {*acl-list exp-acl-list*}| **status**]

Cisco ASR 1000 Series Aggregation Services Routers

show monitor capture [*capture-name* [**parameter** | **buffer** [**brief** | **detailed**| **dump**]]]

Syntax Description

buffer	Displays the contents of the specified capture buffer.
capture-buffer-name	Name of the capture buffer.
parameters	(Optional) Displays values of parameters for the specified buffers or all buffers.
all	Displays values of parameters for all buffers.
merged	Displays values of parameters for any two specified buffers specified.
capture-buffer-name1	Name of the first buffer to be merged.
capture-buffer-name2	Name of the second buffer to be merged.
dump	(Optional) Displays a hexadecimal dump of the captured packet in addition to the metadata.
filter	(Optional) Displays filter parameters configured for packets stored in the buffer.

filter-parameters	(Optional) Displays the value of the specified parameter applied for defining the filter. Any of the following parameters can be specified: • **direction** {**ingress** | **egress**}—Filters output based on direction. Two types of direction can be specified: **ingress**, **egress**. • **input-interface** *interface-type number* —Filters packets on an input interface. • **l3protocol** —Filters packets with specific Layer 3 protocol. Three types of Layer 3 protocols that can be specified are as follows: **IPV4**, **IPV6**, **MPLS**. • **output-interface** *interface-type number* —Filters packets on an output interface. • **pak-size** *minimum-size maximum-size* —Filters output based on packet size. The minimum and maximum size for the packets must be specified. The range for the minimum size is from 1 to 2147483647 and for the maximum size is from 23 to 2147483647. • **time** *hh***:***mm day month* **duration** *seconds* —Filters packets from a specific date and time. The time is in the hh:mm format. The day, month of the year, and duration (in seconds) must be specified. The range for duration is from 1 to 2147483647.
point	Displays the contents of the specified capture point.
all	Displays all parameters for all the capture points.
capture-point-name	Displays all parameters for the specified capture point.
start-index	(Optional) The source index. The range is from 1 to 4294967295.
end-index	(Optional) The destination index. The range is from 1 to 4294967295.
brief	(Optional) Provides a brief output of the captured packet information.
acl	(Optional) Displays the output of captured packets for the specified access control list (ACL) only.

acl-list	(Optional) The IP access list (standard or extended). The range is from 0 to 199.
exp-acl-list	(Optional) The IP expanded access list (standard or extended). The range is from 1300 to 2699.
detail	(Optional) Provides a detailed output of the captured packet information.
dump	(Optional) Specifies the hexadecimal dump of the captured packets.
nowrap	(Optional) Prevents wrapping of the display output.
dump-length	(Optional) The hexadecimal dump length of the captured packets. The range is from 14 to 256.
status	(Optional) Displays the capture status.
parameter	Reconstructs and displays EXEC commands that were used to specify the capture.
detailed	Provides a detailed output of the captured packet information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI on Catalyst 6500 series routers.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD on Cisco 7600 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelin

Note The availability of keywords depends on your system and platform.

If you are using Cisco 6500 series routers or Cisco 7600 series routers, refer to the following usage guidelines:

You can enter the **show monitor capture** command when the capture buffer is not in the running state. You can enter the **show monitor capture status** command even when the capture is enabled to see how many packets are captured.

If you enter the **show monitor capture** command without any keywords or arguments, the output displays the configuration. If you enter the **dump nowrap** keywords, one hexadecimal line is printed per packet. Up to 72 characters of packet bytes is dumped.

If you enter the **dump nowrap** *dump-length* keywords and argument value, the specified length of bytes per line is dumped. If you enter the **brief** keyword, only the Source IP Address, Destination IP Address, Source Port, Destination Port, and Protocol fields are displayed along with the packet length and item number.

If you enter the **detail** keyword, packets are decoded to the Layer 4 protocol level and displayed. If you enter the **dump** keyword, non-IP packets are displayed in hexadecimal dump format. An ACL can be configured as a display filter so that only packets permitted by the ACL are displayed.

Examples

The following example shows how to display all parameters for all capture buffers:

```
Device# show monitor capture buffer all parameters

Capture buffer buff (circular buffer)
Buffer Size : 262144 bytes, Max Element Size : 68 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Configuration:
monitor capture buffer buff circular
Capture buffer buff1 (linear buffer)
Buffer Size : 262144 bytes, Max Element Size : 68 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Configuration:
```

The table below describes the significant fields shown in the display.

Table 1: show monitor capture Field Descriptions

Field	Description
Buffer Size	Size of the buffer defined.
Max Element Size	Specifies the maximum packet size based on which output has been filtered.
Allow-nth-pak	Specifies that every *n*th packet in the captured data through the buffer is allowed.
Associated Capture Points	Specifies all capture points that are associated with capture buffers.

The following sample output displays a hexadecimal dump of the captured packet. The output is self-explanatory and contains the interface type, switching path of the specified buffer, and a hexadecimal dump for the specified buffer.

```
Device# show monitor capture buffer pktrace1 dump
```

```
11:13:00.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F00 0000FE01 92AF5801 13025801  .@....~../X...X.
65B6F520: 58090800 4D1A1169 00000000 0005326C  X...M..i......2l
65B6F530: 01CCABCD ABCDABCD ABCDABCD ABCDABCD  .L+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCD00    +M+M+M+M+M+M+M.
11:13:20.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F02 0000FE01 92AD5801 13025801  .@....~..-X...X.
65B6F520: 58090800 FEF91169 00000000 0005326C  X...~y.i......2l
65B6F530: 4FECABCD ABCDABCD ABCDABCD ABCDABCD  Ol+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCDFF    +M+M+M+M+M+M+M.
```

The following sample output displays all capture points:

```
Device# show monitor capture point all

Status Information for Capture Point ipceffa0/1
IPv4 CEF
Switch Path: IPv4 CEF, Capture Buffer: pktrace1
Status : Inactive
Configuration:
monitor capture point ip cef ipceffa0/1 FastEthernet0/1 both
Status Information for Capture Point local
IPv4 CEF
Switch Path: IPv4 From Us, Capture Buffer: None
Status : Inactive
```

The table below describes the significant fields shown in the display.

Table 2: show monitor capture point all Field Descriptions

Field	Description
IPv4 CEF	Specifies that the capture point contains IPv4 Cisco Express Forwarding (formerly known as CEF) packets.
Switch Path	Indicates the type of switching path used by the capture point.
Capture Buffer	Specifies the name of the configured capture buffer.
Status	Indicates the status of the capture point.

Examples

The following example shows how to display the captured packets in a specific access control list (ACL):

```
Device# show monitor capture buffer acl 1

Capture instance [1] :
======================
session status : up
rate-limit value : 10000
buffer-size : 2097152
capture state : ON [running for 00:02:12.736]
capture mode : Linear
capture length : 68
```

The table below describes the significant fields shown in the display.

Table 3: show monitor capture buffer acl Field Descriptions

Field	Description
session status	Indicates the status of the capture session.
rate-limit value	Specifies the rate at which packets are captured, in bytes per second.
buffer-size	Specifies the capture buffer size, in bytes.
capture state	Indicates the status of the capture buffer.
capture mode	Indicates the shape of the capture buffer.
capture length	Specifies the length of the capture buffer.

The following sample output from the **show monitor capture buffer** command displays all packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture buffer

1 IP: s=10.12.0.5 , d=209.165.200.225, 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=10.12.0.7 , d=209.165.200.225, len 116
6 IP: s=10.12.0.1 , d=209.165.200.250, len 60
```

The following example shows how to display packets that are decoded to the layer 4 protocol level. The output is self-explanatory.

```
Device# 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=209.165.200.230, 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
```

The following example shows how to display non-IP packets in hexadecimal dump format. The output is self-explanatory.

```
Device# show monitor capture buffer dump

1 IP: s=10.12.0.5 , d=172.16.0.1, 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 424203000000000000800000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 0001080006040001001244
5 IP: s=10.12.0.6 , d=172.16.0.2, 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]...........
```

The following example shows how to display one hexadecimal line per packet, with up to 72 characters of packet bytes dumped. The output is self-explanatory.

```
Device# 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
```

Examples

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture mycap buffer
```

```
buffer size (KB) : 2048000
buffer used (KB) : 128
packets in buf : 17
packets dropped : 0
packets per sec : 3
```

The following example shows how to display the list of commands that were used to specify the capture:

```
Device# show monitor capture cap1 parameter
```

```
  monitor capture cap1 interface GigabitEthernet 1/0/1 both
  monitor capture cap1 match any
  monitor capture cap1 buffer size 10
  monitor capture cap1 limit pps 1000
```

The following example shows how to display brief output from the captured packet information. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer brief
```

```
------------------------------------------------------------------
#   size   timestamp     source             destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.0.0.1         ->  203.0.113.254  UDP
   1   46    0.267992   10.0.1.2         ->  203.0.113.204  IGMP
   2   76    0.428979   172.16.255.3     ->  172.16.255.3   UDP
   3   62    1.613982   10.0.29.1        ->  172.16.200.2   UDP
   4   74    1.659970   10.0.1.3         ->  10.0.0.10      EIGRP
   5   90    2.016006   10.29.0.4        ->  203.0.113.224  UDP
   6   74    2.088008   10.1.9.2         ->  203.0.113.10   EIGRP
   7   76    2.114008   172.17.254.1     ->  172.16.255.1   UDP
   8   74    2.245990   10.29.0.3        ->  203.0.113.10   EIGRP
   9   46    2.262987   10.0.0.0         ->  203.0.113.1    IGMP
  10   77    2.362988   10.1.9.2         ->  203.0.113.10   EIGRP
  11   62    2.631971   10.29.0.2        ->  203.0.113.2    UDP
  12   74    2.934009   10.29.0.5        ->  203.0.113.10   EIGRP
  13   74    3.331984   10.29.0.6        ->  203.0.113.10   EIGRP
  14   46    3.499974   10.0.0.0         ->  203.0.113.1    IGMP
  15   46    4.304992   10.0.0.0         ->  203.0.113.1    IGMP
  16   76    5.157005   172.16.255.3     ->  172.17.255.3   UDP
```

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer detailed
```

```
 -----------------------------------------------------------------
#   size   timestamp     source             destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.29.0.2         ->  172.16.255.3   UDP
  0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
  0010:  00300000 00000111 CFDC091D 0002E000   .0.............
  0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
  0030:  1D006369 73636F00 0000091D 0001       ..example.......

   1   46    0.267992   10.0.0.0          ->  172.16.255.1   IGMP
  0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
  0010:  00200000 00000102 44170000 0000E000   . ......D.......
  0020:  00019404 00001700 E8FF0000 0000       ..............

   2   76    0.428979   172.16.255.3     ->  172.17.255.3    UDP
  0000:  00000C07 AC1DB414 89031124 080045C0   ...........$..E.
  0010:  003E0000 0000FF11 64C5AC10 FF03AC11   .>......d.......
  0020:  FF030286 0286002A 84A40001 001EAC10   .......*........
  0030:  FF030000 01000014 00000000 04000004   ................

   3   62    1.613982   10.26.11.3        ->  172.16.255.1    UDP
  0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
  0010:  00300000 00000111 CFDB091D 0003E000   .0.............
  0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
  0030:  1D006369 73636F00 0000091D 0001       ..example.......

   4   74    1.659970   10.29.3.2         ->  172.16.255.2   EIGRP
  0000:  01005E00 000A001B 2BF69280 080045C0   ..^.....+.....E.
  0010:  003C0000 00000258 CE81091D 0002E000   .<.....X........
  0020:  000A0205 F3000000 00000000 00000000   ................
  0030:  00000000 00D10001 000C0100 01000000   ................

   5   90    2.016006   10.22.1.4         ->  203.0.113.1     UDP
  0000:  FFFFFFFF FFFF001C 0F2EDC00 080045C0   ..............E.
  0010:  004C0000 00000111 AFC1091D 0004FFFF   .L..............
  0020:  FFFF007B 007B0038 5B14E500 06E80000   ...{.{.8[.......
  0030:  00000021 BE23494E 49540000 00000000   ...!.#INIT......
```

The following example shows how to display a hexadecimal dump of the captured packet:

```
Device# show monitor capture cap1 buffer dump
0
 0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
 0010:  00300000 00000111 CFDC091D 0002E000   .0.............
 0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

1
 0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
 0010:  00200000 00000102 44170000 0000E000   . ......D.......
 0020:  00019404 00001700 E8FF0000 0000       ..............

2
 0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
 0010:  00300000 00000111 CFDB091D 0003E000   .0.............
 0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

3
 0000:  01005E00 000A001C 0F2EDC00 080045C0   ..^...........E.
 0010:  003C0000 00000258 CE7F091D 0004E000   .<.....X........
 0020:  000A0205 F3000000 00000000 00000000   ................
 0030:  00000000 00D10001 000C0100 01000000   ................
 0040:  000F0004 00080501 0300               ..........
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture	Enables and configures monitor packet capturing.
monitor capture buffer	Configures a buffer to capture packet data.

Command	Description
monitor capture point	Defines a monitor capture point and associates it with a capture buffer.