monitor capture through show monitor capture

- monitor capture, page 2
- monitor capture (access list/class map), page 6
- monitor capture (interface/control plane), page 8
- monitor capture buffer, page 10
- monitor capture clear, page 13
- monitor capture export, page 14
- monitor capture match, page 15
- monitor capture limit, page 18
- monitor capture point, page 20
- monitor capture point associate, page 22
- monitor capture point disassociate, page 24
- monitor capture point start, page 26
- monitor capture point stop, page 28
- monitor capture point tcp, page 29
- monitor capture point udp, page 31
- monitor capture start, page 33
- monitor capture stop, page 34
- show monitor capture, page 35
monitor capture

To enable and configure monitor packet capturing, use 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

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXI</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays the capture buffer contents.</td>
</tr>
</tbody>
</table>
monitor capture through show monitor capture
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>The name of the capture.</td>
</tr>
<tr>
<td>access-list</td>
<td>Configures an access list with the specified name.</td>
</tr>
<tr>
<td>class-map</td>
<td>Configures a class map with the specified name.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>Name of the capture.</td>
</tr>
<tr>
<td>interface type number</td>
<td>Configures an interface with the specified type and number as an attachment point.</td>
</tr>
<tr>
<td>control-plane</td>
<td>Configures a control plane as an attachment point.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies the inbound traffic direction.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies the outbound traffic direction.</td>
</tr>
<tr>
<td>both</td>
<td>Specifies both inbound and outbound traffic directions.</td>
</tr>
</tbody>
</table>

**Command Default**
The monitor packet capture filter specifying is not configured.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer-name</td>
<td>Name of the capture buffer.</td>
</tr>
<tr>
<td>clear</td>
<td>(Optional) Clears the contents of capture buffer.</td>
</tr>
<tr>
<td>export export-location</td>
<td>(Optional) Exports data from capture buffer in packet capture (PCAP) file format to the export location specified: ftp:, http:, https:, pram:, rcp:, scp:, tftp:</td>
</tr>
<tr>
<td>filter access-list</td>
<td>(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.</td>
</tr>
<tr>
<td>ip-access-list</td>
<td>(Optional) IP access list number. The range is from 1 to 199.</td>
</tr>
<tr>
<td>ip-expanded-list</td>
<td>(Optional) IP expanded access list number. The range is from 1300 to 2699.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>(Optional) Name of the access list.</td>
</tr>
<tr>
<td>limit</td>
<td>(Optional) Limits the packets captured based on the parameters specified.</td>
</tr>
<tr>
<td>allow-nth-pak nth-packet</td>
<td>(Optional) Allows every <code>nth</code> packet in the captured data through the buffer.</td>
</tr>
<tr>
<td>duration seconds</td>
<td>(Optional) Specifies the duration for which the data is captured, in seconds. The range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><strong>packet-count</strong></td>
<td>total-packets</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>(Optional) Specifies the total number of packets captured. The range is from 1 to 2147483647.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>packets-per-sec</strong></th>
<th>packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Specifies the number of packets copied per second. The range is from 1 to 2147483647.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>max-size</strong></th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Specifies the maximum size of the element in the buffer, in bytes. The range is from 68 to 9500.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>size</strong></th>
<th>buffer-size</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Specifies the size of the buffer.</td>
<td></td>
</tr>
<tr>
<td>• The range is from 246 KB to 102400 KB. The default is 1024 KB.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In Cisco IOS XE software, the range is from 1 MB to 100 MB. The default is 1 MB.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>circular</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>linear</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Specifies that the buffer is of a linear type. The linear type of buffer stops capturing data when the buffer is fully consumed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>capture-name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the capture.</td>
</tr>
</tbody>
</table>

**Command Default**
Data packets are not captured into a capture buffer.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was integrated into Cisco IOS XE Release 3.7S.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet-capture</td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td>monitor capture point</td>
<td>Defines a monitor capture point and associates it with a capture buffer.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>Name of the capture.</td>
</tr>
</tbody>
</table>

### Command Default

The buffer content is not cleared.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor capture export</code></td>
<td>Stores the captured packets in a file.</td>
</tr>
<tr>
<td><code>monitor capture stop</code></td>
<td>Stops the capture of packet data at a traffic trace point.</td>
</tr>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays packet capture details.</td>
</tr>
</tbody>
</table>
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 file-location/file-name`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>Name of the capture.</td>
</tr>
<tr>
<td>export</td>
<td>Stores all the packets in capture buffer to a file of type .PCAP.</td>
</tr>
<tr>
<td>file-location/file-name</td>
<td>Destination file location and name.</td>
</tr>
</tbody>
</table>

**Command Default**
The captured packets are not stored.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture stop</td>
<td>Terminates the packet capture.</td>
</tr>
</tbody>
</table>
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 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 match`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture-name</code></td>
<td>Name of the capture.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies all packets.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>Specifies IPv4 packets.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>Specifies IPv6 packets.</td>
</tr>
<tr>
<td><code>source-prefix/length</code></td>
<td>The network prefix and length of the IPv4 or IPv6 source address.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies network prefix of any source IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specifies the source host.</td>
</tr>
<tr>
<td><code>source-ip-address</code></td>
<td>Source IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><code>destination-prefix/length</code></td>
<td>Destination IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies the network prefix and length of any IPv4 or IPv6 destination address.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specifies the destination host.</td>
</tr>
<tr>
<td><code>destination-ip-address</code></td>
<td>Destination IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Specifies the protocol.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Specifies the TCP protocol.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Specifies the UDP protocol.</td>
</tr>
<tr>
<td><strong>eq</strong></td>
<td>(Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched.</td>
</tr>
<tr>
<td><strong>gt</strong></td>
<td>(Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched.</td>
</tr>
<tr>
<td><strong>lt</strong></td>
<td>(Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched.</td>
</tr>
<tr>
<td><strong>neq</strong></td>
<td>(Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched.</td>
</tr>
<tr>
<td><strong>port-number</strong></td>
<td>(Optional) The port number associated with the IP address. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><strong>range</strong></td>
<td>(Optional) Specifies the range of port numbers.</td>
</tr>
<tr>
<td><strong>start-port-number</strong></td>
<td>(Optional) The start of the range of port numbers. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><strong>end-port-number</strong></td>
<td>(Optional) The end of the range of port numbers. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><strong>mac</strong></td>
<td>Specifies a Layer 2 packet.</td>
</tr>
<tr>
<td><strong>source-mac-address</strong></td>
<td>The source MAC address.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Specifies the network prefix of any source MAC address.</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>Specifies the MAC source host.</td>
</tr>
<tr>
<td><strong>source-mac-address-mask</strong></td>
<td>The source MAC address mask.</td>
</tr>
<tr>
<td><strong>destination-mac-address</strong></td>
<td>The destination MAC address.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Specifies the network prefix of any destination MAC address.</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>Specifies the MAC source host.</td>
</tr>
<tr>
<td><strong>destination-mac-address-mask</strong></td>
<td>The destination MAC address mask.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor capture (access list/class map)</code></td>
<td>Configures an access list or class map as a core filter.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>Name of the packet capture.</td>
</tr>
<tr>
<td>duration seconds</td>
<td>(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 100000.</td>
</tr>
<tr>
<td>every number</td>
<td>(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.</td>
</tr>
<tr>
<td>packet-length bytes</td>
<td>(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.</td>
</tr>
<tr>
<td>packets packets-number</td>
<td>(Optional) Specifies the number of packets to be processed for capture.</td>
</tr>
<tr>
<td>pps pps-number</td>
<td>(Optional) Specifies the number of packets to be captured per second. The range is from 1 to 100000.</td>
</tr>
</tbody>
</table>

**Command Default**

No capture limits are configured.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays packet capture details.</td>
</tr>
</tbody>
</table>

---

**monitor capture limit**

Cisco IOS Embedded Packet Capture Command Reference
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

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

### Command Default

Monitor capture points are not defined.

### Command Modes

Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug packet-capture</code></td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td><code>monitor capture buffer</code></td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td><code>monitor capture point associate</code></td>
<td>Associates a monitor capture point with a capture buffer.</td>
</tr>
<tr>
<td><code>monitor capture point start</code></td>
<td>Enables a monitor capture point to start capturing packet data.</td>
</tr>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-point-name</td>
<td>Name of the capture point to be associated with the capture buffer.</td>
</tr>
<tr>
<td>capture-buffer-name</td>
<td>Name of the capture buffer.</td>
</tr>
</tbody>
</table>

**Command Default**

Monitor capture points are not associated with capture buffers.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet-capture</td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td>monitor capture buffer</td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>monitor capture point</td>
<td>Defines a monitor capture point.</td>
</tr>
<tr>
<td>monitor capture point disassociate</td>
<td>Disassociates a monitor capture point from the specified monitor capture buffer.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet-capture</td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td>monitor capture buffer</td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td>monitor capture point</td>
<td>Defines a monitor capture point.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>monitor capture point associate</td>
<td>Associates a monitor capture point with a capture buffer.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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.

```bash
monitor capture point start {capture-point-name | all}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture-point-name</code></td>
<td>Name of the capture point to start capturing packet data.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Configures all capture points to start capturing packet data.</td>
</tr>
</tbody>
</table>

**Command Default**

Data packets are not captured into a capture buffer.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**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:

```bash
Router# monitor capture point start ipceff0/1
Mar 21 11:13:34.023: %BUFCAP-6-ENABLE: Capture Point ipceff0/1 enabled.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug packet-capture</code></td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td><code>monitor capture buffer</code></td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td><code>monitor capture point</code></td>
<td>Defines a monitor capture point.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>monitor capture point stop</td>
<td>Disables the packet capture.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture-point-name</code></td>
<td>Name of the capture point to stop the packet capture.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Configures all capture points to stop the packet capture.</td>
</tr>
</tbody>
</table>

**Command Default**

Data packets are not captured into a capture buffer.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug packet-capture</code></td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td><code>monitor capture buffer</code></td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td><code>monitor capture point</code></td>
<td>Defines monitor capture points.</td>
</tr>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-point-name</td>
<td>Name for the capture point.</td>
</tr>
<tr>
<td>both</td>
<td>Specifies that the packets are captured in both ingress and egress directions.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies that the packets are captured in the ingress direction.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies that the packets are captured in the egress direction.</td>
</tr>
<tr>
<td>filter</td>
<td>Specifies the filter for IPv4 TCP packets or IPv6 TCP packets.</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the filter to capture IPv4 TCP packets.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Specifies the filter to capture IPv6 TCP packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Monitor capture points for TCP packets are not defined.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.10S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture buffer</td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td>monitor capture point associate</td>
<td>Associates a monitor capture point with a capture buffer.</td>
</tr>
<tr>
<td>monitor capture point start</td>
<td>Enables a monitor capture point to start capturing packet data.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>capture-point-name</strong></td>
<td>Name for the capture point.</td>
</tr>
<tr>
<td><strong>both</strong></td>
<td>Specifies that the packets are captured in both ingress and egress directions.</td>
</tr>
<tr>
<td><strong>in</strong></td>
<td>Specifies that the packets are captured in the ingress direction.</td>
</tr>
<tr>
<td><strong>out</strong></td>
<td>Specifies that the packets are captured in the egress direction.</td>
</tr>
<tr>
<td><strong>filter</strong></td>
<td>Specifies the filter for IPv4 UDP packets or IPv6 UDP packets.</td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
<td>Specifies the filter to capture IPv4 TCP packets.</td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
<td>Specifies the filter to capture IPv6 TCP packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Monitor capture points for UDP packets are not defined.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.10S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture buffer</td>
<td>Configures a capture buffer to capture packet data.</td>
</tr>
<tr>
<td>monitor capture point associate</td>
<td>Associates a monitor capture point with a capture buffer.</td>
</tr>
<tr>
<td>monitor capture point start</td>
<td>Enables a monitor capture point to start capturing packet data.</td>
</tr>
<tr>
<td>show monitor capture</td>
<td>Displays the contents of a capture buffer or a capture point.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture-name</code></td>
<td>Name of the capture.</td>
</tr>
</tbody>
</table>

**Command Default**

Data packets are not captured into a buffer.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor capture stop</code></td>
<td>Stops the packet data capture.</td>
</tr>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays packet capture details.</td>
</tr>
</tbody>
</table>
**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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor capture capture-name stop</code></td>
<td>Name of the capture.</td>
</tr>
</tbody>
</table>

### Command Default

The packet data capture is ongoing.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor capture start</code></td>
<td>Starts the packet data capture.</td>
</tr>
<tr>
<td><code>show monitor capture</code></td>
<td>Displays packet capture details.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Buffer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer</td>
<td>Displays the contents of the specified capture buffer.</td>
</tr>
<tr>
<td>capture-buffer-name</td>
<td>Name of the capture buffer.</td>
</tr>
<tr>
<td>parameters</td>
<td>(Optional) Displays values of parameters for the specified buffers or all buffers.</td>
</tr>
<tr>
<td>all</td>
<td>Displays values of parameters for all buffers.</td>
</tr>
<tr>
<td>merged</td>
<td>Displays values of parameters for any two specified buffers specified.</td>
</tr>
<tr>
<td>capture-buffer-name1</td>
<td>Name of the first buffer to be merged.</td>
</tr>
<tr>
<td>capture-buffer-name2</td>
<td>Name of the second buffer to be merged.</td>
</tr>
<tr>
<td>dump</td>
<td>(Optional) Displays a hexadecimal dump of the captured packet in addition to the metadata.</td>
</tr>
<tr>
<td>filter</td>
<td>(Optional) Displays filter parameters configured for packets stored in the buffer.</td>
</tr>
</tbody>
</table>
| 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. |
### show monitor capture

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

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI on Catalyst 6500 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRD</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRD on Cisco 7600 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was integrated into Cisco IOS XE Release 3.7S.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

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**

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

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
```
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
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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session status</td>
<td>Indicates the status of the capture session.</td>
</tr>
<tr>
<td>rate-limit value</td>
<td>Specifies the rate at which packets are captured, in bytes per second.</td>
</tr>
<tr>
<td>buffer-size</td>
<td>Specifies the capture buffer size, in bytes.</td>
</tr>
<tr>
<td>capture state</td>
<td>Indicates the status of the capture buffer.</td>
</tr>
<tr>
<td>capture mode</td>
<td>Indicates the shape of the capture buffer.</td>
</tr>
<tr>
<td>capture length</td>
<td>Specifies the length of the capture buffer.</td>
</tr>
</tbody>
</table>

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 424203000000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 000108000060
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 020707526f757465720415
```

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 45CD003C 00000000 ..$H08..E@.<....
08063830: 0258Cd0F 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 424203000000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 0001080000600001001244
5 IP: s=10.12.0.6 , d=172.16.0.2, len 116
0806FCB0: 0100 5E000000 ..^...
0806FCDD: 0015c7d7 AC000000 45CD0074 00000000 ..GW,...E@.t...
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 45c0 003c 0000000000000000
2 346 0180.c200.000e 0012.44d8.5000 88cc 020707526f7574
3 60 0180.c200.0000 0004.c099.06c5 0026 4242030000000000
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 10.26.0.1 -> 203.0.113.10 EIGRP
5 90 2.016006 10.29.0.4 -> 203.0.113.24 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 oc07ac1d 080045c0
```

Cisco IOS Embedded Packet Capture Command Reference
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 007C00AC 080045C0 ..^...........E.
0010: 00300000 00000111 CFDC091D 0002E000 .0..............
0020: 000207C1 07C1001C 802A0000 00030AFA .........*......
0030: 1D006369 73636F00 0000091D 0001 ..example.......

1
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......

2
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......

3
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......
```

```
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 007C00AC 080045C0 ..^...........E.
0010: 00300000 00000111 CFDC091D 0002E000 .0..............
0020: 000207C1 07C1001C 802A0000 00030AFA .........*......
0030: 1D006369 73636F00 0000091D 0001 ..example.......

1
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......

2
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......

3
0000: 01005E00 00020000 007C00AC 080045C0 ..^...........E.
0010: 000207C1 07C1001C 802A0000 00030AFA .........*......
0020: 1D006369 73636F00 0000091D 0001 ..example.......
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug packet-capture</td>
<td>Enables packet capture infra debugs.</td>
</tr>
<tr>
<td>monitor capture</td>
<td>Enables and configures monitor packet capturing.</td>
</tr>
<tr>
<td>monitor capture buffer</td>
<td>Configures a buffer to capture packet data.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>monitor capture point</td>
<td>Defines a monitor capture point and associates it with a capture buffer.</td>
</tr>
</tbody>
</table>
show monitor capture