platform software

To enable ACL or QoS configuration on the software platform, use the **platform software** command.

platform software {**acl** {**log_update** {**rate-limit-msg** {**disable** | **enable**}}} | **qos** {**logging** {**bootup**}}}

Syntax Description

acl	Specifies ACL as the keyword.
log_update	Specifies log updates for the Classification Manager.
rate-limit-msg	Specifies syslog rate limiting.
disable	Disables syslog rate limiting.
enable	Enables syslog rate limiting at one per second.
qos	Specifies QoS as the keyword.
logging	Specifies the logging-related parameters for QoS.
bootup	Enables QoS logging during bootup.

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to enable syslog rate limiting for ACL:

```
Router(config)# platform software acl log-update rate-limit-msg enable
```

platform software met profile

To configure allocation percentages for each block size of the mmulticast expansion, use the **platform software met profile** command. To disable allocation percentages, use the **no** form of this command.

platform software met profile {*value* | *value* | *value* | *value*}

Syntax Description

value	Sets the percentage allocation for each block size; valid values are 0 to 100 percent.

Defaults

The default values are 10 30 50 10 for each of the block sizes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	Support for this command was introduced.

Usage Guidelines

The new profile will take affect on the switch after reload.

You must configure all four of the profile blocks, and the total block percentages cannot exceed 100 percent.

Examples

This example shows how to set the block percentage for 4 blocks:

```
Router# platform software met profile 20 20 10 50
```

Related Commands

Command	Description
debug platform software multicast routing	Displays information about multicast errors.
show platform hardware cef adjacencies entry	Displays a single adjacency entry index.
show platform hardware cef mpls detail	Displays MPLS CEF detail information.
show platform hardware multicast routing	Matches and displays multicast routing group IP addresses.
show platform hardware met read	Displays platform hardware MET table entries.
show platform software met detail	Displays software routing for the MET.

platform system-controller reset-threshold

To configure the system controller reset threshold, use the **platform system-controller reset-threshold** command.

platform system-controller reset-threshold {*threshold-num*}

Syntax Description

threshold-num	Specifies the threshold reset number; valid values are 1 to 100.

Defaults

System controller reset is set to 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI10	Support for this command was introduced.
12.2(33)SXJ4	Support for this command was introduced.
15.1(1)SY	Support for this command was introduced.

Usage Guidelines

If you have a redundant supervisor engine and a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, the affected supervisor engine reloads. When you do not have a redundant supervisor engine and a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, one of the following happens:

- If the system controller reset threshold has not been reached, the system controller ASIC resets the supervisor engine and this message is displayed:

```
%SYSTEM_CONTROLLER-<>-THRESHOLD
%SYSTEM_CONTROLLER-<>-ERROR
%SYSTEM_CONTROLLER-<>-MISTRAL_RESET
```

- If the system controller reset threshold has been reached, the supervisor engine reloads and this message is displayed.

```
%SYSTEM_CONTROLLER-<>-ERROR
%SYSTEM_CONTROLLER-<>-FATAL
```

Examples

This example shows how to configure the system controller reset threshold to 55:

```
Router(config)# platform system-controller reset-threshold 55
```

platform verify

To enable Layer 3 error checking in the hardware, use the **platform verify** command in global configuration mode. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

platform verify ipv4 {**checksum** | **length** {**consistent** | **minimum**} | **same-address** | **tiny-frag**}

platform verify ipv6 {**length** {**consistent**} | **tiny-frag**}

platform verify syslog

Syntax Description

checksum	Enables the checksum-error check.
same-address	Enables the packets having same source and dstination IP.
length consistent	Enables the length-consistency check in Layer 2.
length minimum	Enables the minimum-length packet check in Layer 2.
tiny-frag	Enables the first TCP tiny fragment.
syslog	Enables the syslog packet parse errors.

Command Default

checksum

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The minimum-length packets are the packets with an IP header length or IP total length field that is smaller than 20 bytes.

When entering the minimum keyword, follow these guidelines:

- When enabling the IP "too short" check using the **platform verify ip length minimum** command, valid IP packets with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.
- When entering the **no platform verify ip length minimum** command, minimum-length packets are hardware switched. The packets that have IP protocol = 6 (TCP) are sent to the software.

Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config)# platform verify ip checksum
```

```
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config)# no platform verify ip checksum
Router(config)#
```

platform xconnect l2gre tunnel

To configure the Layer 2 generic routing encapsulation (l2gre) tunnel interface, use the **platform xconnect l2gre tunnel** command in VLAN interface mode.

platform xconnect l2gre *interface-num*

Syntax Description

interface-num	Specifies the tunnel interface number; valid values are 0 to 2147483647.

Command Modes

VLAN interface mode (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples

The following example shows the how to configure the l2gre tunnel to 6:

```
Router # platform xconnect l2gre tunnel 6
```

Related Commands

Command	Description
show platform l2transport gre	Displays platform details for l2gre tunnels.

police

To configure traffic policing, use the **police** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Packets per Second (pps)

police rate *units* **pps** [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

Syntax for Bytes per Second (pps)

police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

Syntax Description

bps	Average rate, in bits per second. Valid values are 8000 to 200000000.
burst-normal	(Optional) Normal burst size in bytes. Valid values are 1000 to 51200000. Default normal burst size is 1500.
burst-max	(Optional) Maximum burst size, in bytes. Valid values are 1000 to 51200000. Default varies by platform.
conform-action	Specifies action to take on packets that conform to the rate limit.
exceed-action	Specifies action to take on packets that exceed the rate limit.
violate-action	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes.

action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-clp-transmit** *value*—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1. • **set-cos-inner-transmit** *value*—Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router. • **set-cos-transmit** *value*—Sets the COS packet value and sends it. • **set-discard-class-transmit**—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • **set-dscp-tunnel-transmit** *value*—Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value. • **set-frde-transmit** *value*—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1. • **set-mpls-experimental-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value. • **set-mpls-experimental-topmost** *value*—Rewrites the experimental value. • **set-mpls-experimental-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value. • **set-prec-tunnel-transmit** *value*—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value. • **set-qos-transmit** *value*—Sets the qos-group value and transmits the packet with the new qos-group value. • **transmit**—Transmits the packet. The packet is not altered.

Command Default Traffic policing is not configured.

Command Modes

Policy-map class configuration (config-pmap-c) when specifying a single action to be applied to a marked packet

Policy-map class police configuration (config-pmap-c-police) when specifying multiple actions to be applied to a marked packet

Command History

Release	Modification
12.0(5)XE	This **police** command was introduced.
12.1(1)E	This command was integrated in Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T. The **violate-action** keyword was added.
12.2(2)T	The following modifications were made to the command: • The **set-clp-transmit** keyword for the *action* argument was added. • The **set-frde-transmit** keyword for the *action* argument was added. **Note** However, the **set-frde-transmit** keyword is not supported for AToM traffic in this release. Also, the **set-frde-transmit** keyword is supported only when Frame Relay is implemented on a physical interface without encapsulation. • The **set-mpls-experimental-transmit** keyword for the *action* argument was added.
12.2(8)T	The command was modified for the Policer Enhancement—Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate.
12.2(13)T	In the *action* argument, the **set-mpls-experimental-transmit** keyword was renamed to **set-mpls-experimental-imposition-transmit**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the **set-dscp-tunnel-transmit** and **set-prec-tunnel-transmit** keywords for the *action* argument were added. These keywords are intended for marking Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packets.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(15)T2	This command was modified to include support for marking Generic Routing Encapsulation (GRE) tunneled packets. **Note** For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF).
15.1(1)T	This command was modified to include support for policing on SVI interfaces for Cisco ISR 1800, 2800, and 3800 series routers.
12.2(50)SY	Support for the **set-mpls-experimental-topmost** *action* argument was added.

Usage Guidelines

Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

In Cisco IOS release 12.2(50)SY, when you apply the **set-mpls-experimental-topmost** *action* in the egress direction the **set-mpls-experimental-imposition** *action* is blocked.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action transmit** and **conform-action drop**.

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in Release 12.0(5)XE, see the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the New Features for 12.0(5)XE documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

The following are explanations of how the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T work.

Token Bucket Algorithm with One Token Bucket

The one-token bucket algorithm is used when the **violate-action** option is not specified in the **police** command CLI.

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, “B” bytes) arrives at specific time (time “T”), the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

  (time between packets (which is equal to T - T1) * policer rate)/8 bytes
- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in conform bucket B (minus the packet size to be limited) is fewer than 0, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets

The two-token bucket algorithm is used when the **violate-action** option is specified in the **police** command.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, "B" bytes) arrives at specific time (time "T") the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

  The token arrival rate is calculated as follows:

  (time between packets (which is equal to T-T1) * policer rate)/8 bytes
- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in conform bucket B is less than the packet size, the excess token bucket is checked for bytes by the packet. If the number of bytes in exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number of bytes in exceed bucket B is less than the packet size, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Using the set-cos-inner-transmit Action for SIPs and SPAs on the Cisco 7600 Series Router

The **set-cos-inner-transmit** keyword action was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value as a policing action when using MPB features on the Enhanced FlexWAN module and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

For more information about QoS and the forms of **police** commands supported by the SIPs on the Cisco 7600 series router, see the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*.

Examples

Token Bucket Algorithm with One Token Bucket: Example

The following example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0:

```
Router(config)# class-map access-match
```

```
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket ((0.25 * 8000)/8), leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets: Example

In this example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet, and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size), is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Conforming to the MPLS EXP Value: Example

The following example shows that if packets conform to the rate limit, the MPLS EXP field is set to 5. If packets exceed the rate limit, the MPLS EXP field is set to 3.

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000 conform-action
set-mpls-experimental-imposition-transmit 5 exceed-action
set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

Setting the Inner CoS Value as an Action for SIPs and SPAs on the Cisco 7600 Series Router: Example

The following example shows configuration of a QoS class that filters all traffic for virtual LAN (VLAN) 100 into a class named "vlan-inner-100" and establishes a traffic shaping policy for the vlan-inner-100 class. The service policy limits traffic to an average rate of 500 kbps, with a normal burst of 1000 bytes and a maximum burst of 1500 bytes, and sets the inner CoS value to 3. Since setting of the inner CoS value is supported only with bridging features, the configuration also shows the service policy being applied as an output policy for an ATM SPA interface permanent virtual circuit (PVC) that bridges traffic into VLAN 100 using the **bridge-domain** command.

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# police 500000 1000 1500 conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

Related Commands

Command	Description
bridge-domain	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay data-link connection identifier (DLCI).
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Specifies the name of the service policy to be attached to the interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

police rate

To configure packet-based or byte-based traffic policing, use the **police rate** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Bytes per Second (bps)

police rate *units* **bps** [**burst** *burst_bytes* **bytes**] [**peak-rate** *peak_rate_bps* **bps**] [**peak-burst** *peak_burst_bytes* **bytes**] [**conform-action** *selected_action*] [**exceed-action** *selected_action*] [**violate-action** *selected_action*]

no police rate *units* **bps** [**burst** *burst_bytes* **bytes**] [**peak-rate** *peak_rate_bps* **bps**] [**peak-burst** *peak_burst_bytes* **bytes**] [**conform-action** *selected_action*] [**exceed-action** *selected_action*] [**violate-action** *selected_action*]

Syntax for Packets per Second (pps)

police rate *units* **pps** [**burst** *burst_packets* **packets**] [**conform-action** *selected_action*] [**exceed-action** *selected_action*] [**violate-action** *selected_action*]

no police rate *units* **pps** [**burst** *burst_packets* **packets**] [**conform-action** *selected_action*] [**exceed-action** *selected_action*] [**violate-action** *selected_action*]

Syntax Description

units	Specifies the police rate in the range of 7-10,000,000,000.
bps	Specifies that bytes per seconds (bps) will be used to determine the rate at which traffic is policed.
pps	Specifies that packets per seconds (pps) will be used to determine the rate at which traffic is policed.
burst *burst_bytes* **bytes**	(Optional) Specifies the burst rate used for policing traffic, in bytes. Valid range of values is 1-2000000000.
burst *burst_packets* **packets**	(Optional) Specifies the burst rate, in packets, will be used for policing traffic. Valid range of values is 1-31250000.
peak-rate *peak_rate_value*	Specifies the peak information rate (PIR) that will be used for policing traffic and calculating the PIR. Valid range of values is 7-10,000,000,000.
peak-burst *peak_burst_bytes* **bytes**	Specifies the burst rate in bytes for the peak-rate used for policing traffic. Valid range of values if 1-2000000000.
conform-action	Specifies action to take on packets that conform to the rate limit.
exceed-action	Specifies action to take on packets that exceed the rate limit.
violate-action	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes.

action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **policed-discard-class-transmit**—Changes discard class per policed-dscp map and sends it. • **policed-dscp-transmit**—Changes the DSCP value according to the policed-dscp map and sends the packet. • **set-cos-transmit** *value*—Sets the COS packet value and sends it. • **set-discard-class-transmit**—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • **set-dscp-tunnel-transmit** *value*—Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value. • **set-mpls-exp-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value. • **set-mpls-exp-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value. • **set-prec-tunnel-transmit** *value*—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value. • **transmit**—Transmits the packet. The packet is not altered.

Command Default

Traffic policing is not configured.

Command Modes

Policy-map class configuration (config-pmap-c) when specifying a single action to be applied to a marked packet

Policy-map class police configuration (config-pmap-c-police) when specifying multiple actions to be applied to a marked packet

port-channel hash-distribution

To set the hash distribution algorithm method, use the **port-channel hash-distribution** command in global configuration mode. To return to the default settings, use the **no** or **default** form of this command.

port-channel hash-distribution {**adaptive** | **fixed**}

{**no** | **default**} **port-channel hash-distribution**

Syntax Description

adaptive	Specifies selective distribution of the bundle select register among the port-channel members.
fixed	Specifies fixed distribution of the bundle select register among the port-channel members.
default	Specifies the default setting.

Command Default

In Cisco IOS Release 12.2(50)SY or later releases, the hash distribution algorithm method is set to adaptive. In earlier releases, the hash distribution algorithm method is set to fixed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The EtherChannel load distribution algorithm uses the bundle select register in the port ASIC to determine the port for each outgoing packet. When you use the **adaptive** algorithm, it does not require the bundle select register to be changed for existing member ports. When you use the **fixed** algorithm and you either add or delete a port from the EtherChannel, the switch updates the bundle select register for each port in the EtherChannel. This update causes a short outage on each port.

Note When you change the algorithm, the change is applied at the next member link event. Example events include link down, up, addition, deletion, no shutdown, and shutdown. When you enter the command to change the algorithm, the command console issues a warning that the command does not take effect until the next member link event.

Examples

The following example shows how to set the hash distribution algorithm method to adaptive:

```
Router(config)# port-channel hash-distribution adaptive
```

priority-queue cos-map

To map CoS values to the receive and transmit strict-priority queues in interface configuration command mode, use the **priority-queue cos-map** command. To return to the default mapping, use the **no** form of this command.

priority-queue cos-map *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]

no priority-queue cos-map

Syntax Description

queue-id	Queue number; the valid value is **1**.
cos1	CoS value; valid values are from 0 to 7.
. . . cos8	(Optional) CoS values; valid values are from 0 to 7.

Command Default

The default mapping is queue 1 is mapped to CoS 5 for the following receive and transmit strict-priority queues:

- 1p1q4t receive queues
- 1p1q0t receive queues
- 1p1q8t receive queues
- 1p2q2t transmit queues
- 1p3q8t transmit queues
- 1p7q8t transmit queues
- 1p3q1t transmit queues
- 1p2q1t transmit queues

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

When mapping CoS values to the strict-priority queues, note the following information:

- The queue number is always **1**.
- You can enter up to 8 CoS values to map to the queue.

Examples

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

Related Commands

Command	Description
show queueing interfaces	Displays queueing information.

priority-queue queue-limit

To set the priority-queue size on an interface, use the **priority-queue queue-limit** command in interface configuration mode. To return to the default priority-queue size, use the **no** form of this command.

priority-queue queue-limit *percent*

no priority-queue queue-limit *percent*

Syntax Description

percent	Priority-queue size in percent; valid values are from 1 to 100.

Command Default

When global quality of service (QoS) is enabled the priority-queue size is 15. When global QoS is disabled the priority-queue size is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF2	Support for this command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is supported on the following modules:

- WS-X6501-10GE—1p2q1t[1]
- WS-X6148A-GE—1p3q8t[2]
- WS-X6148-45—1p3q8t
- WS-X6148-FE-SFP—1p3q8t
- WS-X6748-SFP—1p3q8t
- WS-X6724-SFP—1p7q8t [3]
- WS-X6704-10GE—1p7q4t[4]
- WS-SUP32-10GB-3E—1p7q4t

1. 1p2q1t—One strict-priority queue, two standard queues with one WRED drop threshold and one non-configurable (100%) tail-drop threshold per queue.
2. 1p3q8t—One strict-priority queue, three standard queues with eight WRED drop thresholds per queue.
3. 1p7q8t—One strict-priority queue, seven standard queues with eight WRED drop thresholds per queue.
4. 1p7q4t—One strict-priority queue, seven standard queues with four WRED drop thresholds per queue.

- WS-SUP32-GB-3E—1p3q8t
- WS-X6708-10GE—1p7q4t

Examples

The following example shows how to set the priority-queue size on an interface:

```
priority-queue queue-limit 15
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

queue-buffers ratio

To set the buffer ratio for a queue, use the **queue-buffers ratio** command in QoS policy-map class configuration mode. To remove the queue buffer ratio, use the **no** form of the command.

queue-buffers ratio *number*

no queue-buffers ratio *number*

Syntax Description

number	Sets the size of the queue ratio; valid range is 0 to 100.

Command Default

None

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples

The following example shows how to configure the buffer ratio to 6:

```
Router(config-pmap-c)# queue-buffers ratio 6
```

rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights in interface configuration command mode, use the **rcv-queue bandwidth** command. To return to the default settings, use the **no** form of this command.

rcv-queue bandwidth *weight-1 ... weight-n*

no rcv-queue bandwidth

Syntax Description

weight-1 ... weight-n	WRR weights; valid values are from 0 to 255.

Command Default

The defaults are as follows:

- QoS enabled—4:255
- QoS disabled—255:1

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on 2q8t and 8q8t ports only.

You can configure up to seven queue weights.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

Related Commands

Command	Description
rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues.
show queueing interface	Displays queueing information.

rcv-queue cos-map

To map the class of service (CoS) values to the standard receive-queue drop thresholds, use the **rcv-queue cos-map** command in interface configuration mode. To remove the mapping, use the **no** form of this command.

rcv-queue cos-map *queue-id threshold-id cos-1 ... cos-n*

no rcv-queue cos-map *queue-id threshold-id*

Syntax Description

queue-id	Queue ID; the valid value is 1.
threshold-id	Threshold ID; valid values are from 1 to 4.
cos-1 ... cos-n	CoS values; valid values are from 0 to 7.

Command Default

The defaults are listed in Table 1.

Table 1 CoS-to-Standard Receive Queue Map Defaults

queue	threshold	cos-map	queue	threshold	cos-map
With QoS Disabled			**With QoS Enabled**		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *cos-n* value is defined by the module and port type. When you enter the *cos-n* value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

Examples

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on:  Gi1/1 Gi1/2
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queue queue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

rcv-queue queue-limit *q-limit-1 q-limit-2*

no rcv-queue queue-limit

Syntax Description

q-limit-1	Standard queue weight; valid values are from 1 and 100 percent.
q-limit-2	Strict-priority queue weight; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- 80 percent is for low priority.
- 20 percent is for strict priority.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Valid strict-priority weight values are from 1 to 100 percent, except on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 percent.

The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

Examples

This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
```

Related Commands

Command	Description
show queueuing interface	Displays queueing information.

rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queue random-detect** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id*

Syntax Description

max-threshold	Specifies the maximum threshold.
min-threshold	Specifies the minimum threshold.
queue-id	Queue ID; the valid value is 1.
threshold-percent-1 threshold-percent-n	Threshold weights; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **min-threshold**—80 percent
- **max-threshold**—20 percent

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the QoS chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queue threshold** command in interface configuration mode. To return the thresholds to the default settings, use the **no** form of this command.

rcv-queue threshold *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue threshold

Syntax Description

queue-id	Queue ID; the valid value is 1.
threshold- percent-1 ... threshold- percent-n	Threshold ID; valid values are from 1 to 100 percent.

Command Default

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- Quality of service (QoS) assigns all traffic with class of service (CoS) 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue drop threshold 1, the Cisco 7600 series router drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue drop threshold 2, the Cisco 7600 series router drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue drop threshold 3, the Cisco 7600 series router drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue drop threshold 4, the Cisco 7600 series router drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Cisco 7600 series router drops incoming frames when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.

Note The 100-percent threshold may be actually changed by the module to 98 percent to allow Bridge Protocol Data Unite (BPDU) traffic to proceed. The BPDU threshold is factory set at 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *queue-id* value is always 1.

A value of 10 indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is trust cos.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command.

Examples

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue threshold	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

show fips

To display the FIPs information about the switch, use the **show fips** command in EXEC mode.

show fips

no show fips

Syntax Description This command has no keywords or arguments

Syntax Description EXEC

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples This example shows how to displays if FIPS modes if running on a switch:

```
Router# show fips
Router# The FIPS mode is on.
Router#
```

Related Commands

Command	Description
fips	Enables FIPS security requirements on the switch.

show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode.

Cisco 2500 Series, Cisco 2600 Series, Cisco 4700 Series, and Cisco 7000 Series

show interfaces [*type number*] [*first*] [*last*] [**accounting**]

Catalyst 6500 Series, Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

show interfaces [*type slot*/*port*] [**accounting | counters protocol status | crb | dampening | description | dot1ad | etherchannel** [**module** *number*] **| fair-queue | irb | mac-accounting | mpls-exp | precedence | random-detect | rate-limit | stats | summary | switching | utilization** {*type number*}]

Cisco 7500 Series with Ports on VIPs

show interfaces [*type slot*/*port-adapter*/*port*]

Cisco 7600 Series

show interfaces [*type number* | **null** *interface-number* | **vlan** *vlan-id*]

Channelized T3 Shared Port Adapters

show interfaces serial [*slot*/*subslot*/*port*/*t1-num*:*channel-group*]

Shared Port Adapters

show interfaces *type* [*slot*/*subslot*/*port*[/*sub-int*]]

Syntax Description

type	(Optional) Interface type. Allowed values for *type* can be **atm**, **async**, **auto-template, bvi, bri0**, **ctunnel**, **container**, **dialer**, **e1**, **esconPhy**, **ethernet**, **fastethernet**, **fcpa**, **fddi**, **filter**, **filtergroup**, **gigabitethernet**, **ge-wan**, **hssi**, **longreachethernet**, **loopback**, **mfr**, **module**, **multilink**, **null**, **pos**, **port-channel**, **port-group**, **pos-channel**, **sbc**, **sdcc**, **serial**, **sysclock**, **t1**, **tengigabitethernet**, **token**, **tokenring**, **tunnel**, **vif**, **vmi**, **virtual-access**, **virtual-ppp**, **virtual-template**, **virtual-tokenring**. **voaBypassIn**, **voaBypassOut**, **voaFilterIn**, **voaFilterOut**, **voaIn**, **voaOut**. **Note** The type of interfaces available is based on the type of router used.
number	(Optional) Port number on the selected interface.

first last	(Optional) For Cisco 2500 series routers, ISDN Basic Rate Interfae (BRI) only. The *first* argument can be either 1 or 2. The *last* argument can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
counters protocol status	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
dot1ad	(Optional) Displays interface 802.1ad information.
etherchannel [**module** *number*]	(Optional) Displays interface Ether Channel information. • **module**—The **module** keyword limits the display to interfaces available on the module.
fair-queue	(Optional) Displays interface Weighted Fair Queueing (WFQ) information.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
random-detect	(Optional) Displays interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
summary	(Optional) Displays an interface summary.
switching	(Optional) Displays interface switching.
null *interface-number*	(Optional) Specifies the null interface, that is **0**.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot information.
/port	(Optional) Port number. Refer to the appropriate hardware manual for port information.
/port-adapter	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

[*slot*/*subslot*/*port*/*t1-num*:*channel-group*]	**(Optional) Channelized T3 Shared Port Adapters** Number of the chassis slot that contains the channelized T3 Shared Port Adapters (SPA) (for example, 5/0/0:23), where: • *slot*—(Optional) Chassis slot number. For SPA interface processors (SIPs), refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • /*subslot*—(Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • /*port*—(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide. • /*t1-num*—(Optional) T1 time slot in the T3 line. The value can be from 1 to 28. • :*channel-group*—(Optional) Number 0–23 of the DS0 link on the T1 channel.

[*slot*/*subslot*/*port*[/*sub-int*]]	**(Optional) Shared Port Adapters** Number of the chassis slot that contains the SPA interface (for example, 4/3/0), where: • *slot*—(Optional) Chassis slot number. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • /*subslot*—(Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • /*port*—(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide. • /*sub-int*—(Optional) Subinterface number (for those SPAs that support subinterface configuration).
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was modified to include support for flow-based WRED.
12.0(4)T	This command was modified to include enhanced display information for dialer bound interfaces.
12.0(7)T	This command was modified to include **dialer** as an interface type and to reflect the default behavior.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and introduced a new address format and output for SPA interfaces on the Cisco 7304 router. The *subslot* argument was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(14)SX	This command was modified. Support for this command was introduced.
12.2(17d)SXB	This command was modified. The uplink dual-mode port information was updated.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers, and the **tengigabitethernet** interface type was added. 10-Gigabit Ethernet interfaces were introduced with the release of the 1-Port 10-Gigabit Ethernet SPA.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SXJ01	This command was integrated into Cisco IOS Release 12.2(33)SXJ01.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was updated to display operational status for Gigabit Ethernet interfaces that are configured as primary and backup interfaces (Cisco 7600 series routers).
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was modified. The default value of the command was modified on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(50)SY	This command was integrated in Cisco IOS Release 12.2(50)SY and the **dot1ad** keyword was added.
15.0(01)SY	This command was integrated in Cisco IOS Release 15.1(50)SY.

Usage Guidelines

Display Interpretation

The **show interfaces** command displays statistics for the network interfaces. The resulting output varies, depending on the network for which an interface has been configured. The resulting display on the Cisco 7200 series routers shows the interface processors in slot order. If you add interface processors after booting the system, they will appear at the end of the list, in the order in which they were inserted.

Information About Specific Interfaces

The *number* argument designates the module and port number. If you use the **show interfaces** command on the Cisco 7200 series routers without the *slot*/*port* arguments, information for all interface types will be shown. For example, if you type **show interfaces** you will receive information for all Ethernet, serial, Token Ring, and FDDI interfaces. Only by adding the type *slot*/*port* argument you can specify a particular interface.

Cisco 7600 Series Routers

Valid values for the *number* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** commands. In this case, the duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command shows the operating mode for an interface, and the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Command Variations

You will use the **show interfaces** command frequently while configuring and monitoring devices. The various forms of the **show interfaces** commands are described in detail in the sections that follow.

Dialer Interfaces Configured for Binding

If you use the **show interfaces** command on dialer interfaces configured for binding, the display will report statistics on each physical interface bound to the dialer interface; see the following examples for more information.

Removed Interfaces

If you enter a **show interfaces** command for an interface type that has been removed from the router or access server, interface statistics will be displayed accompanied by the following text: "Hardware has been removed."

Weighted Fair Queueing Information

If you use the **show interfaces** command on a router or access server for which interfaces are configured to use weighted fair queueing through the **fair-queue** interface command, additional information is displayed. This information consists of the current and high-water mark number of flows.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, when a multilink PPP (MLP) interface is down/down, its default bandwidth rate is the sum of the serial interface bandwidths associated with the MLP interface.

In Cisco IOS Release 12.2(31)SB, the default bandwidth rate is 64 Kbps.

Examples

The following is sample output from the **show interfaces** command. Because your display will depend on the type and number of interface cards in your router or access server, only a portion of the display is shown.

Note If an asterisk (*) appears after the throttles counter value, it means that the interface was throttled at the time the command was run.

```
Router# show interfaces

Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
```

```
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
.
.
.
```

Example with Custom Output Queueing

The following shows partial sample output when custom output queueing is enabled:

```
Router# show interfaces

Last clearing of "show interface" counters 0:00:06
Input queue: 0/75/0 (size/max/drops); Total output drops: 21
Output queues: (queue #: size/max/drops)
     0: 14/20/14  1: 0/20/6  2: 0/20/0 3: 0/20/0 4: 0/20/0 5: 0/20/0
     6: 0/20/0 7: 0/20/0  8: 0/20/0  9: 0/20/0  10: 0/20/0
.
.
.
```

When custom queueing is enabled, the drops accounted for in the output queues result from bandwidth limitation for the associated traffic and lead to queue length overflow. Total output drops include drops on all custom queues and the system queue. Fields are described with the weighted fair queueing output in Table 2.

Example Including Weighted-Fair-Queueing Output

For each interface on the router or access server configured to use weighted fair queueing, the **show interfaces** command displays the information beginning with *Input queue:* in the following display:

```
Router# show interfaces

Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Output queue: 7/64/0 (size/threshold/drops)
                    Conversations 2/9 (active/max active)
```

Table 2 describes the input queue and output queue fields shown in the preceding two displays.

Table 2 Weighted-Fair-Queueing Output Field Descriptions

Field	Description
Input Queue	
size	Current size of the input queue.
max	Maximum size of the queue.
drops	Number of messages discarded in this interval.
Total output drops	Total number of messages discarded in this session.
Output Queue	
size	Current size of the output queue.
threshold	Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped.
drops	Number of dropped messages.
Conversations: active	Number of currently active conversations.
Conversations: max active	Maximum number of concurrent conversations allowed.

Example with Accounting Option

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command. When you use the **accounting** option, only the accounting statistics are displayed.

Note Except for protocols that are encapsulated inside other protocols, such as IP over X.25, the accounting option also shows the total bytes sent and received, including the MAC header. For example, it totals the size of the Ethernet packet or the size of a packet that includes High-Level Data Link Control (HDLC) encapsulation.

Per-packet accounting information is kept for the following protocols:

- AppleTalk
- Address Resolution Protocol (ARP) (for IP, Frame Relay, Switched Multimegabit Data Service (SMDS))
- Connectionless Network Service (CLNS)
- Digital Equipment Corporation (DEC) Maintenance Operations Protocol (MOP)

  The routers use MOP packets to advertise their existence to Digital Equipment Corporation machines that use the MOP. A router periodically broadcasts MOP packets to identify itself as a MOP host. This results in MOP packets being counted, even when DECnet is not being actively used.
- DECnet
- HP Probe
- IP
- LAN Manager (LAN Network Manager and IBM Network Manager)

- Novell
- Serial Tunnel Synchronous Data Link Control (SDLC)
- Spanning Tree
- SR Bridge
- Transparent Bridge

Example with DWRED

The following is sample output from the **show interfaces** command when distributed WRED (DWRED) is enabled on an interface. Notice that the packet drop strategy is listed as "VIP-based weighted RED."

```
Router# show interfaces hssi 0/0/0

Hssi0/0/0 is up, line protocol is up
  Hardware is cyBus HSSI
  Description: 45Mbps to R1
Internet address is 10.200.14.250/30
MTU 4470 bytes, BW 45045 Kbit, DLY 200 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Packet Drop strategy: VIP-based weighted RED
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1976 packets input, 131263 bytes, 0 no buffer
Received 1577 broadcasts, 0 runts, 0 giants
0 parity
4 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1939 packets output, 130910 bytes, 0 underruns
0 output errors, 0 applique, 3 interface resets
0 output buffers copied, 0 interrupts, 0 failures
```

Example with ALC

The following is sample output from the **show interfaces** command for serial interface 2 when Airline Control (ALC) Protocol is enabled:

```
Router# show interfaces serial 2

Serial2 is up, line protocol is up
Hardware is CD2430
MTU 1500 bytes, BW 115 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation ALC, loopback not set
Full-duplex enabled.
     ascus in UP state: 42, 46
     ascus in DOWN state:
     ascus DISABLED:
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 output buffer failures, 0 output buffers swapped out
```

```
DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

Example with SDLC

The following is sample output from the **show interfaces** command for an SDLC primary interface supporting the SDLC function:

```
Router# show interfaces

Serial 0 is up, line protocol is up
 Hardware is MCI Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation SDLC-PRIMARY, loopback not set
      Timers (msec): poll pause 100 fair poll 500. Poll limit 1
      [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
      SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
             largest token ring frame 2052]
SDLC addr C1 state is CONNECT
       VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
       Hold queue: 0/12 IFRAMEs 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
       Poll: clear, Poll count: 0, chain: p: C1 n: C1
       SDLLC [largest SDLC frame: 265, XID: disabled]
  Last input 00:00:02, output 00:00:01, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 517 bits/sec, 30 packets/sec
  Five minute output rate 672 bits/sec, 20 packets/sec
       357 packets input, 28382 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       926 packets output, 77274 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets, 0 restarts
       2 carrier transitions
```

Table 3 shows the fields relevant to all SDLC connections.

Table 3 show interfaces Field Descriptions When SDLC Is Enabled

Field	Description
Timers (msec)	List of timers in milliseconds.
poll pause, fair poll, Poll limit	Current values of these timers.
T1, N1, N2, K	Current values for these variables.

Table 4 shows other data given for each SDLC secondary interface configured to be attached to this interface.

Table 4 SDLC Field Descriptions

Field	Description
addr	Address of this secondary interface.
State	Current state of this connection. The possible values follow: • BOTHBUSY—Both sides have told each other that they are temporarily unable to receive any more information frames. • CONNECT—A normal connect state exists between this router and this secondary. • DISCONNECT—No communication is being attempted to this secondary. • DISCSENT—This router has sent a disconnect request to this secondary and is awaiting its response. • ERROR—This router has detected an error, and is waiting for a response from the secondary acknowledging this. • SNRMSENT—This router has sent a connect request (SNRM) to this secondary and is awaiting its response. • THEMBUSY—This secondary has told this router that it is temporarily unable to receive any more information frames. • USBUSY—This router has told this secondary that it is temporarily unable to receive any more information frames.
VS	Sequence number of the next information frame this station sends.
VR	Sequence number of the next information frame from this secondary that this station expects to receive.
RCNT	Number of correctly sequenced I-frames received when the Cisco IOS software was in a state in which it is acceptable to receive I-frames.
Remote VR	Last frame transmitted by this station that has been acknowledged by the other station.
Current retransmit count	Number of times the current I-frame or sequence of I-frames has been retransmitted.
Hold queue	Number of frames in hold queue/Maximum size of hold queue.
IFRAMEs, RNRs, SNRMs, DISCs	Sent and received count for these frames.
Poll	"Set" if this router has a poll outstanding to the secondary; "clear" if it does not.
Poll count	Number of polls, in a row, given to this secondary at this time.
chain	Shows the previous (p) and next (n) secondary address on this interface in the round-robin loop of polled devices.

Sample show interfaces accounting Display

The following is sample output from the **show interfaces accounting** command:

```
Router# show interfaces accounting
```

```
Interface TokenRing0 is disabled

Ethernet0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP     873171  735923409      34624    9644258
                  Novell     163849   12361626      57143    4272468
                 DEC MOP          0          0          1         77
                     ARP      69618    4177080       1529      91740
Interface Serial0 is disabled

Ethernet1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP          0          0         37      11845
                  Novell          0          0       4591     275460
                 DEC MOP          0          0          1         77
                     ARP          0          0          7        420

Interface Serial1 is disabled
Interface Ethernet2 is disabled
Interface Serial2 is disabled
Interface Ethernet3 is disabled
Interface Serial3 is disabled
Interface Ethernet4 is disabled
Interface Ethernet5 is disabled
Interface Ethernet6 is disabled
Interface Ethernet7 is disabled
Interface Ethernet8 is disabled
Interface Ethernet9 is disabled

Fddi0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                  Novell          0          0        183      11163
                     ARP          1         49          0          0
```

When the output indicates that an interface is “disabled,” the router has received excessive errors (over 5000 in a keepalive period).

Example with Flow-Based WRED

The following is sample output from the **show interfaces** command issued for the serial interface 1 for which flow-based WRED is enabled. The output shows that there are 8 active flow-based WRED flows, that the maximum number of flows active at any time is 9, and that the maximum number of possible flows configured for the interface is 16:

```
Router# show interfaces serial 1

Serial1 is up, line protocol is up

  Hardware is HD64570
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
Reliability 255/255, txload 237/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
  Last input 00:00:22, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:17:58
  Input queue: 0/75/0 (size/max/drops); Total output drops: 2479
Queueing strategy: random early detection(RED)
    flows (active/max active/max): 8/9/16
    mean queue depth: 27
    drops: class  random   tail     min-th   max-th   mark-prob
           0      946      0        20       40       1/10
```

```
          1      488       0        22       40       1/10
          2      429       0        24       40       1/10
          3      341       0        26       40       1/10
          4      235       0        28       40       1/10
          5      40        0        31       40       1/10
          6      0         0        33       40       1/10
          7      0         0        35       40       1/10
          rsvp   0         0        37       40       1/10
  30 second input rate 1000 bits/sec, 2 packets/sec
  30 second output rate 119000 bits/sec, 126 packets/sec
     1346 packets input, 83808 bytes, 0 no buffer
     Received 12 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     84543 packets output, 9977642 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Example with DWFQ

The following is sample output from the **show interfaces** command when distributed weighted fair queueing (DWFQ) is enabled on an interface. Notice that the queueing strategy is listed as "VIP-based fair queueing."

```
Router# show interfaces fastethernet 1/1/0

Fast Ethernet 1/1/0 is up, line protocol is up
  Hardware is cyBus Fast Ethernet Interface, address is 0007.f618.4448 (bia 00e0)
  Description: pkt input i/f for WRL tests (to pagent)
  Internet address is 10.0.2.70/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 01:11:01, output hang never
  Last clearing of "show interface" counters 01:12:31
  Queueing strategy: VIP-based fair queueing
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1 packets output, 60 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffers copied, 0 interrupts, 0 failures
```

Example with DNIS Binding

When the **show interfaces** command is issued on an unbound dialer interface, the output looks as follows:

```
Router# show interfaces dialer0

Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 3/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
```

```
  Last input 00:00:34, output never, output hang never
  Last clearing of "show interface" counters 00:05:09
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
     18 packets input, 2579 bytes
     14 packets output, 5328 bytes
```

But when the **show interfaces** command is issued on a bound dialer interface, you will get an additional report that indicates the binding relationship. The output is shown here:

```
Router# show interfaces dialer0

Dialer0 is up, line protocol is up
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Interface is bound to BRI0:1
  Last input 00:00:38, output never, output hang never
  Last clearing of "show interface" counters 00:05:36

Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38 packets input, 4659 bytes
     34 packets output, 9952 bytes
Bound to:
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation PPP)
  LCP Open, multilink Open
  Last input 00:00:39, output 00:00:11, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     78 packets input, 9317 bytes, 0 no buffer
     Received 65 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     93 packets output, 9864 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     4 carrier transitions
```

At the end of the Dialer0 output, the **show interfaces** command is executed on each physical interface bound to it.

Example with BRI

In this example, the physical interface is the B1 channel of the BRI0 link. This example also illustrates that the output under the B channel keeps all hardware counts that are not displayed under any logical or virtual access interface. The line in the report that states "Interface is bound to Dialer0 (Encapsulation

LAPB)" indicates that this B interface is bound to Dialer0 and the encapsulation running over this connection is Link Access Procedure, Balanced (LAPB), not PPP, which is the encapsulation configured on the D interface and inherited by the B channel.

```
Router# show interfaces bri0:1

BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation LAPB)
  LCP Open, multilink Open
  Last input 00:00:31, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     110 packets input, 13994 bytes, 0 no buffer
     Received 91 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     135 packets output, 14175 bytes, 0 underruns
     0 output errors, 0 collisions, 12 interface resets
     0 output buffer failures, 0 output buffers swapped out
     8 carrier transitions
```

Any protocol configuration and states should be displayed from the Dialer0 interface.

Example with a Fast Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces fastethernet** command for the second interface (port 1) in a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the Modular Service Cards (MSC) that is installed in slot 2 on a Cisco 7304 router:

```
Router# show interfaces fastethernet 2/1/1

FastEthernet2/1/1 is up, line protocol is up
  Hardware is SPA-4FE-7304, address is 00b0.64ff.5d80 (bia 00b0.64ff.5d80)
  Internet address is 192.168.50.1/24
  MTU 9216 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:22, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 320 bytes
     Received 1 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     8 packets output, 529 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Example for an Interface with an Asymmetric Receiver and Transmitter Rates

```
Router# show interfaces e4/0

Ethernet4/0 is up, line protocol is up
  Hardware is AmdP2, address is 000b.bf30.f470 (bia 000b.bf30.f470)
  Internet address is 10.1.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, RxBW 5000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 254/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:03:36
  Input queue: 34/75/0/819 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7138000 bits/sec, 14870 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     3109298 packets input, 186557880 bytes, 0 no buffer
     Received 217 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     22 packets output, 1320 bytes, 0 underruns
     11 output errors, 26 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Table 5 describes the significant fields shown in the display.

Table 5 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA

Field	Description
Fast Ethernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-4FE-7304) and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 4-Port 10/100 Fast Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
RxBW	Receiver bandwidth of the interface, in kilobits per second. This value is displayed only when an interface has asymmetric receiver and transmitter rates.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.

Table 5 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)

Field	Description
txload, rxload	Load on the interface (in the transmit "tx" and receive "rx" directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of selective packet discard (SPD). SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.

Table 5 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)

Field	Description
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is first-in, first-out (FIFO).
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 4-Port 10/100 Fast Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the maximum transmission unit (MTU) for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

Table 5 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.

Table 5 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)

Field	Description
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router.

Example with a Gigabit Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces gigabitethernet** command for the first interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show interfaces gigabitethernet 4/0/0

GigabitEthernet4/0/0 is up, line protocol is down
  Hardware is SPA-2GE-7304, address is 00b0.64ff.5a80 (bia 00b0.64ff.5a80)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 1000Mb/s, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     109 packets output, 6540 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Example with Gigabit Ethernet SPAs Configured as Primary and Backup Interfaces on a Cisco 7600 Router

The following examples show the additional lines included in the display when the command is issued on two Gigabit Ethernet interfaces that are configured as a primary interface (gi3/0/0) and as a backup interface (gi3/0/11) for the primary:

```
Router# show interfaces gigabitEthernet 3/0/0

GigabitEthernet3/0/0 is up, line protocol is up (connected)
  Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/0/11, failure delay 0 sec, secondary disable delay 0 sec,
  .
  .
  .

Router# show interfaces gigabitEthernet 3/0/11

GigabitEthernet3/0/11 is standby mode, line protocol is down (disabled)
```

.
.
.

Table 6 describes the fields shown in the display for Gigabit Ethernet SPA interfaces.

Table 6 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA

Field	Description
GigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-2GE-7304) and MAC address.
Backup interface	Identifies the backup interface that exists for this, the primary interface.
Failure and secondary delay	The period of time (in seconds) to delay bringing up the backup interface when the primary goes down, and bringing down the backup after the primary becomes active again. On the Cisco 7600 router, the delay must be 0 (the default) to ensure that there is no delay between when the primary goes down and the backup comes up, and vice versa.
Standby mode	Indicates that this is a backup interface and that it is currently operating in standby mode.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 2-Port 10/100/1000 Gigabit Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
1000Mb/s, 100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
link type	Specifies whether autonegotiation is being used on the link.
media type	Interface port media type: RJ45, SX, LX, or ZX.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.

Table 6 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Table 6 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 2-Port 10/100/1000 Gigabit Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the MTU for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.

Table 6 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.

Example with a Packet over SONET/SDH (POS) SPA on a Cisco 7600 Series Router and Catalyst 6500 Series Switch

The following is sample output from the **show interfaces pos** command on a Cisco 7600 series router or Catalyst 6500 series switch for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show interfaces pos 4/3/0

POS4/3/0 is up, line protocol is up  (APS working - active)
  Hardware is Packet over SONET
  Internet address is 10.0.0.1/8
  MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
  Last input 00:00:34, output 04:09:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 622000 kilobits/sec
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   782 packets input, 226563 bytes, 0 no buffer
   Received 0 broadcasts, 1 runts, 0 giants, 0 throttles
            0 parity
   1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   271 packets output, 28140 bytes, 0 underruns
   0 output errors, 0 applique, 2 interface resets
   0 output buffer failures, 0 output buffers swapped out
   2 carrier transitions
```

Table 7 describes the significant fields shown in this display.

Table 7 show interfaces pos Field Descriptions—POS SPA

Field	Description
POS4/3/0 is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type: • For POSIP—cyBus Packet over SONET • For POS SPAs—Packet over SONET
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.
Scramble	Indicates whether SONET payload scrambling is enabled. SONET scrambling is disabled by default. For the POS SPAs on the Cisco 12000 series routers, scrambling is enabled by default.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Table 7 show interfaces pos Field Descriptions—POS SPA (continued)

Field	Description
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 22^{31} ms (and less than 2^{32} ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

Table 7 show interfaces pos Field Descriptions—POS SPA (continued)

Field	Description
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates an unrecoverable error has occurred on the POSIP applique. The system then invokes an interface reset.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a POS SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces pos** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces pos 1/1/0

POS1/1/0 is up, line protocol is up
  Hardware is Packet over SONET
  Internet address is 10.41.41.2/24
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive not set
  Scramble enabled
  Last input 00:00:59, output 00:00:11, output hang never
  Last clearing of "show interface" counters 00:00:14
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 9582482 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 314 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Example with a POS SPA SDCC Interface on a Cisco 12000 Series Router

The following is sample output from the **show interfaces sdcc** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces sdcc 1/1/0

SDCC1/1/0 is administratively down, line protocol is down
  Hardware is SDCC
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Table 8 describes the significant fields shown in the display.

Table 8 show interfaces sdcc Field Descriptions—POS SPA

Field	Description
SDCC1/1/0 is administratively down, line protocol is down	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type is SDCC—Section Data Communications Channel.
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
crc	Cyclic redundancy check size (16 or 32 bits).
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Table 8 show interfaces sdcc Field Descriptions—POS SPA (continued)

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 22^{31} ms (and less than 2^{32} ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.

Table 8 show interfaces sdcc Field Descriptions—POS SPA (continued)

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Not supported for POS interfaces.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a T3/E3 Shared Port Adapter

The following example shows the interface serial statistics on the first port of a T3/E3 SPA installed in subslot 0 of the SIP located in chassis slot 5:

```
Router# show interfaces serial 5/0/0

Serial5/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 10.1.1.2/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
```

```
   reliability 255/255, txload 234/255, rxload 234/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 40685000 bits/sec, 115624 packets/sec
5 minute output rate 40685000 bits/sec, 115627 packets/sec
   4653081241 packets input, 204735493724 bytes, 0 no buffer
   Received 4044 broadcasts (0 IP multicast)
   0 runts, 0 giants, 0 throttles
            0 parity
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   4652915555 packets output, 204728203520 bytes, 0 underruns
   0 output errors, 0 applique, 4 interface resets
   0 output buffer failures, 0 output buffers swapped out
  2 carrier transitions
```

Table 9 describes the fields shown in the **show interfaces serial** output for a T3/E3 SPA.

Note The fields appearing in the ouput will vary depending on card type, interface configuration, and the status of the interface.

Table 9 show interfaces serial Field Descriptions—T3/E3 SPA

Field	Description
Serial	Name of the serial interface.
line protocol is	If the line protocol is up, the local router has received keepalive packets from the remote router. If the line protocol is down, the local router has not received keepalive packets form the remote router.
Hardware is	Designates the specific hardware type of the interface.
Internet address is	The IP address of the interface.
MTU	The maximum packet size set for the interface.
BW	Bandwidth in kilobits per second.
DLY	Interface delay in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method.
crc	CRC size in bits.
loopback	Indicates whether loopback is set.

Table 9 show interfaces serial Field Descriptions—T3/E3 SPA (continued)

Field	Description
keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing of show interface counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 milliseconds (and less than 232 ms) ago.
Input queue	Packet statistics on the input queue reported as: • Size—Current size of the input queue. • Max—Maximum size of the input queue. • Drops—Packets dropped because the queue was full. • Flushes—Number of times that data on queue has been discarded.
Total output drops	Total number of dropped packets.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue (size), and the maximum size of the queue (max).

Table 9 show interfaces serial Field Descriptions—T3/E3 SPA (continued)

Field	Description
5-minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
5-minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Example with a 1-Port 10-Gigabit Ethernet SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces tengigabitethernet** command for the only interface (port 0) in a 1-Port 10 Gigabit Ethernet SPA located in the top subslot (0) of the carrier card that is installed in slot 7 on a Cisco 12000 series router:

```
Router# show interfaces tengigabitethernet 7/0/0

TenGigabitEthernet7/0/0 is up, line protocol is up (connected)
  Hardware is TenGigEther SPA, address is 0000.0c00.0102 (bia 000f.342f.c340)
  Internet address is 10.1.1.2/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
  Last clearing of "show interface" counters 20:24:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     237450882 packets input, 15340005588 bytes, 0 no buffer
     Received 25 broadcasts (0 IP multicasts)
```

```
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
1676 packets output, 198290 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

Table 10 describes the significant fields shown in the display.

Table 10 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
TenGigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
10Gb/s	Speed of the interface in Gigabits per second.
input flow control ...	Specifies if input flow control is on or off.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.

Table 10 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Table 10 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
L2 Switched	Provides statistics about Layer 2 switched traffic, including unicast and multicast traffic.
L3 in Switched	Provides statistics about received Layer 3 traffic.
L3 out Switched	Provides statistics about sent Layer 3 traffic.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired.
multicast	Number of multicast packets.
pause input	Number of pause packets received.

Table 10 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
pause output	Number of pause packets transmitted.
output buffer failures, output buffers swapped out	Number of output butters failures and output buffers swapped out.

Displaying Traffic for a Specific Interface Example

This example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet1/1

GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0016.9de5.d9d1 (bia 0016.9de5.d9d1)
  Internet address is 172.16.165.40/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:11, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     10 packets input, 2537 bytes, 0 no buffer
     Received 10 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 46 multicast, 0 pause input
     0 input packets with dribble condition detected
     18 packets output, 3412 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     7 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Note The unknown protocol drops field displayed in the above example refers to the total number of packets dropped due to unknown or unsupported types of protocol. This field occurs on several platforms such as the Cisco 3725, 3745, 3825, and 7507 series routers.

This example shows how to display traffic for a FlexWAN module:

```
Router# show interfaces pos 6/1/0.1

POS6/1/0.1 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.2.2/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY <<<+++ no packets info after this line
Arches#sh mod 6
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  6    0  2 port adapter FlexWAN                   WS-X6182-2PA       SAD04340JY3

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  6  0001.6412.a234 to 0001.6412.a273   1.3   12.2(2004022 12.2(2004022 Ok

Mod Online Diag Status
--- -------------------
  6 Pass
Router#
```

Related Commands

Command	Description
fair-queue	Enables WFQ.
interface	Configures an interface type and enters interface configuration mode.

Command	Description
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers pos	Displays information about the POS controllers.
show controllers serial	Displays controller statistics.

show ip cef platform

To display entries in the Forwarding Information Base (FIB) or to display a summary of the FIB, use the **show ip cef platform** command in privileged EXEC mode.

show ip cef *ip-prefix* [*mask*] **platform** [**checksum | detail | internal checksum**]

Syntax Description

ip-prefix [*mask*]	The IP address prefix of the entries to display. You can also include an optional subnet mask.
checksum	(Optional) Displays FIB entry checksums information.
detail	(Optional) Displays detailed FIB entry information.
internal {**checksum**}	(Optional) Displays internal data structures. The **checksum** option includes FIB entry checksums information in the output.

Command Default

None

Command History

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following example shows FIB entry information for IP address prefix 10.4.4.4:

```
Router# show ip cef 10.4.4.4 platform

10.4.4.4/32
Fib Entry: 0xD6680610 XCM leaf from 0x50805550(RP) 0xA0805550(FP):
load_bal_or_adj[0] 0x0 load_bal_or_adj[1] 0x18 load_bal_or_adj[2] 0x1C
leaf points to an adjacency, index 0x607
ip_mask 0x0 as_number 0x0 precedence_num_loadbal_intf 0xF0 qos_group 0x0
Label object OCE Chain:
Label(0x12, real) Adjacency
c10k_label_data = 0x450467F8
tag_elt_addr = 0x50003038
ipv6_tag_elt_addr = 0x0
tag_index = 0x607
tt_tag_rew = 0x45046800
Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
pktswitched = 0 byteswitched = 0
XCM Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
mac_index_extension = 0x0
XCM mac rewrite from index 0x395
mtu from 0x53800E54(RP) 0xA3800E54(FP)
frag_flags = 0x0
mtu = 1496
mac length 0x12 encap length 0x16 upd_offset=0x02FF
```

```
mac string start from bank4 0x32001CA8(RP)
0x82001CA8(FP)
mac string end from bank9 0x50801CA8(RP)
0xA0801CA8(FP)
Encap String: 0005DC387B180003A011A57881000002884700012000
```

Related Commands

Command	Description
show cef	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ipv6 cef platform

To display platform-specific Cisco Express Forwarding (CEF) data, use the **show ipv6 cef platform** command in user EXEC or privileged EXEC mode.

show ipv6 cef platform [**checksum** | **detail** | **internal**]

Syntax Description

checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed platform-specific Cisco Express Forwarding data.
internal	(Optional) Displays internal platform-specific Cisco Express Forwarding data.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

If none of the optional keywords are used, data for all of the platforms is displayed.

Examples

The following example displays all platform-specific Cisco Express Forwarding data:

```
Router# show ipv6 cef platform
```

show mac address-table

To display the MAC address table, use the **show mac address-table** command in privileged EXEC mode.

show mac address-table [**address** *mac-addr* [**all** | **interface** *type/number* | **module** *number* | **vlan** *vlan-id*] | [**count** [**module** *number* | **vlan** *vlan-id*]] | [**interface** *type/number*] | [**limit** [**vlan** *vlan-id* | **module** *number* | **interface** *interface-type*]] | [**module** *number*] | [**multicast** [**count** | {**igmp-snooping** | **mld-snooping** [**count**] | **user** [**count**] | **vlan** *vlan-id*}]] | [**notification** {**mac-move** [**counter** [*vlan*] | **threshold** | **change**} [**interface** [*interface-number*]]] | [**synchronize statistics**] | [**unicast-flood**] | **vlan** *vlan-id* [**module** *number*]]

Syntax Description

address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address. See the "Usage Guidelines" section for formatting information.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
interface *type/number*	(Optional) Displays addresses for a specific interface; valid values are **atm**, **fastethernet**, **gigabitethernet**, and **port-channel**.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
vlan *vlan-id*	(Optional) Displays addresses for a specific VLAN, valid values are from 1 to 4094.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

If you do not specify a module number, the output of the **show mac address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

The *interface-number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The optional **module** *number* keyword and argument are supported only on DFC modules. The **module** *number* keyword and argument designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the **show mac address-table unicast-flood** command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
  - ALERT—Information is updated approximately every 3 seconds.
  - SHUTDOWN—Information is updated approximately every 3 seconds.

Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

  - Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The **show mac address-table synchronize statistics** command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

The following is sample output from the **show mac address-table** command:

```
Switch# show mac address-table

Dynamic Addresses Count:                 9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:             41
Total MAC addresses:                     50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Note In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

This example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac address-table address 001.6441.60ca

Codes: * - primary entry

  vlan   mac address     type    learn qos            ports
------+----------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
```

This example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac address-table address 0100.5e00.0128

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

This example shows how to display the entry count for a specific slot:

```
Router# show mac address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:                 4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
```

This example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Router# show mac address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
```

Note A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

This example shows how to display the limit information for a specific slot:

```
Router# show mac address-table limit vlan 1 module 1

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          1        7       warning      500      0              enabled
1          1        11      warning      500      0              enabled
1          1        12      warning      500      0              enabled

Router#show mac address-table limit vlan 1 module 2

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          2         7      warning      500      0              enabled
1          2         9      warning      500      0              enabled
```

The following example shows how to display the MAC-move notification status:

```
Router# show mac address-table notification mac-move

MAC Move Notification: Enabled
Router#
```

The following example shows how to display the MAC move statistics:

```
Router> show mac address-table notification mac-move counter
```

```
-------------------------------------------------------------------------------
Vlan Mac Address From Mod/Port To Mod/Port Count
---- ---------------- ---------------------- ---------------------- ------------
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac address-table notification threshold

Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

This example shows how to display the MAC notification parameters and history table:

```
Router# show mac address-table notification change

MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
--------------------------------------------------
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
```

This example shows how to display the MAC notification parameters and history table for a specific interface:

```
Router# show mac address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
GigabitEthernet5/2          Disabled       Disabled
```

This example shows how to display unicast-flood information:

```
Router# show mac address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > ------+----------+-----------------+----------
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> >-----+------+----------------+-----------------------------+------------------
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> >------+---------------+-------------------------------------------------
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
```

```
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

This example shows how to display the information about the MAC address table for a specific VLAN:

```
Router# show mac address-table vlan 1300

     vlan  mac address     type    learn   age            ports
----+----+---------------+-------+-----+----------+--------------------------
*    1300 2000.0000.0031  dynamic  Yes     0         VPLS peer 100.0.0.77(2:1)
```

This example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Router# show mac address-table multicast mld-snooping

vlan mac address type learn qos ports
-----+---------------+--------+-----+---+--------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

Related Commands

Command	Description
clear mac address-table	Deletes entries from the MAC address table.
mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac address-table limit	Enables MAC limiting.
mac address-table notification mac-move	Enables MAC-move notification.
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
mac address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac address-table static	Displays static MAC address table entries only.

show mac address-table aging-time

To display the MAC address aging time, use the **show mac address-table aging-time** command in privileged EXEC mode.

show mac address-table aging-time [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 1005.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced

Examples

The following example shows how to display the current configured aging time for all VLANs. The fields shown in the display are self-explanatory.

```
Router# show mac address-table aging-time

Vlan    Aging Time
----    ----------
100     300
200     1000
```

The following example shows how to display the current configured aging time for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router# show mac address-table aging-time vlan 100

Vlan    Aging Time
----    ----------
 100    300
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table detail	Displays detailed MAC address table information.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table multicast	Displays multicast MAC address table information.
show mac address-table protocol	Displays MAC address table information based on protocol.

Command	Description
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac address-table dynamic

To display dynamic MAC address table entries only, use the **show mac address-table dynamic** command in privileged EXEC mode.

show mac address-table dynamic [{**address** *mac-addr*} | {**interface** *interface interface-num* [**all** | **module** *number*]} | {**module** *num*} | {**vlan** *vlan-id* [**all** | **module** *number*]}]

Syntax Description

address *mac-addr*	(Optional) Specifies a 48-bit MAC address; valid format is H.H.H.
interface *interface interface-num*	(Optional) Specifies an interface to match. Valid type values are FastEthernet and GigabitEthernet, valid number values are from 1 to 9.
all	(Optional) Specifies that the output display all dynamic MAC address table entries.
module *num*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
vlan *vlan-*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The *mac-address* is a 48-bit MAC address and the valid format is H.H.H.

The optional **module** *num* keyword and argument are supported only on DFC modules. The **module** *num* keyword and argument designate the module number.

Examples

This example shows how to display all the dynamic MAC address entries for a specific VLAN.

```
Router# show mac address-table dynamic vlan 200 all

Legend: * - primary entry
        age - seconds since last seen
        n/a - not aevailable
vlan     mac address      type   learn    age              ports
------+----------------+--------+-----+----------+--------------------------
 200  0010.0d40.37ff   dynamic    NO      23        Gi5/8
Router#
```

This example shows how to display all the dynamic MAC address entries.

```
Router# show mac address-table dynamic

Legend: * - primary entry
age - seconds since last seen
n/a - not applicable
vlan     mac address      type   learn    age              ports
```

```
------+----------------+--------+-----+----------+--------------------------
* 10   0010.0000.0000   dynamic  Yes   n/a        Gi4/1
* 3    0010.0000.0000   dynamic  Yes   0          Gi4/2
* 1    0002.fcbc.ac64   dynamic  Yes   265        Gi8/1
* 1    0009.12e9.adc0   static   No    -          Router
Router#
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.
show mac address-table aging-time	Displays the MAC address aging time.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table detail	Displays detailed MAC address table information.
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table multicast	Displays multicast MAC address table information.
show mac address-table protocol	Displays MAC address table information based on protocol.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac address-table learning

To display the MAC address learning state, use the **show mac address-table learning** command in user EXEC mode.

show mac address-table learning [**vlan** *vlan-id* | **interface** *interface slot/port*] [**module** *num*]

Syntax Description

vlan *vlan-id*	(Optional) Displays information about the MAC address learning state for the specified switch port VLAN; valid values are from 1 to 4094.
interface *interface slot/port*	(Optional) Displays information about the MAC address learning state for the specified routed interface type, the slot number, and the port number.
module *num*	(Optional) Displays information about the MAC address learning state for the specified module number.

Defaults

This command has no default settings.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The **module** *num* keyword and argument can be used to specify supervisor engines or Distributed Forwarding Cards (DFCs) only.

The **interface** *interface slot/port* keyword and arguments can be used on routed interfaces only. The **interface** *interface slot/port* keyword and arguments cannot be used to configure learning on switch port interfaces.

If you specify the **vlan** *vlan-id*, the state of the MAC address learning of the specified VLAN on all modules, including router interfaces, is displayed.

If you specify the **vlan** *vlan-id* and the **module** *num*, the state of the MAC address learning of a specified VLAN on a specified module is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC address learning of the specified interface on all modules is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC address learning of the specified interface on the specified module is displayed.

If you enter the **show mac address-table learning** command with no arguments or keywords, the status of MAC learning on all the existing VLANs on all the supervisor engines or DFCs configured on a Cisco 7600 series router is displayed.

Examples

This example shows how to display the MAC address learning status on all the existing VLANs on all of the supervisor engines or DFCs configured on a Cisco 7600 series router:

```
Router# show mac address-table learning

VLAN/Interface          Mod1   Mod4   Mod7
--------------------    ---------------------
1                       yes    yes    yes
100                     yes    yes    yes
150                     yes    yes    yes
200                     yes    yes    yes
250                     yes    yes    yes
1006                     no     no     no
1007                     no     no     no
1008                     no     no     no
1009                     no     no     no
1010                     no     no     no
1011                     no     no     no
1012                     no     no     no
1013                     no     no     no
1014                     no     no     no
GigabitEthernet6/1       no     no     no
GigabitEthernet6/2       no     no     no
GigabitEthernet6/4       no     no     no
FastEthernet3/4          no     no     no
FastEthernet3/5          no     no     no
GigabitEthernet4/1       no     no     no
GigabitEthernet4/2       no     no     no
GigabitEthernet7/1       no     no     no
GigabitEthernet7/2       no     no     no

Router#
```

Table 11 describes the fields that are shown in the example.

Table 11 show mac address-table learning Field Descriptions

Field	Description
VLAN/Interface[1]	VLAN ID or interface type, module, and port number.
Mod#	Module number of a supervisor engine or DFC.
yes	MAC address learning is enabled.
no	MAC address learning is disabled.

1. The interfaces displayed are routed interfaces that have internal VLANs assigned to them.

This example shows how to display the status of MAC address learning on all the existing VLANs on a single supervisor engine or a DFC:

```
Router# show mac address-table learning module 4

VLAN/Interface          Mod4
--------------------    -----
1                       yes
100                     yes
150                     yes
200                     yes
250                     yes
1006                     no
1007                     no
1008                     no
```

```
1009                    no
1010                    no
1011                    no
1012                    no
1013                    no
1014                    no
GigabitEthernet6/1      no
GigabitEthernet6/2      no
GigabitEthernet6/4      no
FastEthernet3/4         no
FastEthernet3/5         no
GigabitEthernet4/1      no
GigabitEthernet4/2      no
GigabitEthernet7/1      no
GigabitEthernet7/2      no

Router#
```

This example shows how to display the status of MAC address learning for a specific VLAN on all the supervisor engines and DFCs:

```
Router# show mac address-table learning vlan 100

VLAN    Mod1   Mod4   Mod7
----    ---------------------
100      no     no     yes
Router
```

This example shows how to display the status of MAC address learning for a specific VLAN on a specific supervisor engine or DFC:

```
Router# show mac address-table learning vlan 100 module 7

VLAN    Mod7
----    -----
100     yes
Router
```

This example shows how to display the status of MAC address learning for a specific supervisor engine or DFC:

```
Router# show mac address-table learning interface FastEthernet 3/4

Interface       Mod1   Mod4   Mod7
---------       ---------------------
Fa3/4            no     yes    no
Router
```

This example shows how to display the status of MAC address learning for a specific interface on a specific supervisor engine or DFC:

```
Router# show mac address-table learning interface FastEthernet 3/4 module 1

Interface       Mod1
---------       -----
Fa3/4            no
Router
```

Related Commands

Command	Description
mac address-table learning	Enables MAC address learning.

show mac address-table static

To display static MAC address table entries only, use the **show mac address-table static** command in privileged EXEC mode.

show mac address-table static [**address** *mac-address* | **aging-time routed-mac** | **interface** *type number* | **module** *number* | **notification** {**change** | **mac-move**} | **synchronize statistics** | **vlan** *vlan-id*]

Syntax Description

address *mac-address*	(Optional) Specifies a 48-bit MAC address to match; valid format is H.H.H.
aging-type routed-mac	(Optional) Specifies the routed MAC address status.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface *type number*	(Optional) Specifies an interface to match; valid type values are Ethernet, FastEthernet, and Gigabit Ethernet and valid number values are from 1 to 9.
module *number*	(Optional) Specifies a module to match; valid values are from 1 to 4.
notification change	(Optional) Specifies the MAC address notification parameters and history table.
notification mac-move	(Optional) Specifies status for the MAC address move notifications.
synchornize statistics	(Optional) Specifies the statistics for MAC address synchronzation.
vlan *vlan*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The keyword definitions for the protocol argument are:

- **ip**—Specifies IP protocol.
- **ipx**—Specifies Internetwork Packet Exchange (IPX) protocols.
- **assigned**—Specifies assigned protocol entries.
- **other**—Specifies other protocol entries.

Examples

The followig examples shows how to display the static MAC address entries:

```
Router# show mac address-table static

*Oct 22 12:15:35: %SYS-5-CONFIG_I: Configured from console by console
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Router
 100  0050.3e8d.6400  static   assigned  --  Router
```

```
4092  0050.f0ac.3058  static      other  --  Router
 917  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
   5  0050.3e8d.6400  static   assigned  --  Router
 303  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 850  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
1002  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 802  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
   2  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 304  0100.5e00.0001  static         ip  --  Fa5/9,Switch
.
```

The following example shows how to display static MAC address entries with a specific protocol type (in this case, assigned):

```
Router# show mac address-table static protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Router
 100  0050.3e8d.6400  static   assigned  --  Router
   5  0050.3e8d.6400  static   assigned  --  Router
```

The following example shows the detailed output for the previous example:

```
Router# show mac address-table static protocol assigned detail

       MAC Table shown in details
=======================================
 Type   Always Learn Trap Modified Notify Capture Protocol Flood
-------+------------+----+--------+------+-------+--------+-----+
     QoS bit      L3 Spare   Mac Address  Age Byte Pvlan Xtag SWbits Index
-----------------+--------+--------------+--------+-----+----+------+-----
STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      200    1     0     0x3

STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      100    1     0     0x3

STATIC      NO        NO     NO      NO     NO    assigned   NO
   Bit Not On        0     0050.3e8d.6400  254      5      1     0     0x3

S   Bit Not On        0     0050.f0ac.3058  254      4092   1     0     0x3
.
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.
show mac address-table aging-time	Displays the MAC address aging time.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table detail	Displays detailed MAC address table information.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table multicast	Displays multicast MAC address table information.

Command	Description
show mac address-table protocol	Displays MAC address table information based on protocol.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mvr

To display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible), use the **show mvr** privileged EXEC command.

show mvr

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0(1)SY	This command was introduced.

Examples

This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **interface** and **members** keywords are appended to the command.
show mvr members	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

show mvr interface

To display the Multicast VLAN Registration (MVR) receiver and source ports, use the **show mvr interface** privileged EXEC command without keywords . Use the command with keywords to display MVR parameters for a specific receiver port.

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]]

Syntax Description

interface-id	(Optional) Displays MVR type, status, and Immediate Leave setting for the interface; valid interfaces include physical ports (including type, stack member [stacking-capable switches only] module, and port number).
members	(Optional) Displays all MVR groups to which the specified interface belongs.
vlan *vlan-id*	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0(1)SY	This command was introduced.

Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface appear. If you enter a VLAN ID, all MVR group members in the VLAN appear.

Examples

This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port        Type            Status          Immediate Leave
----        ----            -------         ---------------
Gi1/0/1      SOURCE          ACTIVE/UP       DISABLED
Gi1/0/2      RECEIVER        ACTIVE/DOWN     DISABLED
```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Inactive means that the port is not yet part of any VLAN.
- Up/Down means that the port is forwarding/nonforwarding.

This is an example of output from the **show mvr interface** command for a specified port:

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface** *interface-id* **members** command:

```
Switch# show mvr interface gigabitethernet1/0/2 members
239.255.0.0     DYNAMIC ACTIVE
239.255.0.1     DYNAMIC ACTIVE
239.255.0.2     DYNAMIC ACTIVE
239.255.0.3     DYNAMIC ACTIVE
239.255.0.4     DYNAMIC ACTIVE
239.255.0.5     DYNAMIC ACTIVE
239.255.0.6     DYNAMIC ACTIVE
239.255.0.7     DYNAMIC ACTIVE
239.255.0.8     DYNAMIC ACTIVE
239.255.0.9     DYNAMIC ACTIVE
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

To display all receiver and source ports that are currently members of an IP multicast group, use the **show mvr members** privileged EXEC command.

show mvr members [*ip-address*]

Syntax Description

ip-address	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0(1)SY	This command was introduced.

Usage Guidelines

The **show mvr members** command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.

Examples

This example shows the status of all mvr members:

```
Switch# show mvr members
MVR Group IP    Status          Members
------------    ------          -------
239.255.0.1     ACTIVE          Gi1/0/1(d), Gi1/0/5(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None

<output truncated>
```

This example shows the status of an IP address and the members of the IP multicast group with that IP address:

```
Switch# show mvr members 239.255.0.2
239.255.003.--22     ACTIVE          Gi1//1(d), Gi1/0/2(d), Gi1/0/3(d),
                                     Gi1/0/4(d), Gi1/0/5(s)
```

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **members** keyword is appended to the command.

show platform acl

To display ACL software-switched setting, use the **show platform acl** command.

show platform acl {**software-switched**}

Syntax Description

software-switched	Displays the ACL software-switched setting.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to display software-switched platform ACLs:

```
Router# show platform acl software-switched
```

Related Commands

Command	Description
platform acl software-switched	Configures the platform ACL software-switched settings.

show platform acl software-switched

To display whether ACLs are enabled for software-switched WAN packets, use the **show platform acl software-switched** command in privileged EXEC mode.

show platform acl software-switched

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

By default, ACLs are not applied to packets that are software-switched between WAN cards and the route processor. To determine whether ACLs are enabled for software-switched ingress or egress WAN packets, use the **show platform acl software-switched** command.

Examples

This example shows how to display whether ACLs are enabled for software-switched WAN packets:

```
Router# show platform acl software-switched
 CWAN: ACL treatment for software switched in INGRESS is enabled
 CWAN: ACL treatment for software switched in EGRESS is disabled
```

Related Commands

Command	Description
platform cwan acl software-switched	Allows ACLs to be applied to WAN packets that are software-switched.

show platform bridge

To display distributed or hardware-based bridging information, use the **show platform bridge** command in privileged EXEC mode.

show platform bridge [*interface-type interface-number*] [**vlan** *vlan-id*] [**summary**]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.
vlan *vlan-id*	(Optional) Displays VLAN bridging information.
summary	(Optional) Displays a summary of bridging information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following is sample output from the **show platform bridge** command:

```
Router# show platform bridge

VLAN Interface            CircuitId  LTL  PseudoPort State Options
  12 PO1/1/3.1               102    0xC3F    1/256   up    dot1q
  13 PO1/1/3.1               103    0xC3F    1/256   up    dot1q
  14 PO1/1/3.2               104    0xC3F    1/256   up    default
  15 PO1/1/3.2               105    0xC3F    1/256   up    default
  16 PO1/1/3.3               106    0xC3F    1/256   up    dot1q-tunnel
  17 PO1/1/3.3               107    0xC3F    1/256   up    dot1q-tunnel
  41 Gi8/0/17               1201    0xDE2    8/227   up    access
  41 Gi8/0/17               1202    0xDE3    8/228   up    access
  41 Gi8/0/17               1203    0xDE4    8/229   up    access
  41 Gi8/0/17               1204    0xDE5    8/230   up    access
  41 Gi8/0/17               1205    0xDE6    8/231   up    access
  41 Gi8/0/17               1206    0xDE7    8/232   up    access
  41 Gi8/0/17               1207    0xDE8    8/233   up    access
  41 Gi8/0/17               1208    0xDE9    8/234   up    access
  41 Gi8/0/17               1209    0xDEA    8/235   up    access
  41 Gi8/0/17               1210    0xDEB    8/236   up    access
  41 Gi8/0/17               1211    0xDEC    8/237   up    access
  41 Gi8/0/17               1212    0xDED    8/238   up    access
  41 Gi8/0/17               1213    0xDEE    8/239   up    access
  41 Gi8/0/17               1214    0xDEF    8/240   up    access
  41 Gi8/0/17               1215    0xDF0    8/241   up    access
```

Table 12 describes the significant fields shown in the display.

Table 12 show platform bridge Field Descriptions

Field	Description
VLAN	The VLAN for which bridging is configured.
Interface	The WAN interface on which bridging is configured. This can be an ATM, Gigabit Ethernet, PoS, or serial interface.
CircuitId	The circuit ID. The range is from 0 to 65536.
LTL	The local target logic (LTL) of the interface. LTL is 13-bits long. The format is eee ssss pppppp (e=extended port bits, s=slot bits, p=port bits). Extended bits along with port bits identify the pseudoport and slot bits identifies the slot.
PseudoPort	In the case of FlexWAN, the port numbering is from 133 to 192 for Bay 0 and 197 to 256 for Bay 1. There are 60 ports per packet processing engine (PPE). For the SIP200, the pseudoports are in the range of 137 to 256.
State	State indicates the status of the physical interface on which bridging is configured. The state is either up or down. If the state is down, then there is a problem and debugging needs to be done.
Options	Options specify whether split-horizon is enabled on the WAN interface. This can be access, default, dot1q, or dot1q-tunnel.

Related Commands

Command	Description
show platform	Displays platform information.

show platform cfib

To display platform FIB information, use the **show platform cfib** command.

show platform cfib

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to display platform FIB information:

```
Router# show platform cfib
```

Related Commands

Command	Description
platform cfib	Performs platform FIB configuration.

show platform cfm

To display connectivity fault management (CFM) commands, use the **show platform cfm** command in privileged EXEC mode.

show platform cfm {**db** | **info** | **interface** {**gigabitethernet** | **port-channel** | **tengigabitethernet**} *number* }

Syntax Description

db	Displays CFM DB details.
info	Displays the CFM Platform Adaptation Layer (PAL) information.
interface	Specifies the interface type.
gigabitethernet	Specifies the Gigabit Ethernet interface.
port-channel	Specifies the port channel interface.
tengigabitethernet	Specifies the 10-Gigabit Ethernet interface.
number	Interface number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following is sample output from the **show platform cfm info** command. The field descriptions are self-explanatory.

```
Router# show platform cfm info

CFM is disabled
 CFM unicast MAC 00d0.2b6c.b103, CFM multicast MAC 0180.c200.0030, AEB multicast MAC
0100.0ccc.ccc0
 CFM Ingress Control Packet System Statistics:
     Current software Rate Limit Setting: 1100 pkts/sec
     Statistics are collected in intervals of 3 seconds.
     Allow the first 3300 packets to pass each interval, drop thereafter
       Current Ingress Count in this interval: 0 pkts
       In this interval have we Exceeded Rate and Dropped pkts: NO
       For the last 3 intervals the maximum sample had 0 packets in one interval.
```

Related Commands

Command	Description
show platform	Displays platform information.

show platform cts reflector interface

To display platform Cisco Trusted Security (CTS) reflector interface configuration, use the **show platform cts reflector interface** command.

show platform cts reflector interface {**gigabitethernet** *number* | **tengigabitethernet** *number* | **summary**}

Syntax Description

gigabitethernet *number*	Specifies GigabitEthernet interface number. Range is 1–6.
tengigabitethernet *number*	Specifies TenGigabitEthernet interface number. Range is 1–6.
summary	Specifies the platform CTS interface configuration summary.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to display the platform CTS reflector interface configuration for tengigabitethernet interface number 4:

```
Router(config)# show platform cts reflector interface tengigabitethernet 4
```

Related Commands

Command	Description
platform cts	Enables platform CTS configuration.

show platform datapath qos

To display QoS packet data path trace on the platform, use the **show platform datapath qos** command.

show platform datapath qos {**cos | ingress-interface | last | lif | packet-data | pkt-length | recirc | src-index**}

Syntax Description

cos	Specifies the packet ingress CoS.
ingress-interface	Specifies the packet ingress interface (port, subinterface, service instance).
last	Specifies data from the last data path capture.
lif	Specifies packet ingress LIF from Eureka or shim header.
packet-data	Specifies packet header data specification.
pkt-length	Specifies the packet length.
recirc	Specifies the recirculated packet.
src-index	Specifies the packet ingress port source index.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to display QoS packet data from the last data path capture:

```
Router# show platform datapath qos last
```

Related Commands

Command	Description
platform datapath qos	Enables QoS packet data path trace on the platform.

show platform eobc crs-delay

To display Ethernet out-of-band channel (EOBC) Carrier Router Service (CRS) delay on the platform, use the **show platform eobc crs-delay** command.

show platform eobc crs-delay

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to display EOBC CRS delay on the platform:

```
Router# show platform eobc crs-delay
```

Related Commands

Command	Description
platform eobc crs-delay	Configures EOBC CRS delay on the platform.