Cisco 10000 Series Router CLI Command Changes in Cisco IOS Release 12.2(33)SB

First Published: April, 2008

This feature guide describes changes in command line interface (CLI) command behavior in Cisco IOS Release 12.2(33)SB.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for CLI Command Changes" section on page 192.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

- Restrictions for CLI Command Changes, page 1
- Information About CLI Command Changes, page 2
- Additional References, page 13
- Command Reference, page 15
- Feature Information for CLI Command Changes, page 192

Restrictions for CLI Command Changes

Cisco IOS Release 12.2(33)SB or a later release must be running on the router.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About CLI Command Changes

Cisco IOS Release 12.2(33)SB introduces changes to the following CLI commands:

- card Command, page 2
- CoPP-Related show Commands, page 3
- debug ipv6 icmp Command Output for IPv6 ICMP, page 3
- frame-relay broadcast-queue, page 3
- frame-relay switching Command, page 4
- hw-module slot, page 4
- no fair-queue Command, page 4
- plim qos input map Command, page 4
- police Command, page 5
- service-policy Command, page 7
- show atm vp Command, page 8
- show controller Command, page 8
- show diag Command, page 9
- show interfaces Command, page 10
- show policy-map Command and Hierarchical Policies, page 10
- show policy-map Command and Police Actions, page 10
- show pxf cpu ipv6 table Command, page 11
- show pxf cpu queue interface summary Command, page 11
- show vpdn tunnel summary Command, page 11
- snmp-server enable traps alarms Command, page 11
- Virtual-Access show Commands, page 12
- virtual-template snmp Command, page 12
- vpdn enable and vpdn-group Commands, page 12

card Command

Cisco IOS Release 12.2(33)SB introduces the **4jacket-1** keyword and the *spa-type* option for the **card** command. The **4jacket-1** keyword enables you to preprovision a line card slot to accept a Cisco 10000 SIP-600. The *spa-type* option preprovisions a line card slot to accept a shared port adaptor (SPA) interface.

Use the following syntax to preprovision a line card slot to accept a Cisco 10000 SIP-600:

card *slot subslot* **4jacket-1**

Use the following syntax to preprovision a line card slot to accept a SPA interface:

card *slot subslot spa-type*

The following example preprovisions line card slot 3 to accept a Cisco 10000 SIP-600 and a 2-port Gigabit Ethernet SPA in subslot 0:

```
Router(config)# card 3 4jacket-1

Router(config)# card 3/0 spa-2x1ge-v2
```

CoPP-Related show Commands

The router supports the following CoPP-related **show** commands:

- The **show pxf cpu statistics diversion** command displays statistical information about diverted packets. In Cisco IOS Release 12.2(33)SB and later releases, divert causes with the string "ipv6..." display as "v6..." in the output of all **show pxf cpu statistics diversion** commands.
- The output from the **show pxf cpu statistics diversion pxf** command was enhanced in Cisco IOS Release 12.2(33)SB to display the provisioned burst size for any divert causes.
- The **show pxf cpu statistics diversion pxf interface** *interface* command displays statistical information about the divert cause policer on a specific interface. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session. This command was introduced in Cisco IOS Release 12.2(33)SB.
- The **show pxf cpu statistics diversion pxf interface** *vcci* command displays statistical information about the divert cause policer on a specific VCCI. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session. This command was introduced in Cisco IOS Release 12.2(33)SB.
- The **show pxf cpu statistics diversion top** *number* command displays the interfaces, subinterfaces, and sessions with the highest number of punter packets. This command was introduced in Cisco IOS Release 12.2(33)SB.

debug ipv6 icmp Command Output for IPv6 ICMP

In Cisco IOS Release 12.2(33)SB, output from the **debug ipv6 icmp** command displays information similar to the following:

```
ICMPv6: Received echo reply from 2010:1:1:1:1:1:1:2
```

In Cisco IOS Release 12.2(31)SB, the **debug ipv6 icmp** command output displays information similar to the following:

```
ICMPv6: Received ICMPv6 packet from 2010:1:1:1:1:1:1:2, type 129
```

frame-relay broadcast-queue

In Cisco IOS Release 12.2(33)SB, the default queue size for the frame-relay broadcast-queue is 256 packets.

In Cisco IOS Release 12.2(31)SB, the default queue size is 64 packets.

frame-relay switching Command

In Cisco IOS Release 12.2(33)SB, you do not need to configure the **frame-relay switching** command when configuring a Frame Relay interface as the DCE.

In Cisco IOS Release 12.2(31)SB, you must configure the **frame-relay switching** command when you configure a Frame Relay interface as the DCE.

hw-module slot

In Cisco IOS Release 12.2(33)SB, when you enter the **hw-module slot** *slot-number* **reset** command, the software asks you to confirm the command. In Cisco IOS Release 12.2(31)SB, the software does not ask you to confirm the command.

Cisco IOS Release 12.2(33)SB introduces the **hw-module slot** *slot-number* **reload** command on the router. The **reload** keyword enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).

no Commands Removed from the Default Configuration

In Cisco IOS Release 12.2(33)SB, the router removes the following **no** commands from the default configuration:

- **no scripting tcl init**
- **no scripting tcl encdir**
- **no ip dhcp use vrf connection**

no fair-queue Command

In Cisco IOS Release 12.2(33)SB, the router removes the **no fair-queue** command from serial interfaces.

plim qos input map Command

Cisco IOS Release 12.2(33)SB introduces the **plim qos input map** command on the router. This command configures a priority queue on Gigabit Ethernet SPAs, separating high-priority traffic from low-priority traffic and placing the traffic in the appropriate interface queue. The command separates priority and non-priority traffic at the SPA interface processor (SIP) to prevent the dropping of high priority traffic in an oversubscription case. Each shared port adaptor (SPA) supports one priority queue.

The command has the following syntax:

plim qos input map {cos {**enable | ***cos-value* **queue low-latency**} **| ip** {**dscp-based | dscp** *dscp-value* **queue low-latency**} **| ip** {**precedence-based | precedence** *precedence-value* **queue low-latency**} **| ipv6 tc** *tc-value* **queue low-latency | mpls exp** *exp-value* **queue low-latency**

The router supports the following classification types for the prioritization of ingress traffic on the Gigabit Ethernet SPAs:

- VLAN 802.1Q priority bits
- IP DSCP bits
- IP precedence bits
- IPv6 traffic class bits
- MPLS experimental (EXP) bits

police Command

Cisco IOS Release 12.2(33)SB supports a police submode and dual police actions.

The output from the **show policy-map interface** command displays the police actions in the police submode, displaying each action on a new line. Regardless of whether you configure a single action or dual actions for the colors, the police actions display on a new line as shown in the following sample output:

```
Router# show policy-map interface ATM1/0/0.131
ATM1/0/0.131: VC 1/131 -

 Service-policy input: test

  Class-map: prec1 (match-any)
   0 packets, 00 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match: ip precedence 1
    0 packets, 0 bytes
    5 minute rate 0 bps
   Police:
    7504000 bps, 100 limit, 10 extended limit
    conformed 0 packets, 0 bytes; action:
    set-clp-transmit
    set-mpls-exp-imposition-transmit 1
    exceeded 0 packets, 0 bytes; action:
    set-clp-transmit
    violated 0 packets, 0 bytes; action:
    set-clp-transmit

  Class-map: class-default (match-any)
   0 packets, 0 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match: any
   0 packets, 0 bytes
   5 minute rate 0 bps
```

The router supports only the following combinations of dual actions:

- set-clp-transmit and set-mpls-exp-transmit
- set-frde-transmit and set-mpls-exp-transmit
- set-cos-transmit and set-cos-inner-transmit

When configuring the **police** command, if you specify actions and then later modify the configured rate parameters, but not the actions, the specified actions change to the default values if only *one* action is specified for each conform, exceed, and violate color. However, if at least one color has dual actions configured, then modifying only the rate parameters does not change the actions to the default value, but instead preserves the previous actions.

For example, the following sample configuration configures the police rate parameters and only one action for each conform, exceed, and violate color:

```
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 100 0 conform-action set-clp-transmit exceed-action
set-clp-transmit violate-action set-clp-transmit
```

The output from the **show policy-map** command displays the following police configuration:

```
Router# show policy-map test
  Policy Map test
    Class prec1
     police 504000 100 0
      conform-action set-clp-transmit
      exceed-action set-clp-transmit
      violate-action set-clp-transmit
```

The following configuration modifies the police rate parameters, but not the actions:

```
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 750000 100 0
```

The following output from the **show policy-map** command indicates that the color values were changed to the default values. This is because only one action was configured for each color.

```
Router# show policy-map test
  Policy Map test
    Class prec1
     police 752000 100 100
      conform-action transmit
      exceed-action drop
      violate-action drop
```

The following output from the **show policy-map** command displays a police configuration in which the conform color has dual actions configured:

```
Router# show policy-map test
  Policy Map test
    Class prec1
     police 504000 100 0
      conform-action set-clp-transmit
      conform-action set-mpls-exp-imposition-transmit 1
      exceed-action set-clp-transmit
      violate-action set-clp-transmit
```

The following configuration modifies the police rate parameters, but not the actions:

```
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 7500000 100 10
```

The following output from the **show policy-map** command indicates that the color values did not change when the rate parameters were modified. Instead, the original values were preserved.

```
Router# show policy-map test
  Policy Map test
    Class prec1
     police 7500000 100 10
      conform-action set-clp-transmit
      conform-action set-mpls-exp-imposition-transmit 1
      exceed-action set-clp-transmit
      violate-action set-clp-transmit
```

In Cisco IOS Release 12.2(31)SB and later releases, if you modify the police rate parameters, but not the action parameters, the police actions default to **conform-action transmit**, **exceed-action drop**, and **violate-action drop**.

For example, the following sample configuration shows the **police** command configured in the policy map named test. The police actions are set to set-clp-transmit for conforming, exceeding, and violating traffic. The police rate parameters are then changed to 500000, 250, and 200, but no actions are modified. When you display the test policy map again, you can see that the police actions default to transmit, drop, and drop.

```
Router# show policy-map test
Policy Map test
    Class prec1
        police 248000 100 10 conform-action set-clp-transmit exceed-action
        set-clp-transmit violate-action set-clp-transmit
Router#
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 250 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
    Class prec1
        police 504000 250 200 conform-action transmit exceed-action drop violate-action
        drop
```

service-policy Command

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the abbreviated form (**ser**) of the **service-policy** command. Instead, you must spell out the command name **service-** before the router accepts the command.

For example, when attaching a policy map the following error message displays when you attempt to use the abbreviated form of the **service-policy** command:

```
Router(config)# interface gigabit1/1/0
Router(config-if)# ser out ?
% Unrecognized command
Router(config-if)# ser ?
% Unrecognized command
```

When you enter the command as **service-**, the router accepts the command as shown in the following example:

```
Router(config-if)# service- ?
    input   Assign policy-map to the input of an interface
    output  Assign policy-map to the output of an interface
    type    Configure CPL Service Policy
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the **service-policy** command. For example, the router accepts the following commands:

```
Router(config)# interface gigabit1/1/0
Router(config-if)# ser out test
```

show atm vp Command

In Cisco IOS Release 12.2(33)SB, the output from the **show atm vp** command nolonger displays "ATM" as the type of interface, as shown in the following sample output:

```
Router# show atm vp
                    Data   CES   PEAK   CES    Avg/Min Burst  MCR
Interface  VPI   SC  VCs    VCs   Kbps   Kbps   Kbps   Cells   Kbps  CDVT    Status
3/0/0      200 N/A    0      0   2000      0     NA      NA      NA   140.0   ACTIVE
```

In Cisco IOS Release 12.2(31)SB, the output from the **show atm vp** command displays the ATM interface type:

```
Router# show atm vp
                    Data   CES   PEAK   CES    Avg/Min Burst  MCR   CDVT
Interface  VPI   SC  VCs    VCs   Kbps   Kbps   Kbps   Cells   Kbps  Usecs   Status
ATM3/0/0   200         0      0   2000      0     NA      NA      NA   140.0   ACTIVE
```

show controller Command

This section describes the following changes in the **show controller** command:

- show controllers and Loopback CLI Commands, page 8
- show controller and Line Code Information, page 9

show controllers and Loopback CLI Commands

In releases prior to Cisco IOS Release 12.2(33)SB, when you configure the **t1 loopback remote** command on the local router, the command also displays in the running-config file of the far-end router. This is due to the route processor (RP) updating an incorrect parameter when it receives the loopback event message from the line card for loopback requests from the far end.

In Cisco IOS Release 12.2(33)SB, the RP updates the correct parameter and the **show controllers** command correctly displays the loopback CLI commands applied on the local end and displays the loopback events and status received from the line card in response to loopback requests from the far end.

This change in behavior affects the following line cards and is documented in the CSCsm84447 caveat:

- 4-port channelized STM1
- 1-port channelized OC-12
- 6-port channelized T3
- 4-port half-height channelized T3

show controller and Line Code Information

In Cisco IOS Release 12.2(33)SB, the output from the **show controller** command includes line code information for the 6-port channelized T3 line card and the 8-port E3/DS3 line card. However, because SONET line cards do not have a direct physical link at the T3 or E3 level, the output from the **show controller t3** command does not include line code information.

In Cisco IOS Release 12.2(31)SB, the output from the **show controller** command displays line code information. The output of the **show controller t3** command for SONET-based T3 also includes line code information.

The following examples from the **show controller t3** command show the information that displays when the router is running Cisco IOS Release 12.2(33)SB and Cisco IOS Release 12.2(31)SB:

Cisco IOS Release 12.2(33)SB —No Line Code Information Displays

```
Router# show controller t3 5/0/0.1
T3 5/0/0.1 is up. Hardware is C10K CHOC12 line card
    Applique type is Channelized T3.
    Controller is in unchannelized mode.
    No alarms detected.
    MDL transmission is disabled.

    FEAC code received: No code is being received.
    Framing is C-BIT Parity (Configured), Clock Source is Internal.
    DSU mode is cisco, DSU bandwidth is 44210.
```

Cisco IOS Release 12.2(31)SB —Line Code Information Displays

```
Router# show controller t3 5/0/0.1
T3 5/0/0.1 is up. Hardware is C10K CHOC12 line card
    Applique type is Channelized T3.
    Controller is in channelized mode.
    No alarms detected.
    MDL transmission is disabled.

    FEAC code received: No code is being received
    Framing is C-BIT Parity (Configured)
    Line Code is B3ZS, Clock Source is Internal.
```

show diag Command

The **show diag** command has a new **crashdump** option to display any crashdump files collected on the SPA Interface Processor (SIP). The SIP stores the crashdump files by a reference number from 1 to 60.

To view a crashdump file, perform the following steps:

Step 1 Determine the most recent crashdump number:

a. Enter the **show diag** *slot*/*subslot* command.

b. Look for the latest crashdump number in the following section of the command output:

```
Number of crashdumps : output number
```

Step 2 Enter the following command to view the crashdump file:

```
show diag slot/subslot crashdump number
```

Note The subslot value is always zero for the SIP.

show interfaces Command

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

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

show policy-map Command and Hierarchical Policies

In Cisco IOS Release 12.2(33)SB, the output of the **show policy-map** command is slightly different from previous releases when the policy is an hierarchical policy.

For example, in Cisco IOS Release 12.2(33)SB output similar to the following displays when you specify a hierarchical policy in the **show policy-map** command:

```
Router# show policy-map Bronze
policy-map bronze
 class class-default
   shape average 34386000
   service-policy Child
```

In Cisco IOS Release 12.2(31)SB, output similar to the following displays when you specify a hierarchical policy in the **show policy-map** command:

```
Router# show policy-map Gold
policy-map Gold
 Class class-default
   Average Rate Traffic Shaping
   cir 34386000 (bps)
   service-policy Child2
```

show policy-map Command and Police Actions

In Cisco IOS Release 12.2(33)SB, the output from the **show policy-map** command displays police actions on separate lines as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P1
  priority
  police percent 50 25 ms 0 ms
   conform-action transmit
   exceed-action transmit
   violate-action drop
```

In Cisco IOS Release 12.2(31)SB, the output from the **show policy-map** command displays police actions on one line as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P1
  priority
  police percent 50 25 ms 0 ms conform-action transmit exceed-action transmit violate-
action drop
```

show pxf cpu ipv6 table Command

In Cisco IOS Release 12.2(33)SB, the **show pxf cpu ipv6 table** command displays the global table, but does not display the leafs that correspond to the IPv6 prefixes ::1/128 (Loopback) and ::/128 (All Zero). The microcode checks for these prefixes.

The **show pxf cpu ipv6 table** command replaces the **show pxf cpu ipv6** command in Cisco IOS Release 12.2(31)SB.

show pxf cpu queue interface summary Command

In Cisco IOS Release 12.2(33)SB and later releases, the output from the **show pxf cpu queue interface summary** command displays only the physical interface and the number of logical links. The output does not display the number of priority queues, class queues, and so on. This modification applies to the PRE3 and PRE4.

show vpdn tunnel summary Command

In Cisco IOS Release 12.2(33)SB, the **show vpdn tunnel summary** command no longer displays the active PPPoE sessions. Instead, use the **show pppoe sessions** command to display the active sessions.

In Cisco IOS Release 12.2(31)SB, the **show vpdn tunnel summary** command does display the active PPPoE sessions.

snmp-server enable traps alarms Command

In releases prior to Cisco IOS Release 12.2(33)SB, the **snmp-server enable traps alarms** command displayed information about major, minor, critical, and informational alarms.

In Cisco IOS Release 12.2(33)SB, by default, the **snmp-server enable traps alarms** command displays information for informational alarms only. You can enable the following commands separately:

- **snmp-server enable traps alarms critical**
- **snmp-server enable traps alarms major**
- **snmp-server enable traps alarms minor**

Virtual-Access show Commands

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual-access interface (VAI) as **vi***X.Y* in the **show pxf cpu queue** and **show interfaces** commands. Instead, you must spell out the VAI as **virtual-access**.

For example, when you enter the following commands, the router accepts the commands:

```
Router# show pxf cpu queue virtual-access2.1

Router# show interface virtual-access 2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following commands:

```
Router# show pxf cpu queue vi2.1

Router# show interface vi2.1
```

virtual-template snmp Command

The **virtual-template snmp** command has a new default configuration in Cisco IOS Release 12.2(33)SB. The new default configuration was changed from enabled by default to disabled by default: **no virtual-template snmp**. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

vpdn enable and vpdn-group Commands

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, the following warning message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays the following warning message:

```
% VPDN is not enabled
```

Additional References

The following sections provide references related to the CLI command changes.

Related Documents

Related Topic	Document Title
Control Plane Policing (CoPP)	*Control Plane Policing, Release 12.2(31)SB* feature module
Policing	*Cisco 10000 Series Router Quality of Service Configuration Guide* Policing Traffic
Service policies	*Cisco 10000 Series Router Quality of Service Configuration Guide* Attaching service policies
Virtual template	*Cisco 10000 Series Router Software Configuration Guide (formerly the Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide)* Configuring Remote Access to MPLS VPN
VPDN	*Cisco 10000 Series Router Software Configuration Guide (formerly the Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide)* Configuring the Multihop Feature

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

The following commands are modified in the feature documented in this module. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup.

- card
- debug ipv6 icmp
- fair-queue (WFQ)
- frame-relay broadcast-queue
- frame-relay switching Command
- hw-module slot
- plim qos input map Command
- police (policy map)
- scripting tcl encdir
- scripting tcl init
- service-policy Command
- show atm vp
- show controllers (line card image)
- show controllers t3
- show diag
- show interfaces
- show interfaces virtual-access
- show policy-map
- show pxf cpu ipv6 table Command
- show pxf cpu queue
- show pxf cpu statistics
- show vpdn tunnel
- snmp trap link-status
- virtual-template
- vpdn enable
- vpdn group

card

To preprovision a router slot for a particular interface card so that you can configure the interface without that card being physically present in the slot, use the **card** command in global configuration mode. To remove the preprovisioning for a card so that the physical slot reports being empty, use the **no** form of this command.

card {*slot/subslot* | *slot/subslot/bay*} *card-type*

no card {*slot/subslot* | *slot/subslot/bay*}

Cisco 10000 Series Router

card *slot/subslot* **{lchoc12-1 | lgigethernet-l | 1gigethernet-hh-1 | loc12atm-1 | loc12pos-1 | 1oc48dpt-pos-1 | 24che1t1-1 | 4chstm-1 | 4cht3-hh-1| 4oc3atm-1 | 4oc3atm_lr-1 | 4jacket-1 | 6cht3-1 | 6oc3pos-1 | 8e3ds3-1 | 8e3ds3atm-1 | 8fastethernet-1 [mode {e1 | t1}] |** *spa-type***}**

no card slot/subslot

Cisco uBR10012 Universal Broadband Router - Cisco IOS Release 12.2(33)SCB

card {*slot* | *slot/bay*} *card-type*

no card {*slot* | *slot/bay*}

Syntax Description

slot/subslot	Identifies the chassis slot and subslot for the card. The following are the valid values: • *slot*—1 to 8 • *subslot*—0 or 1
slot/subslot/bay	(Cisco uBR100012 router) Identifies the chassis slot and subslot for the Cisco Wideband SIP, and the bay number in the SIP where the Cisco Wideband SPA is located. The following are the valid values: • *slot*—1 to 3 • *subslot*—0 or 1 (0 is always specified) • *bay*—0 (upper bay) or 1 (lower bay)
card-type	Specifies the type of card for which to preprovision the slot. See Table 0-1 for a list of the supported cards, which varies by platform.
lchoc12-1	Preprovisions a line card slot for a 1-Port Channelized OC-12/STM-4 line card.
lgigethernet-l	Preprovisions a line card slot for a 1-Port Gigabit Ethernet line card.
1gigethernet-hh-1	Preprovisions a line card slot for a 1-Port Gigabit Ethernet Half-Height line card.
loc12atm-1	Preprovisions a line card slot for a 1-Port OC-12 ATM line card.
loc12pos-1	Preprovisions a line card slot for a 1-Port OC-12 Packet over SONET line card.
1oc48dpt-pos-1	Preprovisions a line card slot for a 1-Port OC-48/STM-16 Packet over SONET line card.

24che1t1-1	Preprovisions a line card slot for a 24-Port Channelized E1/T1 line card.
4chstm-1	Preprovisions a line card slot for a 4-Port Channelized OC-3/STM-1 line card.
4cht3-hh-1	Preprovisions a line card slot for a 4-port Channelized Half-Height line card.
4oc3atm-1	Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with intermediate-reach optics.
4oc3atm_lr-1	Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with long-reach optics.
4jacket-1	Preprovisions a line card slot in the Cisco 10000 series router to accept a Cisco 10000 SIP-600.
6cht3-1	Preprovisions a line card slot for a 6-Port Channelized T3 line card.
6oc3pos-1	Preprovisions a line card slot for a 6-Port OC-3/STM-1 Packet over SONET line card.
8e3ds3-1	Preprovisions a line card slot for an 8-Port Unchannelized E3/T3 line card.
8e3ds3atm-1	Preprovisions a line card slot for an 8-Port E3/DS3 ATM line card.
8fastethernet-1	Preprovisions a line card slot for an 8-Port Fast Ethernet Half-Height line card.
mode {e1 | t1}	Indicates the mode of operation of the 24-Port Channelized E1/T1 line card.
spa-type	Specifies the SPA type to preprovision a SPA interface.

Command Default

An empty card slot is not preprovisioned and cannot be configured or displayed.

The default mode of operation for the 24-Port Channelized E1/T1 line card is E1.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)ST	This command was introduced on the Cisco 10000 series routers.
12.0(21)SX	This command was integrated into Cisco IOS Release 12.0(21)SX.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(1)XF1	This command was introduced on the Cisco uBR10012 Universal Broadband Router for the following line cards: • Cisco uBR-LCP-MC28C cable interface line card • Cisco uBR-LCP-MC28C-BNC cable interface line card • Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card • Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card
12.2(4)XF1	Support was added for the Cisco uBR-LCP-MC16C and Cisco uBR-LCP-MC16E cable interface line cards.

Release	Modification
12.2(4)BC1	Support was added for the Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
12.2(8)BC1	Support was added for the Cisco LCP2 line card processor, and all of its combinations with the supported cable interface line cards.
12.2(11)BC3	Support was added for the Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card and Cisco uBR-MC5X20S cable interface line card.
12.2(15)BX	This command was integrated into Cisco IOS Release 12.2(15)BX.
12.2(15)CX1	Support was added for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards.
12.2(15)BC2	Support was added for the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20U cable interface line cards.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command was modified to support the 4-port Channelized Half-Height line card and the 4-Port OC-3/STM-1 ATM line card with long-reach optics by adding the **4cht3-hh-1** and the **4oc3atm_lr-1** keywords.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.3(21)BC	Support was added for the Cisco Wideband SIP and Wideband SPA.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SB	This command was enhanced to provide the **4jacket-1** keyword and the *spa-type* option, which enable you to preprovision a line card slot to accept a Cisco 10000 SIP-600 and a SPA interface, respectively. This enhancement was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB. Support for the Cisco SIP-600 was added. This command was modified to change the addressing format for: • SIPs—From *slot*/*subslot* to *slot* • SPAs—From *slot*/*subslot*/*bay* to *slot*/*bay*

Usage Guidelines

This command is supported on the Cisco uBR10012 Universal Broadband Router and the Cisco 10000 series routers. For platform-specific information about using this command, see the other platform-specific sections of this topic.

Use this command to preprovision a slot in the router to accept a particular line card, so that you can configure the interface without the card being physically present in the chassis. This command allows system administrators to plan for future configurations, without having to wait for the physical hardware to first arrive. When the line card does arrive, the installer can bring the card online by inserting the card into the chassis and connecting the necessary cables, without having to do any further configuration using the command-line interface.

The type of card must be appropriate for the slot being specified. The list of supported card types depends on the Cisco IOS software release in use and your platform. For the latest information about supported hardware for your platform, see the release notes that correspond to your Cisco IOS software release and platform.

Table 0-1 lists the types of cards that are supported as *card-types* for the **card** command:

Table 0-1 Card Types Supported by the card Command

Card Type	Description
1cable-mc16c	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-LCP-MC16C or Cisco uBR-LCP2-MC16C cable interface line card.
1cable-mc16e	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-LCP-MC16E or Cisco uBR-LCP2-MC16E cable interface line card.
1cable-mc16s	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-LCP-MC16S or Cisco uBR-LCP2-MC16S cable interface line card.
lchoc12-1	(Cisco 10000 series router) Preprovisions a line card slot for a 1-Port Channelized OC-12/STM-4 line card.
1gigethernet-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card.
1gigethernet-hh-1	(Cisco 10000 series router) Preprovisions a line card slot for a 1-Port Gigabit Ethernet Half-Height line card.
loc12atm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 1-Port OC-12 ATM line card.
1oc12pos-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card.
1oc48dpt-pos-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card.
2cable-mc28bnc	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-LCP-MC28C-BNC or Cisco uBR-LCP2-MC28C-BNC cable interface line card.
2cable-mc28c	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-LCP-MC28C or Cisco uBR-LCP2-MC28C cable interface line card.
2cable-tccplus	(Cisco uBR10012 router) Preprovisions a slot for a Timing, Control, and Communications Plus (TCC+) utility card. **Note** This option is informational only, because slots 1/1 and 2/1 can be used only for the TCC+ card.
24che1t1-1	(Cisco 10000 series router) Preprovisions a line card slot for a 24-Port Channelized E1/T1 line card.
2jacket-1	(Cisco uBR10012 router) Preprovisions a slot for the Cisco Wideband SPA Interface Processor (SIP).
2oc12srp-sm-lr	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
24rfchannel-spa-1	(Cisco uBR10012 router) Preprovisions a bay in the Cisco Wideband SIP for the Cisco 1-Gbps Wideband Shared Port Adapter (SPA).
4chstm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port Channelized OC-3/STM-1 line card.
4cht3-hh-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-port Channelized Half-Height line card.

Table 0-1 Card Types Supported by the card Command (continued)

Card Type	Description
4oc3atm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with intermediate-reach optics.
4oc3atm_lr-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with long-reach optics.
5cable-mc520s-d	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20S-D cable interface line card.
5cable-mc520u-d	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20U-D cable interface line card.
6cht3-1	(Cisco 10000 series router) Preprovisions a line card slot for a 6-Port Channelized T3 line card.
6oc3pos-1	(Cisco 10000 series router) Preprovisions a line card slot for a 6-Port OC-3/STM-1 Packet over SONET line card.
8e3ds3-1	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port Unchannelized E3/T3 line card.
8e3ds3atm-1	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port E3/DS3 ATM line card.
8fastethernet-1 [**mode {e1 | t1}**]	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port Fast Ethernet Half-Height line card and optionally specifies its mode of operation. E1 is the default.
4jacket-1	(Cisco uBR10012 router) Preprovisions a slot for the Cisco SIP-600.

Cisco uBR10012 Universal Broadband Router Usage Guidelines

On the Cisco uBR10012 router, you can use the **card** command to preprovision a router slot for a line card or to preprovision one or more slots for a SPA interface processor (SIP), such as the Cisco Wideband SIP. You can also use the **card** command to preprovision a SIP bay for a shared port adapter (SPA), such as the Cisco Wideband SPA.

The Cisco uBR10012 Universal Broadband Router has the following card slot requirements:

Note Slot 0/0 is an invalid value for this command.

- Slots 1/1 and 2/1 are reserved for TCC+ utility cards. A utility card and a SPA can co-exist on a Cisco uBR10012 router with an index of 1/1.
- Slots 1/0 through 4/0 are reserved for network uplink line cards.
- Slots 1 and 3 can be used for SIPs. Each SIP occupies two physical slots in a Cisco uBR10012 router (slot pair 1/2 or slot pair 3/4). Slot 1 is recommended for the Cisco Wideband SIP.
- Slot 5/0 through 8/1 are reserved for cable interface line cards.

Tip When a card has been preprovisioned and is not physically present in the chassis, the **show interface** command for that slot displays the message "Hardware is not present." Some **show** commands might also list the preprovisioned card in their displays. In addition, using the **card** command does not change the output of the ENTITY-MIB, which shows only the equipment that is physically installed in the router.

When a line card is inserted in the Cisco uBR10012 chassis, the router performs the following actions, depending on whether the card slot is preprovisioned for the card:

- If the inserted line card matches the type of line card preprovisioned for the slot, the system applies the preprovisioned configuration to the line card.
- If the line card slot was not preprovisioned, the system applies a basic configuration to the line card and adds that configuration to the running configuration file.
- If the line card slot was preprovisioned for one type of line card, but another type of line card has been inserted, the system replaces the preprovisioned configuration (in the running configuration file) with a basic configuration for the line card that was actually inserted. The startup configuration file is not changed.

Tip Use the **show running-config | include card** command to display which slots, if any, are preprovisioned for a particular card type.

The **no** version of the command removes the preprovisioning information from the given card slot. This also removes all configuration information for that card slot, as well as any information in the SNMP MIB database about the card and its card slot.

Cisco 10000 Series Router Usage Guidelines

You must specify a line card slot and subslot, and the line card for which you want to preprovision the line card slot.

If you insert a line card into a line card slot that has been preprovisioned for a different line card, the line card will fail.

You can specify a mode of operation for the 24-Port Channelized E1/T1 line card. If you do not, the line card operates in the E1 mode.

In Cisco IOS releases earlier than 12.0(28)S, 12.2(16)BX, and 12.3(7)XI1, you used only the **card** command to change the provisioning of a line card slot. It was not necessary to remove the old line card before using the **card** command to change the line card provisioning.

In Cisco IOS releases after 12.0(28)S, 12.2(16)BX, and 12.3(7)XI1, you must deactivate the installed line card using the **hw-module** and **no card** commands before using the **card** command to provision the line card slot for a different line card. This is a general best practice when using the **card** command.

Examples

Cisco uBR10012 Universal Broadband Router Examples

The following example shows a list of supported card types for Cisco IOS Release 12.2(8)BC1, and then shows that slot 8/0 is being preprovisioned for a Cisco uBR-LCP2-MC28C cable interface line card. The cable interface for slot 8/0 can then be configured.

```
Router# config t
Router(config)# card 5/0 ?
  1cable-mc16c    create a uBR10000 line card with MC16C
  1cable-mc16e    create a uBR10000 line card with MC16E
  1gigethernet-1  create a GE_1_PORT cardtype
  1oc12pos-1      create a OC12POS_1_PORT cardtype
  2cable-mc28bnc  create a uBR10000 line card with MC28C, BNC connector
  2cable-mc28c    create a uBR10000 line card with MC28C
  2oc12srp-sm-lr  create a uBR10000 oc12 SRP card with SM LR
Router(config)# card 8/0 2cable-mc28c
Router(config)# int c8/0
Router(config-if)#
```

The following example shows how to preprovision a Cisco Wideband SIP in Cisco IOS Release 12.2(33)SCB:

```
Router# configure terminal
Router(config)# card 1 2jacket-1
```

The following example shows how to preprovision a Cisco Wideband SPA on a Cisco Wideband SIP in Cisco IOS Release 12.2(33)SCB:

```
Router# configure terminal
Router(config)# card 1/0 24rfchannel-spa-1
```

The following example shows how to preprovision a Cisco SIP-600 in Cisco IOS Release 12.2(33) SCB:

```
Router# configure terminal
Router(config)# card 3 4jacket-1
```

The following example shows how to preprovision a Cisco Wideband SPA on a Cisco SIP-600 in Cisco IOS Release 12.2(33) SCB:

```
Router# configure terminal
Router(config)# card 3/0 24rfchannel-spa-1
```

Cisco 10000 Series Router Examples

The following example preprovisions line card slot 2 to accept a 24-Port Channelized E1/T1 line card operating in E1 mode:

```
Router(config)# card 2/0 24che1t1-1 mode e1
```

The following example shows how to change the provisioning for line card slot 5 from the 1-Port Gigabit Ethernet Half-Height line card to the 4-Port OC-3/STM-1 ATM line card.

```
Router(config)# hw-module subslot 5/0 shut
Aug 22 21:52:19.619 UTC: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 5/0.
Aug 22 21:52:19.619 UTC: %IPCOIR-2-CARD_UP_DOWN: Card in slot 5/0 is down.  Notifying
1gigethernet-hh-1 driver.
Aug 22 21:52:21.627 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to
down
Aug 22 21:52:22.627 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet5/0/0, changed state to down
Router(config)# no card 5/0 1gigethernet-hh-1
Aug 22 21:53:20.008 UTC: %C10K-3-DEACTIVATED: card in slot [5/0] disabled.
Router(config)# card 5/0 4oc3atm-1
[ Remove the 1-Port Gigabit Ethernet Half-Height line card and
insert the 4-Port OC-3/STM-1 ATM line card ]
```

Related Commands

Command	Description
show interface	Displays the current configuration and status for a specified interface type.

debug ipv6 icmp

To display debugging messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions), use the **debug ipv6 icmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 icmp

no debug ipv6 icmp

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 ICMP is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

The **debug ipv6 icmp** command is similar to the **debug ip icmp** command, except that it is IPv6-specific.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

This command helps you determine whether the router is sending or receiving IPv6 ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.

Note For more information about the fields in **debug ipv6 icmp** output, refer to RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6).*

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, output from the **debug ipv6 icmp** command displays information similar to the following:

```
ICMPv6: Received echo reply from 2010:1:1:1:1:1:1:2
```

In Cisco IOS Release 12.2(31)SB, the **debug ipv6 icmp** command output displays information similar to the following:

```
ICMPv6: Received ICMPv6 packet from 2010:1:1:1:1:1:1:2, type 129
```

Examples

The following is sample output from the **debug ipv6 icmp** command:

```
Router# debug ipv6 icmp

13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

Table 2 describes significant fields shown in the first line of the display.

Table 2 debug ipv6 icmp Field Descriptions

Field	Description
13:28:40:	Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred.
*n*w*n*d: (not shown in sample output)	Indicates time (weeks, days) since last reboot of the event occurring. For example, 1w4d: indicates the time (since the last reboot) of the event occurring was 1 week and 4 days ago.
ICMPv6:	Indication that this message describes an ICMP version 6 packet.
Received ICMPv6 packet from 2000:0:0:3::2	IPv6 address from which the ICMP version 6 packet is received.
type 136	The number variable indicates one of the following IPv6 ICMP message types: • 1—Destination unreachable. The router cannot forward a packet that was sent or received. • 2—Packet too big. The router attempts to send a packet that exceeds the maximum transmission unit (MTU) of a link between itself and the packet destination. • 3—Time exceeded. Either the hop limit in transit or the fragment reassembly time is exceeded. • 4—Parameter problem. The router attempts to send an IPv6 packet that contains invalid parameters. An example is a packet containing a next header type unsupported by the router that is forwarding the packet. • 128—Echo request. The router received an echo reply. • 129—Echo reply. The router sent an echo reply. • 133—Router solicitation messages. Hosts send these messages to prompt routers on the local link to send router advertisement messages. • 134—Router advertisement messages. Routers periodically send these messages to advertise their link-layer addresses, prefixes for the link, and other link-specific information. These messages are also sent in response to router solicitation messages. • 135—Neighbor solicitation messages. Nodes send these messages to request the link-layer address of a station on the same link. • 136—Neighbor advertisement messages. Nodes send these messages, containing their link-local addresses, in response to neighbor solicitation messages. • 137—Redirect messages. Routers send these messages to hosts when a host attempts to use a less-than-optimal first hop address when forwarding packets. These messages contain a better first hop address that should be used instead.

Following are examples of the IPv6 ICMP messages types that can be displayed by the **debug ipv6 icmp** command:

- ICMP echo request and ICMP echo reply messages. In the following example, an ICMP echo request is sent to address 2052::50 and an ICMP echo reply is received from address 2052::50.

```
1w4d:ICMPv6:Sending echo request to 2052::50
1w4d:ICMPv6:Received echo reply from 2052::50
```

- ICMP packet too big messages. In the following example, a router tried to forward a packet to destination address 2052::50 via the next hop address 2052::52. The size of the packet was greater than 1280 bytes, which is the MTU of destination address 2052::50. As a result, the router receives an ICMP packet too big message from the next hop address 2052::52.

```
1w4d:Received ICMP too big from 2052::52 about 2052::50, MTU=1300
```

- ICMP parameter problem messages. In the following example, an ICMP parameter problem message is received from address 2052::52.

```
1w4d:Received ICMP parameter problem from 2052::52
```

- ICMP time exceeded messages. In the following example, an ICMP time exceeded message is received from address 2052::52.

```
1w4d:Received ICMP time exceeded from 2052::52
```

- ICMP unreachable messages. In the following example, an ICMP unreachable message with code 1 is received from address 2052::52. Additionally, an ICMP unreachable message with code 1 is sent to address 2060::20 about address 2062::20.

```
1w4d:Received ICMP unreachable code 1 from 2052::52
1w4d:Sending ICMP unreachable code 1 to 2060::20 about 2062::20
```

Table 3 lists the codes for ICMP unreachable messages.

Table 3 ICMP Unreachable Messages—Code Descriptions

Code	Description
0	The router has no route to the packet destination.
1	Although the router has a route to the packet destination, communication is administratively prohibited.
3	The address is unreachable.
4	The port is unreachable.

Related Commands

Command	Description
debug ipv6 nd	Displays debugging messages for IPv6 ICMP neighbor discovery transactions.

fair-queue (WFQ)

To enable weighted fair queueing (WFQ), use the **fair-queue** command in interface configuration or policy-map class configuration mode. To disable WFQ, use the **no** form of this command.

fair-queue [*congestive-discard-threshold* [*dynamic-queues* [*reservable-queues*]]]

no fair-queue

Syntax Description

congestive-discard-threshold	(Optional) Number of messages allowed in each queue. The range is 1 to 4096 and the default is 64 messages. When a conversation reaches this threshold, new message packets are discarded. **Note** If you have hierarchical queueing framework (HQF) configured, then the values are 16 to 4096.
dynamic-queues	(Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are **16**, **32**, **64**, **128**, **256**, **512**, **1024**, **2048**, and **4096**. See the tables in the **fair-queue** (class-default) command for the default number of dynamic queues.
reservable-queues	(Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP).

Command Default

Fair queueing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps and that do not use the following:

- X.25 and Synchronous Data Link Control (SDLC) encapsulations
- Link Access Procedure, Balanced (LAPB)
- Tunnels
- Loopbacks
- Dialer
- Bridges
- Virtual interfaces

Fair queueing is not an option for the protocols listed above. However, if you enable custom queueing or priority queueing for a qualifying link, it overrides fair queueing, effectively disabling it. Additionally, fair queueing is automatically disabled if you enable the autonomous or silicon switching engine mechanisms.

Note A variety of queueing mechanisms can be configured using multilink; for example, Multichassis Multilink PPP (MMP). However, if only PPP is used on a tunneled interface—for example, virtual private dialup network (VPND), PPP over Ethernet (PPPoE), or PPP over Frame Relay (PPPoFR)—no queueing can be configured on the virtual interface.

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See Table 4 in the **fair-queue** (class-default) command for the default number of dynamic queues that WFQ and class-based WFQ (CBWFQ) use when they are enabled on an interface. See Table 4 in the **fair-queue** (class-default) command for the default number of dynamic queues used when WFQ and CBWFQ are enabled on an ATM PVC.

Command Modes

Interface configuration (config-if)
Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command was modified to remove Apollo, VINES, and XNS from the list of protocols and traffic stream discrimination fields. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.
12.4(20)T	Support was added for HQF and user-defined classes using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Usage Guidelines

High-Level Overview

This command enables WFQ. With WFQ, packets are classified by flow. For example, packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, and protocol belong to the same flow; see Table 4 for a full list of protocols and traffic stream discrimination fields.

When you enable WFQ on an interface, WFQ provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. Enabling WFQ requires use of this command only.

When you enable WFQ on an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive discard threshold has been met. However, low-bandwidth conversations, which include control message conversations, continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

WFQ uses a traffic data stream discrimination registry service to determine which traffic stream a message belongs to. For each forwarding protocol, Table 4 shows the message attributes that are used to classify traffic into data streams.

Table 4 Weighted Fair Queueing Traffic Stream Discrimination Fields

Forwarder	Fields Used
AppleTalk	• Source net, node, socket • Destination net, node, socket • Type
Connectionless Network Service (CLNS)	• Source network service access point (NSAP) • Destination NSAP
DECnet	• Source address • Destination address
Frame Relay switching	• Data-link connection identified (DLCI) value
IP	• Type of service (ToS) • IP protocol • Source IP address (if message is not fragmented) • Destination IP address (if message is not fragmented) • Source TCP/UDP port • Destination TCP/UDP port
Transparent bridging	• Unicast: source MAC, destination MAC • Ethertype Service Advertising Protocol (SAP)/Subnetwork Access Protocol (SNAP) multicast: destination MAC address
Source-route bridging	• Unicast: source MAC, destination MAC • SAP/SNAP multicast: destination MAC address
Novell NetWare	• Source/destination network/host/socket • Level 2 protocol
All others (default)	• Control protocols (one queue per protocol)

IP Precedence

IP Precedence, congestion in Frame Relay switching, and discard eligible (DE) flags affect the weights used for queueing.

IP Precedence, which is set by the host or by policy maps, is a number in the range from 0 to 7. Data streams of precedence *number* are weighted so that they are given an effective bit rate of *number*+1 times as fast as a data stream of precedence 0, which is normal.

FECN and BECN

In Frame Relay switching, message flags for forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), and DE message flags cause the algorithm to select weights that effectively impose reduced queue priority. The reduced queue priority provides the application with "slow down" feedback and sorts traffic, giving the best service to applications within their committed information rate (CIR).

Fair Queueing, Custom Queueing, and Priority Queueing

Fair queueing is supported for all LAN and line (WAN) protocols except X.25, including LAPB and SDLC; see the notes in the section "Command Default." Because tunnels are software interfaces that are themselves routed over physical interfaces, fair queueing is not supported for tunnels. Fair queueing is on by default for interfaces with bandwidth less than or equal to 2 Mbps.

Note For Release 10.3 and earlier releases for the Cisco 7000 and 7500 routers with a Route Switch Processor (RSP) card, if you used the **tx-queue-limit** command to set the transmit limit available to an interface on a Multiport Communications Interface (MCI) or serial port communications interface (SCI) card and you configured custom queueing or priority queueing for that interface, the configured transmit limit was automatically overridden and set to 1. With Cisco IOS Release 12.0 and later releases, for WFQ, custom queueing, and priority queueing, the configured transmit limit is derived from the bandwidth value set for the interface using the **bandwidth** (interface) command. Bandwidth value divided by 512 rounded up yields the effective transmit limit. However, the derived value only applies in the absence of a **tx-queue-limit** command; that is, a configured transmit limit overrides this derivation.

RSVP

When you configure Resource Reservation Protocol (RSVP) on an interface that supports fair queueing or on an interface that is configured for fair queueing with the reservable queues set to 0 (the default), the reservable queue size is automatically configured using the following method: interface bandwidth divided by 32 kbps. You can override this default by specifying a reservable queue other than 0. For more information on RSVP, refer to the chapter "Configuring RSVP" in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 10000 Series Routers

In Cisco IOS Release 12.2(33)SB, the router removes the **no fair-queue** command from serial interfaces.

HQF

Beginning with Cisco IOS Release 12.4(20)T, if your image has HQF support, the **fair-queue** command is not enabled automatically under class default. You should enable the **fair-queue** command and any other supported queueing features before using an HQF-capable image.

Examples

The following example enables WFQ on serial interface 0, with a congestive threshold of 300. This threshold means that messages are discarded from the queueing system only when 300 or more messages have been queued and the message is in a data stream that has more than one message in the queue. The transmit queue limit is set to 2, based on the 384-kilobit (Kb) line set by the **bandwidth** command:

```
interface serial 0
 bandwidth 384
 fair-queue 300
```

Unspecified parameters take the default values.

The following example requests a fair queue with a congestive discard threshold of 64 messages, 512 dynamic queues, and 18 RSVP queues:

```
interface serial 3/0
 ip unnumbered ethernet 0/0
 fair-queue 64 512 18
```

You can apply the **fair-queue** command to a user-defined class as shown in the following example:

```
policy-map p1
```

```
class c1
 bandwidth 1000
 fair-queue
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
custom-queue-list	Assigns a custom queue list to an interface.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
fair-queue (DWFQ)	Enables DWFQ.
priority-group	Assigns the specified priority list to an interface.
priority-list default	Assigns a priority queue for those packets that do not match any other rule in the priority list.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing	Lists all or selected configured queueing strategies.
tx-queue-limit	Controls the number of transmit buffers available to a specified interface on the MCI and SCI cards.

frame-relay broadcast-queue

To create a special queue for a specified interface to hold broadcast traffic that has been replicated for transmission on multiple data-link connection identifiers (DLCIs), use the **frame-relay broadcast-queue** command in interface configuration mode.

frame-relay broadcast-queue *size byte-rate packet-rate*

Syntax Description

size	Number of packets to hold in the broadcast queue.
byte-rate	Maximum number of bytes to be sent per second.
packet-rate	Maximum number of packets to be sent per second.

Defaults

size: 64 packets
byte-rate: 256000 bytes per second
packet-rate: 36 packets per second

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)SB	This command was enhanced to support a default queue size of 256 packets and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

For purposes of the Frame Relay broadcast queue, *broadcast traffic* is defined as packets that have been replicated for transmission on multiple DLCIs. However, the broadcast traffic does not include the original routing packet or service access point (SAP) packet, which passes through the normal queue. Because of timing sensitivity, bridged broadcasts and spanning-tree packets are also sent through the normal queue. The Frame Relay broadcast queue is managed independently of the normal interface queue. It has its own buffers and a configurable service rate.

A broadcast queue is given a maximum transmission rate (throughput) limit measured in bytes per second and packets per second. The queue is serviced to ensure that only this maximum is provided. The broadcast queue has priority when transmitting at a rate below the configured maximum, and hence has a guaranteed minimum bandwidth allocation. The two transmission rate limits are intended to avoid flooding the interface with broadcasts. The actual limit in any second is the first rate limit that is reached.

Given the transmission rate restriction, additional buffering is required to store broadcast packets. The broadcast queue is configurable to store large numbers of broadcast packets.

The queue size should be set to avoid loss of broadcast routing update packets. The exact size will depend on the protocol being used and the number of packets required for each update. To be safe, set the queue size so that one complete routing update from each protocol and for each DLCI can be stored. As a general rule, start with 20 packets per DLCI. Typically, the byte rate should be less than both of the following:

- *N/4* times the minimum remote access rate (measured in *bytes* per second), where *N* is the number of DLCIs to which the broadcast must be replicated.
- 1/4 the local access rate (measured in *bytes* per second).

The packet rate is not critical if you set the byte rate conservatively. Set the packet rate at 250-byte packets.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the default queue size for the frame-relay broadcast-queue is 256 packets.

In Cisco IOS Release 12.2(31)SB, the default queue size is 64 packets.

Examples

The following example specifies a broadcast queue to hold 80 packets, to have a maximum byte transmission rate of 240000 bytes per second, and to have a maximum packet transmission rate of 160 packets per second:

```
frame-relay broadcast-queue 80 240000 160
```

frame-relay switching

To enable permanent virtual switching (PVC) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI), use the **frame-relay switching** command in global configuration mode. To disable switching, use the **no** form of this command.

frame-relay switching

no frame-relay switching

Syntax Description

This command has no arguments or keywords.

Defaults

Switching is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

You must add this command to the configuration file before configuring the routes.

Cisco 10000 Serie Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, you do not need to configure the **frame-relay switching** command when configuring a Frame Relay interface as the DCE.

In Cisco IOS Release 12.2(31)SB, you must configure the **frame-relay switching** command when you configure a Frame Relay interface as the DCE.

Examples

The following example shows the command that is entered in the configuration file before the Frame Relay configuration commands to enable switching:

```
frame-relay switching
```

hw-module slot

To enable the router shelf to restart a stopped Dial Shelf Controller (DSC) card, to stop a DSC card, or to cause a shutdown, reset, or reload of any specified dial shelf feature board, use the **hw-module slot** command in privileged EXEC mode.

hw-module slot *shelf-id/slot-number* {**reload** | **reset** | **shutdown** | **start** | **stop**}

Syntax Description

shelf-id	Number of the dial shelf. The default number for the dial shelf is 1.
/slot-number	Number of the slot in the shelf where the target feature board or DSC is installed. If the **start** or **stop** keyword is used, the slot number must be either 12 or 13, because these keywords apply only to DSCs.
reload	Enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).
reset	Resets a feature board.
shutdown	Shuts down a feature board.
start	Restarts the specified DSC.
stop	Stops the specified DSC.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)AA	The **hw-module** command was introduced.
12.1	• The **hw-module** command was expanded to become the **hw-module slot** command. • The **reload** keyword was added to enable a remote reload of a feature board.
12.3(2)T	The **reset** and **shutdown** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4, and the **reload** option was introduced on the router.

Usage Guidelines

The **stop** form of this command is issued from the router shelf console instead of by pressing the attention (ATTN) button on the target DSC. Confirmation of when the start or stop took place is displayed. Warnings are issued and confirmation input is required if a **stop** command will result in a loss of service when backup functionality is not available.

When a DSC card is stopped, removed, and then reinstalled, there is no need to restart the card (whether the card is the original or a replacement) because a freshly installed card reboots as the backup DSC automatically. However, if a DSC is stopped, either by using the ATTN button or by issuing the **hw-module slot stop** command, it must be restarted by using the **start** form of the same command, or the DSC must be removed and reinstalled in order to reboot.

Press the ATTN button on the DSCs to shut down a card manually before removing the card. This is equivalent to issuing a **hw-module slot** command for that card at the router command prompt. Use the ATTN button to shut down the card before it is swapped out or tested in place, or to restart it, if the card has not been removed after having been shut down.

Tip The **hw-module slot** *shelf-id*/*slot-number* **reload** form of this command is useful for simulating an OIR event in the case of a feature board failure when physical access to the feature board card is restricted.

Entering the **hw-module slot** *shelf-id*/*slot-number* **reload** command initiates the feature board reload process through power cycling. The **hw-module slot** *shelf-id*/*slot-number* **reload** command cannot be used to reload DSCs.

Use the **reset** form of this command to reset the specified feature card and drop all active calls.

Use the **shutdown** form of this command to shut down the specified feature card and drop all active calls.

Cisco 10000 Series Router Usage Guidelines,

In Cisco IOS Release 12.2(33)SB, when you enter the **hw-module slot** *slot-number* **reset** command, the software asks you to confirm the command.

In Cisco IOS Release 12.2(31)SB, the software does not ask you to confirm the **hw-module slot** *slot-number* **reset** command.

Examples

The following example shows how to stop the DSC in slot 13 and start the other DSC in slot 12 (which was previously stopped):

```
Router# hw-module slot 1/13 stop
Router# hw-module slot 1/12 start
```

The following example shows how to reload the dial shelf feature board in slot 6:

```
Router# hw-module slot 1/6 reload
```

The following example shows how to reset the card in slot 3:

```
Router# hw-module slot 1/3 reset
```

The following example shows how to shut down the PRE card located in slot 3:

```
Router# hw-module slot 1/3 shutdown
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) DSC cards.
show redundancy	Displays current or historical status and related information on dual (redundant) DSC cards.

plim qos input map

To configure a priority queue on Gigabit Ethernet SPAs, use the **plim qos input map** command in interface or subinterface configuration mode. To remove a priority queue, use the no form of this command.

plim qos input map {cos {**enable** | *cos-value* **queue low-latency**} | **ip** {**dscp-based** | **dscp** *dscp-value* **queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value* **queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value* **queue low-latency**

Syntax Description

cos enable	Enables classification of ingress VLAN traffic according to the 802.1Q priority bits. **Note** This command can only be applied to VLAN interfaces.
cos *cos-value* **queue low-latency**	Classifies incoming VLAN traffic on a subinterface according to the 802.1Q priority bits and places the traffic into the appropriate queue. By default, traffic with 802.1Q priority bits set to 6 or 7 are placed in the high-priority queue and all other traffic is placed in the low-priority queue. *cos-value s*pecifies the IEEE 802.1Q/ISL CoS value from 0 to 7. **Note** When you configure a class of service (CoS) value on a QinQ subinterface, the CoS value applies to all QinQ subinterfaces with the same outer VLAN ID. **low-latency** specifies the high priority queue.
ip dscp-based	Enables the classification of incoming IP traffic according to the value of the DSCP bits. **Note** This command only applies to physical interfaces.
ip dscp *dscp-value* **queue low-latency**	Classifies incoming IP traffic according to the value of the DSCP bits and places the traffic into the appropriate queue. By default, IP traffic with the DSCP bits equal to EF will use the low-latency queue, and traffic with any other DSCP value will use the low-priority queue. *dscp-value* is the value of the DSCP bits. You can specify a range of values separated by a dash or a list of value. For a list of valid values, see the Usage Guidelines. **low-latency** specifies the high priority queue.
ip precedence-based	Enables the classification of incoming IP traffic according to the IP precedence value. **Note** This command applies only to physical interfaces.
ip precedence *precedence-value* **queue low-latency**	Classifies incoming IP traffic according to the value of the IP precedence bits and places the traffic into the appropriate queue. IP traffic with the IP precedence bits set to 6 or 7 uses the low-latency queue; all other traffic uses the low-priority queue. *precedence-value* is the value of the IP precedence bits (0 to 7). You can specify a range of values separated by a dash or a list of values. **low-latency** specifies the high priority queue.

ipv6 tc *tc-value* **queue low-latency**	Classifies ingress IPv6 traffic based on the value of the traffic-class bits and places the traffic into the appropriate queue. By default, IPv6 traffic with a traffic-class value equal to **ef** uses the high-priority queue and all other traffic uses the low-priority queue. Only the most significant six bits of the traffic-class octet is used for the classification. **Note** This command applies only to physical interfaces. *tc-value* is the value of the traffic class bits. You can specify a range of values separated by a dash or a list of values. For a list of valid values, see the Usage Guidelines. **low-latency** specifies the high priority queue.
mpls exp *exp-value* **queue low-latency**	Classifies incoming MPLS traffic according to the value of the EXP bits and places the traffic into the appropriate queue. By default, traffic with the EXP bits set to 6 or 7 uses the high-priority queue and all other traffic uses the low-priority queue. **Note** This command applies only to physical interfaces. *exp-value* is the value of the EXP bits (0 to 7). You can specify a range of values separated by a dash or a list of values. **low-latency** specifies the high priority queue.

Defaults

Disabled

Command Modes

Interface or subinterface configuration

Command History

Cisco IOS Release	Modification
12.2(33)SB	This command was introduced on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **plim qos input map** command separates high-priority traffic from low-priority traffic and places the traffic in the appropriate interface queue. The command separates priority and non-priority traffic at the SPA interface processor (SIP) to prevent the dropping of high priority traffic in an oversubscription case. Each shared port adaptor (SPA) supports one priority queue.

The router supports the following classification types for the prioritization of ingress traffic on the Gigabit Ethernet SPAs:

- VLAN 802.1Q priority bits
- IP DSCP bits
- IP precedence bits
- IPv6 traffic class bits
- MPLS experimental (EXP) bits

For the **plim qos input map ip dscp** *dscp-value* **queue low-latency** command, valid values for *dscp-value* are one of the following:

- 0 to 63—Differentiated services codepoint value
- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110
- af41—100010
- af42—100100
- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

For the **plim qos input map ipv6 tc** *tc-value* **queue low-latency** command, valid values for *tc-value* are one of the following:

- 0 to 63—Differentiated services codepoint value
- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110
- af41—100010
- af42—100100

- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

Examples

The following example enables DSCP-based classification on the SPA that is located in subslot 0 of the SIP in slot 1 of the Cisco 10000 series router:

```
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# plim qos input map ip dscp-based
```

Related Commands

Command	Description
card	Preprovisions the SIP-600 and SPAs.
negotiation auto	Enables autonegotiation on a Gigabit Ethernet SPA interfaces on the Cisco 10000 SIP-600.
mtu	Configures the maximum packet size for an interface. The default is 1500 bytes. The maximum configurable MTU is 9129 bytes.

police (policy map)

To create a per-interface policer and configure the policy-map class to use it, use the **police** command in policy-map class configuration mode. To delete the per-interface policer from the policy-map class, use the **no** form of this command.

police

police *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police *bps*

police aggregate

police aggregate *name*

no police aggregate *name*

police cir

police cir *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir *bps*

police cir percent

police cir percent *percent* [*burst* **ms** [**be**] [*burst* **ms**]] [**pir percent** *percent* [**be** *burst* **ms**]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir percent

police flow

police flow *bps* [*normal-burst-bytes*] [**conform-action** *action* [**exceed-action** *action*]]

police flow mask {**dest-only** | **full-flow** | **src-only**} *bps* [*normal-burst-bytes*] [**conform-action** *action* [**exceed-action** *action*]]

no police flow

Syntax Description

bps	The target bit rate in bits per second (bps). The postfix values **k**, **m**, and **g** are allowed, as is a decimal point. Valid range is from 8000 (or 8k) to 64000000000 (or 64g).
normal-burst-bytes	(Optional) The CIR token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.
maximum-burst-bytes	(Optional) The PIR token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.
burst-bytes	(Optional) The token-bucket size in bytes for handling a burst. Valid range is from 1000 to 512000000.

bc	(Optional) Specifies in bytes the allowed (conforming) burst size.
be	(Optional) Specifies in bytes the allowed excess burst size.
pir	(Optional) Specifies the peak information rate (PIR).
cir	Specifies the committed information rate (CIR).
conform-action *action*	(Optional) Specifies the action to take on packets that conform to the rate limit. See the "Usage Guidelines" section for valid values for the *action* argument.
exceed-action *action*	(Optional) Specifies the action to be taken on packets when the packet rate is greater than the rate specified in the *maximum-burst-bytes* argument. See the "Usage Guidelines" section for valid values for the *action* argument.
violate-action *action*	(Optional) Specifies the action to be taken when the packet rate is greater than the rate specified in the *maximum-burst-bytes* argument. See the "Usage Guidelines" section for valid values for the *action* argument.
aggregate *name*	Specifies a previously defined aggregate policer name and configures the policy-map class to use the specified aggregate policer.
percent *percent*	Specifies the percentage of the interface bandwidth to be allowed. Valid range is from 1 to 100.
burst	(Optional) The token-bucket size in milliseconds (ms) for handling a burst. Valid range is from 1 to 2000.
ms	Milliseconds. When bandwidth is specified as a percentage, this keyword must follow the *burst* argument.
flow	Specifies a microflow policer that will police each flow.
mask	Specifies the flow mask to be used for policing.
dest-only	Specifies the destination-only flow mask.
full-flow	Specifies the full-flow mask.
src-only	Specifies the source-only flow mask.

Command Default

No policing is performed.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
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(17d)SXB3	The **police** *bps* minimum rate was lowered from 32,000 to 8,000 on FlexWAN interfaces only.

Release	Modification
12.2(18)SXD	This command was changed as follows: • Added **set-mpls-exp-topmost-transmit** to the valid values for the **conform-action** keyword. • Changed the **set-mpls-exp-transmit** keyword to **set-mpls-exp-imposition-transmit**.
12.2(18)SXE	The *bps* maximum rate was increased from 4,000,000,000 to 10,000,000,000 bps to support 10-Gigabit Ethernet.
12.2(18)SXF	The CIR maximum rate was increased to 10,000,000,000 bps.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions default to the default actions: conform-action transmit, exceed-action drop, and violate-action drop. This was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SB	The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions are preserved. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4. For more information, see the "Usage Guidelines" section.
12.2(33)SXH2	The CIR maximum rate was increased to 64,000,000,000 bps.
12.2(33)SXI	The minimum CIR token bucket size was reduced to 1 byte.

Usage Guidelines

In Cisco IOS Release 12.2(17d)SXB3, valid values for the *bps* argument for the FlexWAN interfaces only are from 8,000 to 4,000,000,000 bps.

Use the **mls qos aggregate-policer** *name* command to create a named aggregate policer.

You can create two types of aggregate policers: named and per-interface. Both types can be attached to more than one port as follows:

- You create named aggregate policers using the **mls qos aggregate-policer** command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.
- You define per-interface aggregate policers in a policy-map class using the **police** command. If you attach a per-interface aggregate policer to multiple ingress ports, it polices the matched traffic on each ingress port separately.

Use the **no police aggregate** *name* command to clear the use of the named aggregate policer.

Enter the **police flow** command to define a microflow policer (you cannot apply microflow policing to ARP traffic).

Enter the **police** command to define per-interface (not named) aggregate policers.

If the traffic is both aggregate and microflow policed, the aggregate and the microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keywords.

Values for the action Argument

The valid values for the *action* argument are as follows:

- **drop**—Drops packets that do not exceed the rate set for the *bps* argument.
- **set-clp-transmit**—Sets and sends the ATM cell loss priority (CLP).

- **set-cos-inner-transmit** {*new-cos*}—Marks the matched traffic with a new inner class of service (CoS) value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit** {*new-cos*}—Marks the matched traffic with a new CoS value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit**—Sets and sends the ATM cell loss priority (CLP).
- **set-dscp-transmit** {*dscp-bit-pattern* | *dscp-value* | **default** | **ef**}—Marks the matched traffic with a new DSCP value:
  - *dscp-bit-pattern*—Specifies a DSCP bit pattern. Valid values are listed in Table 5.
  - *dscp-value*—Specifies a DSCP value. Valid values are from 0 to 63.
  - **default**—Matches packets with the default DSCP value (000000).
  - **ef**—Matches packets with the Expedited Forwarding (EF) per-hop behavior (PHB) DSCP value (101110).

Table 5 Valid DSCP Bit Pattern Values

Keyword	Definition
af11	Matches packets with AF11 DSCP (001010).
af12	Matches packets with AF12 DSCP (001100).
af13	Matches packets with AF13 DSCP (001110).
af21	Matches packets with AF21 DSCP (010010).
af22	Matches packets with AF22 DSCP (010100).
af23	Matches packets with AF23 DSCP (010110).
af31	Matches packets with AF31 DSCP (011010).
af32	Matches packets with AF32 DSCP (011100).
af33	Matches packets with AF33 DSCP (011110).
af41	Matches packets with AF41 DSCP (100010).
af42	Matches packets with AF42 DSCP (100100).
af43	Matches packets with AF43 DSCP (100110).
cs1	Matches packets with CS1 (precedence 1) DSCP (001000).
cs2	Matches packets with CS2 (precedence 2) DSCP (010000).
cs3	Matches packets with CS3 (precedence 3) DSCP (011000).
cs4	Matches packets with CS4 (precedence 4) DSCP (100000).
cs5	Matches packets with CS5 (precedence 5) DSCP (101000).
cs6	Matches packets with CS6 (precedence 6) DSCP (110000).
cs7	Matches packets with CS7 (precedence 7) DSCP (111000).

- **set-frde-transmit**—Sets and sends the Frame Relay discard eligible (FR DE) bit. This is valid for the **exceed-action** *action* keyword and argument combination.
- **set-mpls-exp-imposition-transmit** *new-mpls-exp*—Rewrites the Multiprotocol Label Switching (MPLS) experimental (exp) bits on imposed label entries and transmits the bits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map. Valid values for the *new-mpls-exp* argument are from 0 to 7.

- **set-mpls-exp-topmost-transmit**—Sets experimental bits on the topmost label and sends the packet.

Note The **set-mpls-exp-topmost-transmit** keyword is not supported in some releases of the Catalyst 6500 series switch or the Cisco 7600 series router.

- **set-prec-transmit** *new-precedence* [**exceed-action**]—Marks the matched traffic with a new IP-precedence value and transmits it. Valid values for the *new-precedence* argument are from 0 to 7. You can also follow this action with the **exceed-action** keyword.
- **set-qos-transmit**—Rewrites qos-group and sends the packet.
- **transmit**—Transmits the packets that do not exceed the rate set for the *bps* argument. The optional keyword and argument combination for the **transmit** keyword is **exceed-action** *action*.

If the following keywords are not specified, the default actions are as follows:

- **conform-action** is **transmit**.
- **exceed-action** is **drop**.
- **violate-action** is **drop**.

Cisco 10000 Series Router

In releases earlier than Cisco IOS Release 12.2(31)SB, if you modify the police rate parameters, but not the action parameters, the action parameters revert to the default actions.

For example, the following sample configuration shows the **police** command configured in the policy map named test. The police actions are set to set-clp-transmit for conforming, exceeding, and violating traffic. The police rate parameters are then changed to 500000, 250, and 200, respectively, but no actions are modified. When you display the test policy map again, you can see that the police actions default to transmit, drop, and drop, respectively.

```
Router# show policy-map test

Policy Map test
    Class prec1
        police 248000 100 10 conform-action set-clp-transmit exceed-action
        set-clp-transmit violate-action set-clp-transmit

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 250 200
Router(config-pmap-c)# end
Router# show policy-map test

Policy Map test
    Class prec1
        police 500000 250 200 conform-action transmit exceed-action drop violate-action
        drop
```

Cisco IOS Release 12.2(33)SB and later releases support dual police actions and a police submode; therefore, if you use the **police** command to modify only the rate parameters, the police actions do not default to the default actions and the previous actions are preserved.

For example, the following sample configuration shows the **police** command configured under the traffic class named prec1 in the policy map named test. The police rate is specified and the police actions are then specified in police submodes. After you change only the police rate parameters, the police actions do not default, but rather they retain their original settings.

```
Router# show policy-map test

Policy Map test
    Class prec1
        police 248000 1000 100
         conform-action set-clp-transmit
         exceed-action set-clp-transmit
         violate-action set-clp-transmit

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 100 200
Router(config-pmap-c)# end
Router# show policy-map test

Policy Map test
    Class prec1
        police 500000 100 200
         conform-action set-clp-transmit
         exceed-action set-clp-transmit
         violate-action set-clp-transmit
```

Examples

This example shows how to specify a previously defined aggregate-policer name and configure the policy-map class to use the specified aggregate policer:

```
Router(config-pmap-c)# police aggregate agg1
```

This example shows how to create a policy map named police-setting that uses the class map access-match, which is configured to trust received IP-precedence values and is configured with a maximum-capacity aggregate policer and a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 1000000000 200000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Accesses QoS class-map configuration mode to configure QoS class maps.
mls qos aggregate-policer	Defines a named aggregate policer for use in policy maps.
police	Configures traffic policing in QoS policy-map class configuration mode or QoS policy-map class police configuration mode.
service-policy	Attaches a policy map to an interface.
show class-map	Displays class-map information.

Command	Description
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

scripting tcl encdir

To specify the default location of external encoding files used by the Tool Command Language (Tcl) shell, use the **scripting tcl encdir** command in global configuration mode. To remove the default location, use the **no** form of this command.

scripting tcl encdir *location-url*

no scripting tcl encdir

Syntax Description

location-url	The URL used to access external encoding files used by Tcl.

Defaults

Tcl does not use external encoding files.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Character strings in Tcl are encoded using 16-bit Unicode characters. Different operating system interfaces or applications can generate character strings using other encoding methods. Use the **scripting tcl encdir** command to configure a location URL for the external Tcl character encoding files to support the Tcl **encoding** command.

Tcl contains only a few character sets within the Tcl shell. Additional characters sets are loaded, as needed, from external files.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the router removes the **no scripting tcl encdir** command from the default configuration.

Examples

The following example shows how to specify a default location for external encoding files to be used by Tcl:

```
Router# configure terminal
Router(config)# scripting tcl encdir tftp://10.18.117.23/file2/
```

Related Commands

Command	Description
scripting tcl init	Specifies an initialization script for the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl init

To specify an initialization script for the Tool Command Language (Tcl) shell, use the **scripting tcl init** command in global configuration mode. To remove the initialization script, use the **no** form of this command.

scripting tcl init *init-url*

no scripting tcl init

Syntax Description

init-url	The URL used to access the initialization script to be used by Tcl.

Defaults

Tcl does not run an initialization script.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Use the **scripting tcl init** command when you want to predefine Tcl procedures to run in an initialization script. The initialization script runs when the Tcl shell is entered and saves manual sourcing of the individual scripts.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the router removes the **no scripting tcl init** command from the default configuration.

Examples

The following example shows how to specify an initialization script to run when the Tcl shell is enabled:

```
Router# configure terminal
Router(config)# scripting tcl init ftp://user:password@172.17.40.3/tclscript/initfile3.tcl
```

Related Commands

Command	Description
scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

no service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

Cisco 10000 Series and Cisco 7600 Series Routers

service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

no service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

Syntax Description

type access-control	Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
output	Attaches the specified policy map to the output interface or output VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.
history	(Optional) Maintains a history of Quality of Service (QoS) metrics.
type control *control-policy-name*	(Optional) Creates a Class-Based Policy Language (CPL) control policy map that is applied to a context.

Command Default

No service policy is specified.
A control policy is not applied to a context.
No policy map is attached.

Command Modes

ATM bundle-VC configuration (config-atm-bundle)
ATM PVP configuration (config-if-atm-l2trans-pvp)
ATM VC mode (config-if-atm-vc)
Global configuration (config)
Interface configuration (config-if)
Map-class configuration (config-map-class)
PVC-in-range configuration (cfg-if-atm-range-pvc)
PVC range subinterface configuration (config-subif)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was implemented on the Cisco 10000 series routers.

Release	Modification
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs.
12.2(14)SX	Support for this command was implemented on Cisco 7600 series routers. This command was changed to support output policy maps.
12.2(15)BX	This command was implemented on the ESR-PRE2.
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.
12.4(2)T	This command was modified to support PVC range subinterface configuration mode and i PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.
12.4(4)T	The **type stack** and the **type control** keywords were added to support flexible packet matching (FPM).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.3(7)XI2	This command was modified to support PVC range configuration mode and PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router.
12.2(18)ZY	The **type stack** and the **type control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
12.2(33)SRC	Support for this command was enhanced on Cisco 7600 series routers.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.3	This command was modified to support ATM PVP configuration mode.

Usage Guidelines

Choose the command mode according to the intended use of the command, as follows:

Application	Mode
Standalone VC	VC submode
ATM VC bundle members	Bundle-VC configuration
A range of ATM PVCs	PVC range subinterface configuration
Individual PVC within a PVC range	PVC-in-range configuration
Frame Relay VC	Map-class configuration

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

A service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent (99 percent on the Cisco 10008 router) of the interface bandwidth or the bandwidth allocated to the VC.

To enable Low Latency queueing (LLQ) for Frame Relay (priority queueing [PQ]/CBWFQ), you must first enable Frame Relay Traffic Shaping (FRTS) on the interface using the **frame-relay traffic-shaping** command in interface configuration mode. You then attach an output service policy to the Frame Relay VC using the **service-policy** command in map-class configuration mode.

For a policy map to be successfully attached to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC. For a Frame Relay VC, the total amount of bandwidth allocated must not exceed the minimum committed information rate (CIR) configured for the VC less any bandwidth reserved by the **frame-relay voice bandwidth** or **frame-relay ip rtp priority** map-class commands. If these values are not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is possible only if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use weighted fair queueing (WFQ) by default. Other interfaces use first-in first-out (FIFO) by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

When you attach a service policy with CBWFQ enabled to an interface, commands related to fancy queueing such as those pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED) are available using the modular quality of service command-line interface (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

You can modify a policy map attached to an interface or VC, changing the bandwidth of any of the classes that make up the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amount for all classes that make up the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

After you apply the **service-policy** command to set a class of service (CoS) bit to an Ethernet interface, the policy is set in motion as long as there is a subinterface that is performing 8021.Q or Inter-Switch Link (ISL) trunking. Upon reload, however, the service policy is removed from the configuration with the following error message:

```
Process ‘set’ action associated with class-map voip failed: Set cos supported only with
IEEE 802.1Q/ISL interfaces.
```

Cisco 10000 Series Router Usage Guidelines

The Cisco 10000 series router does not support applying CBWFQ policies to unspecified bit rate (UBR) VCs.

For a policy map to be successfully attached to an interface or a VC, the aggregate of the configured minimum bandwidth of the classes that make up the policy map must be less than or equal to 99 percent of the interface bandwidth or the bandwidth allocated to the VC. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

The total bandwidth is the speed (rate) of the ATM layer of the physical interface. The router converts the minimum bandwidth that you specify to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65535, the router chooses the nearest multiple.

The bandwidth percentage is based on the interface bandwidth. In a hierarchical policy, the bandwidth percentage is based on the nearest parent shape rate.

By default, a minimum bandwidth guaranteed queue has buffers for up to 50 milliseconds of 256-byte packets at line rate, but not less than 32 packets.

For Cisco IOS Release 12.0(22)S and later releases, to enable LLQ for Frame Relay (priority queueing (PQ)/CBWFQ) on the Cisco 10000 series router, first create a policy map and then assign priority to a defined traffic class using the **priority** command. For example, the following sample configuration shows how to configure a priority queue with a guaranteed bandwidth of 8000 kbps. In the example, the Business class in the policy map named "map1" is configured as the priority queue. The map1 policy also includes the Non-Business class with a minimum bandwidth guarantee of 48 kbps. The map1 policy is attached to serial interface 2/0/0 in the outbound direction.

```
class-map Business
    match ip precedence 3
policy-map map1
    class Business
    priority
    police 8000
    class Non-Business
    bandwidth 48
interface serial 2/0/0
    frame-relay encapsulation
    service-policy output map1
```

On the PRE2, you can use the **service-policy** command to attach a QoS policy to an ATM subinterface or to a PVC. However, on the PRE3, you can attach a QoS policy only to a PVC.

Cisco 7600 Series Routers

The **output** keyword is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure QoS based on policy feature cards (PFCs) on the WAN ports on the OC-12 ATM optical services modules (OSM) and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input policy map and an output-policy map to a VLAN interface.

Cisco 10000 Series Routers Control Policy Maps

A control policy map must be activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts, which are listed in order of precedence:

1. Global
2. Interface
3. Subinterface
4. Virtual template
5. VC class

6. PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context. Only one control policy map can be applied to a given context.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the abbreviated form (**ser**) of the **service-policy** command. Instead, you must spell out the command name **service-** before the router accepts the command.

For example, the following error message displays when you attempt to use the abbreviated form of the **service-policy** command:

```
interface GigabitEthernet1/1/0
 ser out ?
% Unrecognized command
 ser ?
% Unrecognized command
```

As shown in the following example, when you enter the command as **service-** followed by a space, the router parses the command as **service-policy**. Entering the question mark causes the router to display the command options for the **service-policy** command.

```
service- ?
inputAssign policy-map to the input of an interface
outputAssign policy-map to the output of an interface
typeConfigure CPL Service Policy
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the **service-policy** command. For example, the router accepts the following commands:

```
interface GigabitEthernet1/1/0
 ser out test
```

Examples

The following example shows how to attach a policy map to a Fast Ethernet interface:

```
interface fastethernet 5/20
 service-policy input pmap1
```

The following example shows how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enables LLQ for Frame Relay:

```
interface Serial1/0.1 point-to-point
 frame-relay interface-dlci 100
 class fragment
 map-class frame-relay fragment
 service-policy output policy9
```

The following example shows how to attach the service policy map named “policy9” to input serial interface 1:

```
interface Serial1
 service-policy input policy9
```

The following example attaches the service policy map named “policy9” to the input PVC named “cisco”:

```
pvc cisco 0/34
service-policy input policy9
vbr-nt 5000 3000 500
precedence 4-7
```

The following example shows how to attach the policy named "policy9" to output serial interface 1 to specify the service policy for the interface and enable CBWFQ on it:

```
interface serial1
 service-policy output policy9
```

The following example attaches the service policy map named "policy9" to the output PVC named "cisco":

```
pvc cisco 0/5
service-policy output policy9
vbr-nt 4000 2000 500
precedence 2-3
```

Cisco 10000 Series Router Examples

The following example shows how to attach the service policy named "userpolicy" to DLCI 100 on serial subinterface 1/0/0.1 for outbound packets:

```
interface serial 1/0/0.1 point-to-point
 frame-relay interface-dlci 100
 service-policy output userpolicy
```

Note You must be running Cisco IOS Release 12.0(22)S or a later release to attach a policy to a DLCI in this way. If you are running a release prior to Cisco IOS Release 12.0(22)S, attach the service policy as described in the previous configuration examples using the legacy Frame Relay commands.

The following example shows how to attach a QoS service policy named "map2" to PVC 0/101 on the ATM subinterface 3/0/0.1 for inbound traffic:

```
interface atm 3/0/0
 atm pxf queuing
interface atm 3/0/0.1
 pvc 0/101
 service-policy input map2
```

Note The **atm pxf queuing** command is not supported on the PRE3 or PRE4.

The following example shows how to attach a service policy named "myQoS" to physical Gigabit Ethernet interface 1/0/0 for inbound traffic. VLAN 4, configured on Gigabit Ethernet subinterface 1/0/0.3, inherits the service policy of physical Gigabit Ethernet interface 1/0/0.

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

The following example shows how to apply the policy map named "policy1" to the virtual template named "virtual-template1" for all inbound traffic. In this example, the virtual template configuration also includes Challenge Handshake Authentication Protocol (CHAP) authentication and PPP authorization and accounting.

```
interface virtual-template1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
 service-policy input policy1
```

The following example shows how to attach the service policy map named "voice" to ATM VC 2/0/0 within a PVC range of a total of three PVCs and enable PVC range configuration mode where a point-to-point subinterface is created for each PVC in the range. Each PVC created as part of the range has the voice service policy attached to it.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
```

The following example shows how to attach the service policy map named "voice" to ATM VC 2/0/0 within a PVC range, where every VC created as part of the range has the voice service policy attached to it. The exception is PVC 1/51, which is configured as an individual PVC within the range and has a different service policy named "data" attached to it in PVC-in-range configuration mode.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
 pvc-in-range 1/51
 service-policy input data
```

The following example shows how to configure a service group named "PREMIUM-SERVICE" and apply the input policy named "PREMIUM-MARK-IN" and the output policy named "PREMIUM-OUT" to the service group:

```
policy-map type service PREMIUM-SERVICE
 service-policy input PREMIUM-MARK-IN
 service-policy output PREMIUM-OUT
```

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports,
frame-relay traffic-shaping	Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface.
frame-relay voice bandwidth	Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Command	Description
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.

show atm vp

To display the statistics for all virtual paths (VPs) on an interface or for a specific VP, use the **show atm vp** command in privileged EXEC mode.

show atm vp [*vpi*]

Syntax Description

vpi	(Optional) ATM network virtual path identifier (VPI) of the permanent virtual path. The range is from 0 to 255. The VPI is an 8-bit field in the header of the ATM cell.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)SB	This command was enhanced in Cisco IOS Release 12.2(33)SB to support VP-based rate counters and enable you to display the average traffic load on the VP for the last 5 minutes. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the output from the **show atm vp** command nolonger displays “ATM” as the type of interface, as shown in the following sample output:

```
Router# show atm vp
    DataCES PEAKCES Avg/Min BurstMCR
InterfaceVPISCVCsVCsKbpsKbpsKbpsCellsKbpsCDVTStatus
3/0/0200N/A00  20000NANANA 140.0ACTIVE
```

In Cisco IOS Release 12.2(31)SB, the output from the **show atm vp** command displays the ATM interface type:

```
Router# show atm vp
    DataCES PEAKCES Avg/Min BurstMCRCDVT
InterfaceVPISCVCsVCsKbpsKbpsKbpsCellsKbpsUsecsStatus
ATM3/0/020000  20000NANANA 140.0ACTIVE
```

Examples

The following is sample output from the **show atm vp** command. This output shows the interface name, the status of the interface, the administrative status of the interface, the port type, and the number of channels in use on the interface. The status of the interface can be UP (in operation) or DOWN (not in operation).

```
Router# show atm vp 1

ATM6/0  VPI: 1, PeakRate: 155000, CesRate: 1742, DataVCs: 1, CesVCs:1, Status: ACTIVE

     VCD    VCI   Type   InPkts   OutPkts   AAL/Encap     Status
     1      100   PVC    n/a      n/a       CES-AAL1      ACTIVE
     13     13    PVC    0        0         AAL5-SNAP     ACTIVE
     409    3     PVC    0        0         F4 OAM        ACTIVE
     410    4     PVC    0        0         F4 OAM        ACTIVE

   TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0, TotalBroadcasts: 0
```

Table 6 describes the fields shown in the display.

Table 6 show atm vp Field Descriptions

Field	Description
ATM6/0	Interface type, slot, and port number of the VP.
VPI	Virtual path identifier of the VP.
PeakRate	Maximum rate, in kbps, at which the VP can send data. Range is 84 kbps to line rate. The default is the line rate.
CesRate	Total circuit emulation service (CES) bandwidth allocated for the VP.
DataVCs	Number of data virtual circuits (VCs) on the VP.
CesVCs	Number of CES VC on the VP.
Status	Current status of the VP. Values are ACTIVE and INACTIVE.
VCD	Virtual circuit descriptor of the VC associated with this VP.
VCI	Virtual channel identifier of the VC associated with this VP.
Type	Type of VC associated with this VP. Values are PVC and SVC.
InPkts	Number of packets received on the VP.
OutPkts	Number of packets transmitted on the VP.
AAL/Encap	Type of encapsulation used on the VC associated with this VP.
Status	Status of the VP (ACTIVE or INACTIVE).
TotalInPkts:	Total number of input packets process-switched and fast-switched on the VP.
TotalOutPkts:	Total number of output packets process-switched and fast-switched on the VP.
TotalInFast	Total number of input packets fast-switched.
TotalOutFast:	Total number of output packets fast-switched.
TotalBroadcasts:	Total number of broadcast packets fast-switched.

Related Commands

Command	Description
atm pvp	Creates a PVP used to multiplex (or bundle) one or more VCs (especially CES and data VCs).

show controllers (line card image)

To display information that is specific to the hardware on a line card, use the **attach** command in privileged EXEC mode to connect to the line card and then use the **show controllers** command in privileged EXEC mode or the **execute-on** command in privileged EXEC mode.

show controllers atm [[*port-number*] [**all** | **sar** | **summary**]]

show controllers fia [**register**]

show controllers {**frfab** | **tofab**} {**bma** {**microcode** | **ms-inst** | **register**} | **qelem** *start-queue-element* [*end-queue-element*] | **qnum** *start-queue-number* [*end-queue-number*] | **queues** | **statistics**}

show controllers io

show controllers l3

show controllers pos {**framers** | **queues** | **registers** | **rxsram** *port-number queue-start-address* [*queue-length*] | **txsram** *port-number queue-start-address* [*queue-length*]}

Syntax Description

atm	Displays the ATM controller information.
port-number	(Optional) Displays request for the physical interface on the ATM card. The range of choices is from 0 to 3.
all	(Optional) Lists all details.
sar	(Optional) Lists SAR interactive command.
summary	(Optional) Lists SAR status summary.
fia	Displays the fabric interface ASIC information.
register	(Optional) Displays the register information.
frfab	(Optional) Displays the "from" (transmit) fabric information.
tofab	(Optional) Displays the "to" (receive) fabric information.
bma	For the **frfab** or **tofab** keywords, displays microcode, micro sequencer, or register information for the silicon queuing engine (SQE), also known as the buffer management ASIC (BMA).
microcode	Displays SQE information for the microcode bundled in the line card and currently running version.
mis-inst	Displays SQE information for the micro sequencer instruction.
register	Displays silicon queuing engine (SQE) information for the register.
qelem	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool queue element summary information.
start-queue-element	Specifies the start queue element number from 0 to 65535.
end-queue-element	(Optional) Specifies the end queue element number from 0 to 65535).
qnum	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool queue detail information.

start-queue-number	Specifies the start free queue number (from 0 to 127).
end-queue-number	(Optional) Specifies the end free queue number (from 0 to 127).
queues	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool information.
statistics	For the **frfab** or **tofab** keywords, displays the BMA counters.
io	Displays input/output registers.
l3	Displays Layer 3 ASIC information.
pos	Displays packet-over-sonic (POS) information for framer registers, framer queues, and ASIC registers.
framers	Displays the POS framer registers.
queues	Displays the POS framer queue information.
registers	Displays the ASIC registers.
rxsram	Displays the receive queue SRAM.
port-number	Specifies a port number (valid range is from 0 to 3).
queue-start-address	Specifies the queue SRAM logical starting address.
queue-length	(Optional) Specifies the queue SRAM length.
txsram	Displays the transmit queue SRAM.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command' behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

This information displayed by this command is of use only to technical support representatives in analyzing unexpected system failures in the field. It is documented here in case you need to provide the displayed statistics to an technical support engineer.

Cisco 10000 Series Router Usage Guidelines

In releases prior to Cisco IOS Release 12.2(33)SB, when you configure the **t1 loopback remote** command on the local router, the command also displays in the running-config file of the far-end router. This is due to the route processor (RP) updating an incorrect parameter when it receives the loopback event message from the line card for loopback requests from the far end.

In Cisco IOS Release 12.2(33)SB, the RP updates the correct parameter and the **show controllers** command correctly displays the loopback CLI commands applied on the local end and displays the loopback events and status received from the line card in response to loopback requests from the far end.

This change in behavior affects the following line cards and is documented in the CSCsm84447 caveat:

- 4-port channelized STM1
- 1-port channelized OC-12
- 6-port channelized T3
- 4-port half-height channelized T3

In Cisco IOS Release 12.2(33)SB, the output from the **show controller** command includes line code information for the 6-port channelized T3 line card and the 8-port E3/DS3 line card. However, because SONET line cards do not have a direct physical link at the T3 or E3 level, the output from the **show controller t3** command does not include line code information.

In Cisco IOS Release 12.2(31)SB, the output from the **show controller** command displays line code information. The output of the **show controller t3** command for SONET-based T3 also includes line code information.

Examples

Because you are executing this command on the line card, you must use the **execute-on** command to use the **show** command, or you must connect to the card using the **attach** command. All examples in this section use the **execute-on** command

The following is partial sample output from the **show controllers atm** command:

```
Router# execute-on slot 4 show controllers atm 0

TX SAR (Beta 1.0.0) is Operational;
RX SAR (Beta 1.0.0) is Operational;

Interface Configuration Mode:
        STS-12c

Active Maker Channels: total # 6
VCID  ChnnlID  Type  OutputInfo    InPkts   InOAMs  MacString
   1   0888    UBR    0C010010          0         0  08882000AAAA030000000800
   2   0988    VBR    04010020          0         0  09882000
   3   8BC8    UBR    0C010030          0         0  8BC82000AAAA030000000800
   4   0E08    UBR    0C010040          0         0  0E082000AAAA030000000800
  10   1288    VBR    040100A0          0         0  12882000
  11   8BE8    VBR    0C0100B0          0         0  8BE82000AAAA030000000800

SAR Total Counters:
total_tx_idle_cells 215267  total_tx_paks 0  total_tx_abort_paks 0
total_rx_paks 0  total_rx_drop_paks 0  total_rx_discard_cells 15

Switching Code Counters:
total_rx_crc_err_paks 0  total_rx_giant_paks 0
total_rx_abort_paks 0  total_rx_crc10_cells 0
total_rx_tmout_paks 0  total_rx_unknown_paks 0
total_rx_out_buf_paks 0  total_rx_unknown_vc_paks 0
BATMAN Asic Register Values:
hi_addr_reg 0x8000, lo_addr_reg 0x000C, boot_msk_addr 0x0780,
rmcell_msk_addr 0x0724, rmcnt__msk_addr 0x07C2, txbuf_msk_addr 0x070C,
.
.
.
CM622 SAR Boot Configuration:
txind_q_addr 0x14000 txcmd_q_addr 0x20000
.
.
.
```

```
SUNI-622 Framer Register Values:
Master Rst and Ident/Load Meters Reg (#0x0): 0x10
Master Configuration Reg (#0x1): 0x1F
Master Interrupt Status Reg (#0x2): 0x00
PISO Interrupt Reg (#0x3): 0x04
Master Auto Alarm Reg (#0x4): 0x03
Master Auto Alarm Reg (#0x5): 0x07
Parallel Output Port Reg (#0x6): 0x02
.
.
.
BERM Line BIP Threshold LSB Reg (#0x74): 0x00
BERM Line BIP Threshold MSB Reg (#0x75): 0x00
Router#
```

The following is partial sample output from the **show controllers** command:

```
Router# execute-on slot 6 show controllers

Interface POS0
Hardware is BFLC POS
lcpos_instance struct   60311B40
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000400
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS1
Hardware is BFLC POS
lcpos_instance struct   603142E0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000600
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop
.
.
.
Router#
```

The following is partial sample output from the **show controllers pos framers** command:

```
Router# execute-on slot 6 show controllers pos framers

Framer 0, addr=0x12000400:
master reset            C0
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00

Framer 1, addr=0x12000600:
master reset            C0
```

```
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00

Framer 2, addr=0x12000800:
master reset            C0
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00
.
.
.
Router#
```

The following is partial sample output from the **show controllers fia** command:

```
Router# execute-on slot 7 show controllers fia

========= Line Card (Slot 7) =======

Fabric configuration: Full bandwidth redundant
Master Scheduler: Slot 17

From Fabric FIA Errors
----------------------
redund fifo parity 0          redund overflow 0          cell drops 0
crc32 lkup parity  0          cell parity     0          crc32      0
          0          1          2          3          4
       --------   --------   --------   --------   --------
los    0          0          0          0          0
crc16  0          0          0          0          0

To Fabric FIA Errors
--------------------
sca not pres 0          req error     0          uni fifo overflow 0
grant parity 0          multi req     0          uni fifo undrflow 0
cntrl parity 0          uni req       0          crc32 lkup parity 0
multi fifo   0          empty dst req 0          handshake error   0
```

Related Commands

Command	Description
clear controllers	Resets the T1 or E1 controller.

show controllers t3

To display information about the T3 links and to display the hardware and software driver information for the T3 controller, use the **show controllers t3** command in privileged EXEC mode.

Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 Series, Cisco 3725, and Cisco 3745 Routers

show controllers t3 *slot*/*port* [**brief** | **tabular**]

Cisco 7200 Series Routers

show controllers t3 [*bay*/*port*[/*t1-channel*]] [**brief** | **errors** | **tabular** | **remote performance** [**brief** | **tabular**]]

Cisco 7500 Series Routers

show controllers t3 [*slot*/*bay*/*port*[/*t1-channel*]] [**brief** | **errors** | **tabular** | **remote performance** [**brief** | **tabular**]]

Cisco AS5800 Access Servers

show controllers t3 *dial-shelf*/*slot*/*t3-port*

Syntax Description

slot	Slot number. Refer to the appropriate hardware manual for slot information.
/*port*	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.
/*bay*	(Optional) The port-adaptor-bay number. Refer to the appropriate hardware manual for bay information
/*t1-channel*	(Optional) Number between 1 and 28 that represents the T1 channel for the Channelized T3 Interface Processor (CT3IP) on Cisco 7200 series and Cisco 5200 series routers.
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the CT3 interface card.
/*slot*	Location of the CT3 interface card in the dial shelf chassis.
/*t3-port*	T3 port number. The only valid value is 0.
brief	(Optional) Displays a subset of information.
errors	(Optional) Displays a history of alarm events that causes a T3 controller or a T1 controller of a T3 to transition from an Up state to a Down state. The history size is 18 events.
tabular	(Optional) Displays information in a tabular format.
remote performance	(Optional) Displays the far-end ANSI performance monitor information when enabled on the T1 channel with the **t1 fdl ansi** controller configuration command.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	This command was implemented on the Cisco AS5800 access server.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(19c)	This command was modified to display error throttling and alarm conditions that cause the T3 controller to enter a failure state.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Cisco 7500 Series Routers

This command displays controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

By using the **errors** keyword, this command displays history that identifies which alarm events caused a T3 or T1 controller of a T3 to go down for the Cisco 7500 and Cisco 7200 series routers.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based numbering scheme (0 to 27) used with other Cisco products. This is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

The **show controllers t3** command also displays Maintenance Data Link (MDL) information (received strings) if MDL is configured and framing is set to C-bit.

Cisco 10000 Series Router Usage Guidelines

In releases prior to Cisco IOS Release 12.2(33)SB, when you configure the **t1 loopback remote** command on the local router, the command also displays in the running-config file of the far-end router. This is due to the route processor (RP) updating an incorrect parameter when it receives the loopback event message from the line card for loopback requests from the far end.

In Cisco IOS Release 12.2(33)SB, the RP updates the correct parameter and the **show controllers** command correctly displays the loopback CLI commands applied on the local end and displays the loopback events and status received from the line card in response to loopback requests from the far end.

This change in behavior affects the following line cards and is documented in the CSCsm84447 caveat:

- 4-port channelized STM1
- 1-port channelized OC-12
- 6-port channelized T3
- 4-port half-height channelized T3

In Cisco IOS Release 12.2(33)SB, the output from the **show controller** command includes line code information for the 6-port channelized T3 line card and the 8-port E3/DS3 line card. However, because SONET line cards do not have a direct physical link at the T3 or E3 level, the output from the **show controller t3** command does not include line code information.

In Cisco IOS Release 12.2(31)SB, the output from the **show controller** command displays line code information. The output of the **show controller t3** command for SONET-based T3 also includes line code information.

Examples

Cisco 7200 Series Routers

The following is partial output from the **show controllers t3 errors** command for Cisco IOS Release 12.2(19c) for a specific T1 controller of a T3 on a Cisco 7200 series router with a bay/port of 4/1, displaying the T1 1 alarm event of OOF:

```
Router# show controllers t3 4/1/1 errors

  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
```

The following is partial output from the **show controllers t3 errors** command from Cisco IOS Release 12.2(19c) for a T3 controller on a Cisco 7200 series router with a bay/port of 4/1, displaying a history of all alarm events on all 28 T1 channels:

```
Router# show controllers t3 4/1 errors

  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
  T1 2 Error Log Information
  present alarm: NONE
  T1 3 Error Log Information
  present alarm: NONE
  T1 4 Error Log Information
  present alarm: NONE
  T1 5 Error Log Information
  present alarm: NONE
  T1 6 Error Log Information
  present alarm: NONE
  T1 7 Error Log Information
  present alarm: NONE
  T1 8 Error Log Information
  present alarm: NONE
  T1 9 Error Log Information
  present alarm: NONE
  T1 10 Error Log Information
  present alarm: NONE
  T1 11 Error Log Information
```

```
  present alarm: NONE
.
.
.
```

.Cisco 7500 Series Routers

The following is partial output from the **show controllers t3 errors** command from Cisco IOS Release 12.2(19c) for a T3 controller with a slot/bay/port of 1/4/1, displaying a history of all alarm events on all 28 T1 channels:

```
Router# show controllers t3 1/4/1 errors

  T3 1/4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
  T1 2 Error Log Information
  present alarm: NONE
  T1 3 Error Log Information
  present alarm: NONE
  T1 4 Error Log Information
  present alarm: NONE
  T1 5 Error Log Information
  present alarm: NONE
  T1 6 Error Log Information
  present alarm: NONE
  T1 7 Error Log Information
  present alarm: NONE
.
.
.
```

The following is partial output from the **show controllers t3 errors** command from Cisco IOS Release 12.2(19c) for a specific T1 controller of a T3 on a Cisco 7200 series router with a bay/port of 4/1, displaying the T1 1 alarm event of OOF:

```
Router# show controllers t3 4/1/1 errors

  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
.
.
.
```

Table 7 describes the error field shown in the display.

Table 7 show controllers t3 Error Field Description

Field	Description
AIS	alarm indication signal. In a T1 transmission, an all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity and to indicate to the receiving terminal that there is a transmission fault that is located either at, or upstream from, the transmitting terminal.
RAI	remote alarm indication. Indicates a yellow alarm from the remote end of the T1 transmission.
OOF	out of frame. An OOF defect is detected when any three or more errors in sixteen or fewer consecutive F-bits occur.
LOS	loss of signal. A loss of signal occurs when n consecutive zeros is detected on an incoming signal.
NONE	No error is detected.

The following is partial output from the **show controllers t3** command from Cisco IOS Release 12.2(19c):

```
Router# show controllers t3 2/1/0

T3 2/1/0 is down.  Hardware is 2CT3 single wide port adapter
  CT3 H/W Version:0.2.2, CT3 ROM Version:1.0, CT3 F/W Version:2.5.1
  FREEDM version:1, reset 0 resurrect 0
  Applique type is Channelized T3
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  FEAC code received:No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal
  Rx-error throttling on T1's ENABLED
  Rx throttle total 0, equipment customer loopback
  Data in current interval (545 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     545 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 1:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     900 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 2:
<snip>
```

The following is partial output from the **show controllers t3** command from Cisco IOS Release 12.2(19c) for the T1 channel of the T3 controller:

```
Router# show controllers t3 2/1/0 /1

T3 2/1/0 is down.  Hardware is 2CT3 single wide port adapter
  CT3 H/W Version:0.2.2, CT3 ROM Version:1.0, CT3 F/W Version:2.5.1
  FREEDM version:1, reset 0 resurrect 0

  T1 1 is down
  timeslots:1-24
```

```
  FDL per AT&T 54016 spec.
  Receiver has loss of signal.
  Framing is ESF, Clock Source is Internal
  Data in current interval (0 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
```

The following is partial output from the **show controllers t3** command:

```
Router# show controllers t3 3/0/0

T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 0.10.0
  Mx H/W version: 2, Mx ucode ver: 1.24
  Applique type is Channelized T3
  No alarms detected.
  FEAC code received: No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal.
  Ext1: LOS, Ext2: LOS, Ext3: LOS, Test: OK
  Data in current interval (39 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Severely Err Secs
     0 Severely Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Total Data (last 1 15 minute intervals):
     0 Line Code Violations, 0 P-bit Coding Violation,
     0 C-bit Coding Violation,
     0 P-bit Err Secs, 0 P-bit Severely Err Secs,
     0 Severely Err Framing Secs, 0 Unavailable Secs,
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.
T1 1 is down, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per ANSI T1.403 and AT&T 54016 spec.
  Configured for FDL Remotely Line Looped
  No alarms detected.
  Framing is ESF, LineCode is B8ZS, Clock Source is Internal.
  BERT test result (running)
      Test Pattern: All 0's, Status: Sync, Sync Detected: 1
      Interval: 4 minute(s), Tim Remain: 4 minute(s)
      Bit Errors (Sync BERT Started): 0 bits
      Bit Errors (Sync last Sync): 0 bits, Bits Received: 7 Mbits
```

The following is partial output from the **show controllers t3 brief** command:

```
Router# show controllers t3 3/0/0 brief

T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 0.10.0
  Mxt H/W version: 2, Mxt ucode ver: 1.24
  Applique type is Channelized T3
  No alarms detected.
  FEAC code received: No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal.
  Ext1: LOS, Ext2: LOS, Ext3: LOS, Test: OK

  T1 1 is up, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per ANSI T1.403 and AT&T 54016 spec.
```

```
  Configured for FDL Remotely Line Looped
  No alarms detected.
  Framing is ESF, LineCode is B8ZS, Clock Source is Internal.
  BERT test result (done)
      Test Pattern: All 0's, Status: Not Sync, Sync Detected: 1
      Interval: 4 minute(s), Tim Remain: 0 minute(s)
      Bit Errors(Sync BERT Started): 0 bits
      Bit Errors(Sync last Sync): 0 bits, Bits Received: 368 Mbits
.
.
.
```

The following is partial output from the **show controllers t3 tabular** command:

```
Router# show controllers t3 3/0/0 tabular

T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 1.2, CT3 F/W Version: 2.1.0
  Mx H/W version: 2, Mx ucode ver: 1.25
  Applique type is Channelized T3
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal.
  Ext1: AIS, Ext2: LOS, Ext3: LOS, Test: LOS
  INTERVAL      LCV    PCV    CCV    PES   PSES  SEFS   UAS    LES    CES   CSES
  08:56-09:11     0      0      0      0      0     0      0      0      0      0
  08:41-08:56     0      0      0      0      0     0      0      0      0      0
  08:26-08:41     0      0      0      0      0     0      0      0      0      0
  Total           0      0      0      0      0     0      0      0      0      0
.
.
.

T1 2 is up, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  INTERVAL      LCV    PCV    CSS   SELS    LES     DM     ES    BES    SES    UAS     SS
  08:56-09:11     0      0      0      0      0      0      0      0      0      0      0
  08:41-08:56     0      0      0      0      0      0      0      0      0      0      0
  08:26-08:41     0      0      0      0      0      0      0      0      0      0      0
  Total           0      0      0      0      0      0      0      0      0      0      0
```

The following output shows a controller with a high number of errors on the line, thus showing a throttle count (RX throttles).

```
Router# show controllers t3 6/0/0 tabular

  T1 2 is up
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Clock Source is Line, Rx throttles 47
  INTERVAL      LCV    PCV    CSS   SELS    LES     DM     ES    BES    SES    UAS SS
  07:48-07:53     0      0      0      0      0      0      0      0      0      0
```

The following is partial output from the **show controllers t3 remote performance** command. This information is available if the **t1 fdl ansi** controller configuration command is enabled for a T1 channel on a CT3IP.

```
Router# show controllers t3 3/0/0 remote performance

T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 20.2.0
  Mx H/W version: 2, Mx ucode ver: 1.25

  T1 1 - Remote Performance Data
  Data in current interval (356 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Data in Interval 1:
     1 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     2 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Data in Interval 2:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Total Data (last 2 15 minute intervals):
     1 Path Code Violations
     1 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     2 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
.
.
.
```

Table 8 describes the fields shown in the display.

Table 8 show controllers t3 Field Descriptions—Cisco 7500 Series

Field	Description
T3 3/0/0 is up	T3 controller in slot 3 is operating. The controller's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
CT3 H/W Version	Version number of the hardware.
CT3 ROM Version	Version number of the ROM.
CT3 F/W Version	Version number of the firmware.
Mx H/W version	Hardware version number of the HDLC controller chip.
Mx ucode ver	Microcode version of the HDLC controller chip.
Applique type	Controller type.

Table 8 show controllers t3 Field Descriptions—Cisco 7500 Series (continued)

Field	Description
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled).
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Framing type on the CT3IP. Values are M23, C-Bit, and Auto-detect.
Line Code	Line coding format on the CT3IP.
Clock Source	Clock source on the CT3IP. Values are internal or line.
RX-error throttling	Indicates that error throttling is enabled. The **error throttling** command disables the T1 level clock in order to stop receiving error data packets on a T1 controller. If any single interface receives a burst of errors over a short duration, such as 400 errors in 100 milliseconds, the T1 clock will be turned off for a period of 100 milliseconds.
RX throttles	The presence of the throttle count indicates that there are many input errors on lines. On the CT3 PA, the T1 is throttled when there are a number of input errors on an interface (400 errors in 100 milliseconds). The T1 is throttled even if one of the interfaces on it sees continuous errors. The 1-second periodic process checks for throttled interfaces and unthrottles them back.

Table 8 show controllers t3 Field Descriptions—Cisco 7500 Series (continued)

Field	Description
BERT test result	BERT test information is available if the **t1 bert** controller configuration command is enabled for the T1 channel on the CT3IP. The BERT results include the following information: • Test Pattern—Type of test pattern selected. • Status—Status of the test. • Sync Detected—Number of times the pattern synch is detected (that is, the number of times the pattern goes from No Sync to Sync). • Interval—Duration selected. • Tim Remain—Time remaining on the BERT test. • Bit Errors (Sync BERT Started)—Number of bit errors during the BERT test. • Bit Errors (Sync last Sync)—Number of bit errors since the last pattern sync was detected. • Bits Received—Total bits received. When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.
Data in current interval (39 seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.

Table 8 show controllers t3 Field Descriptions—Cisco 7500 Series (continued)

Field	Description
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, refer to RFC 1407, *DS3 MIB Variables*.
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last 1 15 minute intervals)	Shows the last 15-minute accumulation period.
T1 1 is up	T1 channel is operating. The channel's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
speed	Speed of the T1 channel, in kbps.
non-inverted data	Indicates if the T1 channel is configured for inverted data.
timeslots	Time slots assigned to the T1 channel.
FDL per ANSI T1.403 and AT&T 54016 spec.	Performance monitoring is via Facility Data Link per ANSI T1.403 and AT&T standard specification number 54016.
No alarms detected	Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Framing	Type of framing used on the T1 channel. Values are ESF or SF.
Line Code	Type of line coding used on the T1 channel. Values are B8ZS or AMI.
Clock Source	Clock source on the T1 channel. Values are internal or line.
Path Code Violations	Path coding violation (PCV) error event is a frame synchronization bit error in the D4 and E1-no-CRC formats or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.

Table 8 show controllers t3 Field Descriptions—Cisco 7500 Series (continued)

Field	Description
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, refer to RFC 1406, *Definitions of Managed Objects for DS1 and E1 Interface Types*.
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Stuffed Secs	Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.

Cisco AS5800 Access Servers

The following example shows the summary status of the T3 controller located in shelf 1, slot 4, port 0:

```
Router# show controllers t3 1/4/0 brief

T3 1/4/0 is up.
 Applique type is Channelized T3
 No alarms detected.
 MDL transmission is disabled

 FEAC code received: Multiple DS1 LOS/HBER
 Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line.
 Data in current interval (491 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 80 15 minute intervals):
     3 Line Code Violations, 4 P-bit Coding Violation,
     2 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     2 Unavailable Secs, 0 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The following example shows the detailed status of the T3 controller connected to the Cisco AS5800 in shelf 1, slot 4, port 0. Notice that the detailed information shows the last eighty-six 15-minute time periods.

```
Router# show controllers t3 1/4/0

T3 1/4/0 is up.
 Applique type is Channelized T3
 No alarms detected.
 MDL transmission is disabled

 FEAC code received: Multiple DS1 LOS/HBER
 Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line.
 Data in current interval (91 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 1:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 2:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 3:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 4:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.

Data in Interval 86:
     3 Line Code Violations, 4 P-bit Coding Violation
     2 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     2 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 86 15 minute intervals):
     3 Line Code Violations, 4 P-bit Coding Violation,
     2 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     2 Unavailable Secs, 0 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Table 9 describes the fields shown in the display.

Table 9 show controllers t3 Field Descriptions—Cisco AS5800

Field	Description
T3 1/4/0 is up	T3 controller connected to this Cisco AS5800 access server in shelf 1, slot 4, port 0 is up. The controller's state can be up, down, or administratively down. Loopback conditions are shown by Locally Looped or Remotely Looped.
Applique type	Describes the type of controller.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending alarm indication signal (AIS). • Receiver has loss of signal (LOS). • Receiver is getting AIS. • Receiver has loss of frame (LOF). • Receiver has remote alarm. • Receiver has no alarms.
MDL transmission	Maintenance Data Link status (either enabled or disabled). Used for carrying performance information and control signals across the network toward the far-end T3 unit. It is the counterpart of Facility Data Link (FDL) in a T1 link.
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Standard T3 framing type: M23, C-Bit, or Auto-detect.
Line Code	Standard T3 line-coding format. In this example, the line-coding format is bipolar 3-zero substitution (B3ZS).
Clock Source	The source of the synchronization signal (clock): line or internal. In this example, the line is providing the clock signal.

Table 9 show controllers t3 Field Descriptions—Cisco AS5800 (continued)

Field	Description
Data in current interval (... seconds elapsed)	Summary statistics for T3 signal quality for the current time interval of 900 seconds (15 minutes). In this example, the statistics are for current partial interval. Statistics roll into the 24-hour accumulation buffer every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the Line Code Violations (LCVs) by one regardless of the length of the zero string.
P-bit Coding Violation	P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code. Referred to as PCV.
C-bit Coding Violation	Count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. Referred to as CCV.
P-bit Err Secs	Number of seconds with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
P-bit Severely Err Secs	Number of seconds with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Number of a seconds with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Line Errored Secs	Number of seconds in this interval during which one or more code violations or one or more LOS defects occurred. Referred to as LES.
C-bit Errored Secs	Number of seconds with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted. Referred to as CES.
C-bit Severely Errored Secs	Number of seconds with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last ... 15 minute intervals)	Summary statistics for T3 signal quality for 15-minute intervals. Every 24 hours (96 intervals) the counters in this data block clear.

Cisco 10000 Series Router Examples

The following examples from the **show controller t3** command show the information that displays when the router is running Cisco IOS Release 12.2(33)SB and Cisco IOS Release 12.2(31)SB:

Cisco IOS Release 12.2(33)SB —No Line Code Information

```
Router# show controller t3 5/0/0.1
T3 5/0/0.1 is up. Hardware is C10K CHOC12 line card
    Applique type is Channelized T3.
    Controller is in unchannelized mode.
    No alarms detected.
    MDL transmission is disabled.

    FEAC code received: No code is being received.
    Framing is C-BIT Parity (Configured), Clock Source is Internal.
    DSU mode is cisco, DSU bandwidth is 44210.
```

Cisco IOS Release 12.2(31)SB —Line Code Information

```
Router# show controller t3 5/0/0.1
T3 5/0/0.1 is up. Hardware is C10K CHOC12 line card
    Applique type is Channelized T3.
    Controller is in channelized mode.
    No alarms detected.
    MDL transmission is disabled.

    FEAC code received: No code is being received
    Framing is C-BIT Parity (Configured)
    Line Code is B3ZS, Clock Source is Internal.
```

show diag

To display hardware and diagnostic information for a networking device, a line card, a processor, a jacket card, a chassis, or a network module, use the **show diag** command in privileged EXEC configuration mode.

show diag [*slot-number*] [**details** | **summary**]

Cisco 7304 Router

show diag [*slot-number* | **chassis** | subslot *slot*/*subslot*] [**details** | **summary**]

Shared Port Adapters

show diag [**subslot** *slot*/*subslot*] [**details** | **summary**]

Network Module

show diag [*slot-number*]

Cisco 10000 Series Router

show diag [*slot*/*subslot*] [**details** | **summary**] [**crashdump**]

Syntax Description

slot-number	(Optional) Slot number of the interface. If a slot number is not specified, diagnostic information for all slots is displayed.
details	(Optional) Displays more details than the normal **show diag** output.
summary	(Optional) Displays a summary (one line per slot) of the chassis.
chassis	(Optional) **Cisco 7304 Router** Specifies the display of diagnostic information about the backplane, power supplies, and fan modules.
subslot *slot*/*subslot*	(Optional) **Shared Port Adapters** Specifies display of diagnostic information about the shared port adapter (SPA), where: • *slot*—Chassis slot number. See the appropriate hardware manual for slot information. 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*—Secondary slot number on a SIP where a SPA is installed. See 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.

Defaults

None

Privileged EXEC

Command History

Release	Modification
11.1CA	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.
11.2P	This command output was modified for the PA-12E/2FE port adapter, PA-E3 port adapter, and PA-T3 port adapter.
11.2GS	This command was implemented on the Cisco 12000 series Gigabit Switch Routers (GSRs).
11.3 XA	This command was integrated in Cisco IOS Release 11.3 XA.
12.0	This command was implemented on the Cisco AS5300.
12.0(5)XQ	This command was implemented on the Cisco 1750 router.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(9)EX	This command was introduced on the Cisco 7300 series routers, and the *slot-number* argument and **chassis** keyword were added.
12.1(10)EX	This command was enhanced to display information about Field-Programmable Gate Array (FPGA) image versions on installed NSEs and line cards on Cisco 7304 routers.
12.2(11)YZ	Support was added for the 7300-CC-PA.
12.2(8)T	This command was implemented for AIC and WIC cards on the Cisco 2600 series routers and the Cisco 3600 series routers.
12.2(13)T	This command was implemented for the AIM-VPN/EPII and AIM-VPN/HPII cards on the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII card on the Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S and implemented on the Cisco 7304 router.
12.3(4)T	Support for the AIM-VPN/BPII card on the Cisco 2600XM series was integrated into Cisco IOS Release 12.3(4)T.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and the **subslot** *slot*/*subslot* keyword and arguments were added to support SPAs on the Cisco 7304 router.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and the **subslot** *slot*/*subslot* keyword and arguments were added to support SIPs and SPAs on the Cisco 12000 series router.
12.4(4)T	This command was implemented for the HWIC-1ADSL and HWIC-1ADSLI interface cards on the following platforms: Cisco 1800 (modular) series, Cisco 2800 series, and Cisco 3800 series routers.
12.4(9)T	This command was implemented for the NME-AON-K9= enhanced network module on the following platforms: Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3725, and Cisco 3745 routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
12.2(33)SB	This command was enhanced with a **crashdump** option to enable you to display crashdump files collected on the SIP. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Use this command to determine the type of hardware installed in your router, and to show detailed hardware information and EEPROM version information.

This command displays information for the motherboard, WAN interface cards (WICs), voice interface cards (VICs), high-speed WICs (HWICs), ATM interface cards (AICs), advanced integration modules (AIMs), port adapters, shared port adapters (SPAs), modular services cards (MSCs), SPA interface processors (SIPs), and enhanced network modules (NME).

Cisco 7304 Router Usage Guidelines

For the Cisco 7304 router, this command applies to NEs, line cards, MSCs, and SPAs.

- To display hardware information for an NSE, line card, or MSC in the specified slot, use the *slot-number* argument. For MSCs, using this argument displays information about the MSC and each of its installed SPAs.
- To display hardware information about the backplane, power supplies, and fan modules, use the **chassis** keyword.

Shared Port Adapter Usage Guidelines

- To display hardware information for an MSC or SIP only in a specified slot, use the *slot-number* argument.
- To display hardware information for a SPA only, use the **show diag subslot** *slot*/*subslot* version of this command.

Cisco 10000 Series Router Usage Guidelines

The **crashdump** option of the **show diag** command enables you to display any crashdump files collected on the SPA Interface Processor (SIP). The SIP stores the crashdump files by a reference number from 1 to 60.

To view a crashdump file, do the following:

Step 1 Determine the most recent crashdump number:

a. Enter the **show diag** *slot*/*subslot* command.

b. Look for the latest crashdump number in the following section of the command output:

```
Number of crashdumps : output number
```

Step 2 Enter the following command to view the crashdump file:

```
show diag slot/subslot crashdump number
```

Note The subslot value is always zero for the SIP.

Examples

1-Port T3 Serial Port Adapter: Example

The following is sample output from the **show diag** command for a 1-port T3 serial port adapter in chassis slot 1 on a Cisco 7200 series router:

```
Router# show diag 1

Slot 1:
        Physical slot 1, ~physical slot 0xE, logical slot 1, CBus 0
        Microcode Status 0x4
        Master Enable, LED, WCS Loaded
        Board is analyzed
        Pending I/O Status: None
        EEPROM format version 1
        VIP2 controller, HW rev 2.4, board revision D0
        Serial number: 04372053  Part number: 73-1684-03
        Test history: 0x00        RMA number: 00-00-00
        Flags: cisco 7000 board; 7500 compatible

        EEPROM contents (hex):
          0x20: 01 15 02 04 00 42 B6 55 49 06 94 03 00 00 00 00
          0x30: 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

        Slot database information:
        Flags: 0x4      Insertion time: 0x14A8 (5d02h ago)

        Controller Memory Size: 16 MBytes DRAM, 1024 KBytes SRAM

        PA Bay 0 Information:
                T3 Serial PA, 1 ports
                EEPROM format version 1
                HW rev FF.FF, Board revision UNKNOWN
                Serial number: 4294967295  Part number: 255-65535-255
```

Cisco 12000 Series Internet Router: Example

The following is sample output from the **show diag** command on a Cisco 12000 series Internet router:

```
Router# show diag 3

SLOT 3  (RP/LC 3 ): 4 Port Packet Over SONET OC-3c/STM-1 Multi Mode
  MAIN: type 33,  00-0000-00 rev 70 dev 0
        HW config: 0x01    SW key: 00-00-00
  PCA:  73-2147-02 rev 94 ver 2
        HW version 1.0  S/N 04499695
  MBUS: MBUS Agent (1)  73-2146-05 rev 73 dev 0
        HW version 1.1  S/N 04494882
        Test hist: 0x00    RMA#: 00-00-00    RMA hist: 0x00
  DIAG: Test count: 0x05000001    Test results: 0x00000000
  MBUS Agent Software version 01.27 (RAM) using CAN Bus A
  ROM Monitor version 00.0D
  Fabric Downloader version used 00.0D (ROM version is 00.0D)
  Board is analyzed
  Board State is Line Card Enabled (IOS  RUN )
  Insertion time: 00:00:10 (00:04:51 ago)
  DRAM size: 33554432 bytes
  FrFab SDRAM size: 67108864 bytes
  ToFab SDRAM size: 16777216 bytes
```

The following is sample output from the **show diag** command with the **summary** keyword:

```
Router# show diag summary

SLOT 0  (RP/LC 0 ): Route Processor
SLOT 2  (RP/LC 2 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 4  (RP/LC 4 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 7  (RP/LC 7 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 9  (RP/LC 9 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 11 (RP/LC 11): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 16 (CSC 0   ): Clock Scheduler Card
SLOT 17 (CSC 1   ): Clock Scheduler Card
SLOT 18 (SFC 0   ): Switch Fabric Card
SLOT 19 (SFC 1   ): Switch Fabric Card
SLOT 20 (SFC 2   ): Switch Fabric Card
SLOT 24 (PS A1   ): AC Power Supply
SLOT 26 (PS B1   ): AC Power Supply
SLOT 28 (TOP FAN ): Blower Module
SLOT 29 (BOT FAN ): Blower Module
```

The following is sample output from the **show diag** command with the **details** keyword:

```
Router# show diag 4 details

SLOT 4  (RP/LC 4): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
  MAIN: type 33,  800-2389-01 rev 71 dev 16777215
        HW config: 0x00    SW key: FF-FF-FF
  PCA:  73-2275-03 rev 75 ver 3
        HW version 1.1  S/N 04529465
  MBUS: MBUS Agent (1)  73-2146-06 rev 73 dev 0
        HW version 1.1  S/N 04541395
        Test hist: 0xFF    RMA#: FF-FF-FF    RMA hist: 0xFF
  DIAG: Test count: 0x05000001    Test results: 0x00000000
  EEPROM contents (hex):
  00: 01 00 01 00  49 00 08 62  06 03 00 00  00 FF FF FF
  10: 30 34 35 34  31 33 39 35  FF FF FF FF  FF FF FF FF
  20: 01 01 00 00  00 00 00 FF  FF FF FF FF  FF FF FF FF
  30: A5 FF A5 A5  A5 A5 FF A5  A5 A5 A5 A5  A5 A5 A5 A5
  40: 00 21 01 01  00 49 00 08  E3 03 05 03  00 01 FF FF
  50: 03 20 00 09  55 01 01 FF  FF FF 00 FF  FF FF FF FF
  60: 30 34 35 32  39 34 36 35  FF FF FF FF  FF FF FF FF
  70: FF FF FF FF  FF FF FF FF  05 00 00 01  00 00 00 00
  MBUS Agent Software version 01.24 (RAM)
  Fabric Downloader version 00.0D
  Board is analyzed
  Flags: 0x4
  Board State is Line Card Enabled (IOS  RUN)
  Insertion time: 00:00:10 (00:04:51 ago)
  DRAM size: 33554432 bytes
  FrFab SDRAM size: 67108864 bytes
  ToFab SDRAM size: 16777216 bytes
```

ATM SAR AIM in a Cisco 3660: Example

The following is sample output from the **show diag** command for one ATM Segmentation and Reassembly (SAR) AIM in a Cisco 3660 router:

```
Router# show diag 0

3660 Chassis type: ENTERPRISE

c3600 Backplane EEPROM:
    Hardware Revision        : 1.0
    Top Assy. Part Number    : 800-04740-02
.
.
.
ATM AIM: 1
    ATM AIM module with SAR only (no DSPs)
    Hardware Revision        : 1.0
    Top Assy. Part Number    : 800-03700-01
    Board Revision           : A0
    Deviation Number         : 0-0
    Fab Version              : 02
    PCB Serial Number        : JAB9801ABCD
```

NM-AIC-64 Installed in a Cisco 2611: Example

The following is sample output from the **show diag** command for a Cisco 2611 router with the NM-AIC-64 installed.

```
Router# show diag

Slot 0:
C2611 2E Mainboard Port adapter, 2 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 2.3
PCB Serial Number : JAD044808SG (1090473337)
Part Number : 73-2840-13
RMA History : 00
RMA Number : 0-0-0-0
Board Revision : C0
Deviation Number : 0-0
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 00 92 41 02 03 C1 18 4A 41 44 30 34 34
0x10: 38 30 38 53 47 20 28 31 30 39 30 34 37 33 33 33
0x20: 37 29 82 49 0B 18 0D 04 00 81 00 00 00 00 42 43
0x30: 30 80 00 00 00 00 FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Slot 1:
NM_AIC_64 Port adapter, 3 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 1.0
Part Number : 74-1923-01
Board Revision : 02
PCB Serial Number : DAN05060012
EEPROM format version 4
EEPROM contents (hex):
```

```
0x00: 04 FF 40 02 55 41 01 00 82 4A 07 83 01 42 30 32
0x10: C1 8B 44 41 4E 30 35 30 36 30 30 31 32 FF FF FF
0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Table 10 describes significant fields shown in the display.

Table 10 show diag (AIC) Field Descriptions

Field	Description
C2611 2E Mainboard Port adapter, 2 ports	Line card type; number of ports available.
Port adapter is analyzed	The system has identified the port adapter.
Port adapter insertion time	Elapsed time since insertion.
Hardware Revision	Version number of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
Part Number	Part number of the port adapter.
RMA History	Counter that indicates how many times the port adapter has been returned and repaired.
RMA Number	Return material authorization number, which is an administrative number assigned if the port adapter needs to be returned for repair.
Board Revision	Revision number (signifying a minor revision) of the port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

AIM-VPN in a Cisco 2611XM: Example

The following example shows how to obtain hardware information about an installed AIM-VPN on the Cisco 2611XM router.

```
Router# show diag 0

Encryption AIM 1:
        Hardware Revision        :1.0
        Top Assy. Part Number    :800-03700-01
        Board Revision           :A0
        Deviation Number         :0-0
        Fab Version              :02
        PCB Serial Number        :JAB9801ABCD
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 03 0B 41 01 00 C0 46 03 20 00 0E 74 01
          0x10:42 41 30 80 00 00 00 00 02 02 C1 8B 4A 41 42 39
          0x20:38 30 31 41 42 43 44 03 00 81 00 00 00 00 04 00
          0x30:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Table 11 describes significant fields shown in the display.

Table 11 show diag (AIM-VPN) Field Descriptions

Field	Description
Hardware Revision	Version number of the port adapter.
Top Assy. Part Number	Part number of the port adapter.
Board Revision	Revision number (signifying a minor revision) of the port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
RMA Number	Return material authorization number, which is an administrative number assigned if the port adapter needs to be returned for repair.
RMA History	Counter that indicates how many times the port adapter has been returned and repaired.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

MSC-100 on the Cisco 7304 Router: Example

The following is sample output from the **show diag** *slot-number* version of the command for an MSC-100 located in slot number 4 on a Cisco 7304 router. Information about the MSC is followed by information for its associated SPAs:

```
Router# show diag 4
Slot 4:
        7304-MSC-100 SPA Carrier Card Line Card
        Line Card state: Active
        Insertion time: 00:08:49 ago
        Bandwidth points: 4000000
        EEPROM contents at hardware discovery:
        Hardware Revision        : 0.18
        Boot Time out            : 0000
        PCB Serial Number        : CSJ07288905
        Part Number              : 73-8789-01
        Board Revision           : A0
        Fab Version              : 02
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 0-0
        Product Number           : 7304-MSC-100
        Top Assy. Part Number    : 68-1163-04
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
              Calibration values :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 50 41 00 12 46 00 00 C1 8B 43 53 4A
          0x10: 30 37 32 38 38 39 30 35 82 49 22 55 01 42 41 30
          0x20: 02 02 03 00 81 00 00 00 00 04 00 80 00 00 00 00
```

```
            0x30: CB 94 37 33 30 34 2D 4D 53 43 2D 31 30 30 20 20
            0x40: 20 20 20 20 20 20 87 44 04 8B 04 C4 08 00 00 00
            0x50: 00 00 00 00 00 C5 08 00 00 00 00 00 00 00 00 C8
            0x60: 09 00 00 00 00 00 00 00 00 00 C7 7C F6 44 3F 30
            0x70: 00 00 00 00 00 00 00 00 00 00 00 00 02 EE FF C8
            0x80: C8 37 26 05 DC 64 28 1E 37 26 09 C4 64 32 28 32
            0x90: DD 0C E4 64 32 28 43 24 2E E0 AA 82 64 F4 24 00
            0xA0: 00 00 00 00 00 00 F0 2E FF FF FF FF FF FF FF FF
            0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
            0x1F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          FPGA information:
            Current FPGA version     : 00.23
            IOS bundled FPGA version : 00.23
          CPLD version     : 01.02

Subslot 4/1:
        Shared port adapter: SPA-4FE-7304, 4 ports
        State: ok
        Insertion time: 00:15:13 ago
        Bandwidth: 400000 kbps
        EEPROM contents:
```

NSE-100 on the Cisco 7304 Router: Example

The following example displays diagnostic information about the NSE-100 in slot 0 of a Cisco 7304 router:

```
Router# show diag 0
Slot 0/1:
        NSE Card state:Primary
        Insertion time:00:03:47 ago
C7300 NSE Mainboard EEPROM:
        Hardware Revision        :2.3
        PCB Serial Number        :CAB0532JYYT
        Part Number              :73-5198-02
        Board Revision           :A0
        Fab Version              :02
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :7300-NSE-100
        Top Assy. Part Number    :68-1002-02
        Manufacturing Test Data  :00 00 00 00 00 00 00 00
        Field Diagnostics Data   :00 00 00 00 00 00 00 00
```

```
        Calibration Data         :Minimum:0 dBmV, Maximum:0 dBmV
              Calibration values :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 02 8B 41 02 03 C1 8B 43 41 42 30 35 33
          0x10:32 4A 59 59 54 82 49 14 4E 02 42 41 30 02 02 03
          0x20:00 81 00 00 00 00 04 00 80 00 00 00 00 CB 94 37
          0x30:33 30 30 2D 4E 53 45 2D 31 30 30 20 20 20 20 20
          0x40:20 20 20 87 44 03 EA 02 C4 08 00 00 00 00 00 00
          0x50:00 00 C5 08 00 00 00 00 00 00 00 00 C8 09 00 00
          0x60:00 00 00 00 00 00 00 C7 7C F6 44 3F 30 F6 44 3F
          0x70:30 F6 44 3F 30 00 00 00 00 07 08 64 32 28 37 26
          0x80:09 C4 5A 32 28 32 DD 0C E4 5A 2D 23 43 24 13 88
          0x90:64 32 28 65 BA 2E E0 AA 82 64 F4 24 00 00 00 00
          0xA0:00 00 00 EF 1C FF FF FF FF FF FF FF FF FF FF FF
          0xB0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xC0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

C7300 NSE Daughterboard EEPROM:
        Hardware Revision        :2.0
        PCB Serial Number        :CAB0533K3PP
        Part Number              :73-5673-03
        Board Revision           :A0
        Fab Version              :03
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :7300-NSE-100
        Top Assy. Part Number    :68-1002-02
        Manufacturing Test Data  :00 00 00 00 00 00 00 00
        Field Diagnostics Data   :00 00 00 00 00 00 00 00
        Calibration Data         :Minimum:0 dBmV, Maximum:0 dBmV
              Calibration values :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 02 8C 41 02 00 C1 8B 43 41 42 30 35 33
          0x10:33 4B 33 50 50 82 49 16 29 03 42 41 30 02 03 03
          0x20:00 81 00 00 00 00 04 00 80 00 00 00 00 CB 94 37
          0x30:33 30 30 2D 4E 53 45 2D 31 30 30 20 20 20 20 20
          0x40:20 20 20 87 44 03 EA 02 C4 08 00 00 00 00 00 00
          0x50:00 00 C5 08 00 00 00 00 00 00 00 00 C8 09 00 00
          0x60:00 00 00 00 00 00 00 C7 7C F6 44 3F 30 00 00 00
          0x70:00 00 00 00 00 00 00 00 00 06 72 64 1E 1C 37 26
          0x80:07 08 64 32 28 37 26 00 00 00 00 00 00 00 00 00
          0x90:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xA0:00 00 00 FB BA FF FF FF FF FF FF FF FF FF FF FF
          0xB0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xC0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        FPGA information:
          Current NSE MB FPGA version     :0.3
          IOS bundled NSE MB FPGA version :0.12
          Current NSE DB FPGA version     :0.3
          IOS bundled NSE DB FPGA version :0.10
Fault History Buffer:
7300 Software (C7300-IS-M), Experimental Version 12.1(20011206:191841) [user-ws1 179]
Compiled Tue 29-Jan-02 08:10 by
```

```
Signal = 22, Code = 0x0, Uptime 00:00:48
$0 :FFFFFFFF, AT :47001098, v0 :10020028, v1 :0000006F
a0 :A0000000, a1 :00000005, a2 :00000001, a3 :10020028
t0 :00000028, t1 :3401E101, t2 :34018100, t3 :FFFF00FF
t4 :40332E68, t5 :43204650, t6 :70646174, t7 :69707065
s0 :FFFFFFFF, s1 :FFFFFFFF, s2 :FFFFFFFF, s3 :FFFFFFFF
s4 :FFFFFFFF, s5 :FFFFFFFF, s6 :FFFFFFFF, s7 :FFFFFFFF
t8 :00000000, t9 :00000000, k0 :3041D001, k1 :30410000
gp :FFFFFFFF, sp :41AA8F20, s8 :FFFFFFFF, ra :4036B6A4
EPC :4036B69C, SREG :3401E103, Cause :FFFFFFFF
Error EPC :FFFFFFFF, BadVaddr :FFFFFFFF


ROMMON Last Error Info:
count:19,  reason:reset
pc:0x4020BFBC,  error address:0x00000000
Stack Trace:
FP:0x00000000, PC:0x00000000
FP:0x00000000, PC:0x00000000
```

Shared Port Adapters on the Cisco 7304 Router: Example

The following is sample output from the **show diag subslot** command for a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show diag subslot 4/1

Subslot 4/1:
        Shared port adapter: SPA-4FE-7304, 4 ports
        Info: hw-ver=0x100, sw-ver=0x0 fpga-ver=0x0
        State: ok
        Insertion time: 23:20:42 ago
        Bandwidth: 400000 kbps
        EEPROM contents:
        Hardware Revision        : 1.0
        Boot Time out            : 0190
        PCB Serial Number        : JAB073204G5
        Part Number              : 73-8717-03
        73/68 Level Revision     : 01
        Fab Version              : 02
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 0
        Product Number           : SPA-4FE-7304
        Product Version Id       : V01
        Top Assy. Part Number    : 68-2181-01
        73/68 Level Revision     : A0
        CLEI Code                : CNS9420AAA
        Base MAC Address         : 0000.0000.0000
        MAC Address block size   : 1024
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
```

```
                            00 00 00 00 00 00 00 00
                            00 00 00 00
Calibration Data          : Minimum: 0 dBmV, Maximum: 0 dBmV
      Calibration values :
Power Consumption         : 160000mW max
                  Mode 1 : 0mW
                  Mode 2 : 0mW
                  Mode 3 : 0mW
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 04 35 41 01 00 46 01 90 C1 8B 4A 41 42
  0x10: 30 37 33 32 30 34 47 35 82 49 22 0D 03 8A 30 31
  0x20: 20 20 02 02 03 00 81 00 00 00 00 04 00 88 00 00
  0x30: 00 00 CB 94 53 50 41 2D 34 46 45 2D 37 33 30 34
  0x40: 20 20 20 20 20 20 20 20 89 56 30 31 20 87 44 08
  0x50: 85 01 8A 41 30 20 20 C6 8A 43 4E 53 39 34 32 30
  0x60: 41 41 41 CF 06 00 00 00 00 00 43 04 00 C4 08
  0x70: 00 00 00 00 00 00 00 00 C5 08 00 00 00 00 00 00
  0x80: 00 00 F4 00 64 00 00 00 00 00 00 00 00 00 00 00
  0x90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xD0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xE0: 00 00 00 00 00 00 00 00 00 C8 09 00 00 00 00 00
  0xF0: 00 00 00 00 D7 08 3E 80 00 00 00 00 00 00 F3 00
  0x100: 41 01 08 F6 48 43 34 F6 49 44 35 02 31 04 B0 B4
  0x110: A0 8C 00 00 05 DC 64 46 32 00 00 07 08 64 46 32
  0x120: 00 00 09 C4 64 46 32 00 00 0C E4 64 46 32 00 00
  0x130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE 02
  0x140: F2 A6 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x150: CC A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x170: 00 00 D4 A0 00 00 00 00 00 00 00 00 00 00 00 00
  0x180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FPGA version:
  Software version : 04.17
  Hardware version : 04.17
```

The following is sample output from the **show diag subslot** command for 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 diag subslot 4/0

Subslot 4/0:
        Shared port adapter: SPA-2GE-7304, 2 ports
        Info: hw-ver=0x17, sw-ver=0x0 fpga-ver=0x0
        State: ok
        Insertion time: 00:08:47 ago
        Bandwidth: 2000000 kbps
        EEPROM contents:
        Hardware Revision        : 0.23
        Boot Time out            : 0190
        PCB Serial Number        : JAB073406YH
        Part Number              : 73-8792-02
        73/68 Level Revision     : 01
        Fab Version              : 02
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 0
        Product Number           : SPA-2GE-7304
        Product Version Id       : V01
        Top Assy. Part Number    : 68-2181-01
        73/68 Level Revision     : A0
        CLEI Code                : CNS9420AAA
        Base MAC Address         : 0000.0000.0000
        MAC Address block size   : 1024
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
              Calibration values :
        Power Consumption        : 160000mW max
                         Mode 1 : 0mW
                         Mode 2 : 0mW
                         Mode 3 : 0mW
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 36 41 00 17 46 01 90 C1 8B 4A 41 42
          0x10: 30 37 33 34 30 36 59 48 82 49 22 58 02 8A 30 31
          0x20: 20 20 02 02 03 00 81 00 00 00 00 04 00 88 00 00
          0x30: 00 00 CB 94 53 50 41 2D 32 47 45 2D 37 33 30 34
          0x40: 20 20 20 20 20 20 20 20 89 56 30 31 20 87 44 08
          0x50: 85 01 8A 41 30 20 20 C6 8A 43 4E 53 39 34 32 30
          0x60: 41 41 41 CF 06 00 00 00 00 00 00 43 04 00 C4 08
          0x70: 00 00 00 00 00 00 00 00 C5 08 00 00 00 00 00 00
          0x80: 00 00 F4 00 64 00 00 00 00 00 00 00 00 00 00 00
          0x90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0xC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xD0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xE0: 00 00 00 00 00 00 00 00 00 C8 09 00 00 00 00 00
  0xF0: 00 00 00 00 D7 08 3E 80 00 00 00 00 00 00 F3 00
  0x100: 41 01 08 F6 48 43 34 F6 49 44 35 02 31 03 E8 B4
  0x110: A0 8C 37 26 05 DC 64 46 32 37 26 07 08 64 46 32
  0x120: 37 26 09 C4 64 46 32 32 DD 0C E4 64 46 32 43 24
  0x130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE 02
  0x140: EF E2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x150: CC A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x170: 00 00 D4 A0 00 00 00 00 00 00 00 00 00 00 00 00
  0x180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FPGA version:
  Software version : 04.17
  Hardware version : 04.17
```

Shared Port Adapter on a Cisco 12000 Series Router: Example

The following is sample output from the **show diag subslot** command for the 1-Port OC-192c/STM-64c POS/RPR XFP SPA in subslot 1 of the SIP located in chassis slot 1 on a Cisco 12000 series router:

```
Router# show diag subslot 1/1

SUBSLOT  1/1 (SPA-OC192POS-XFP): 1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter
       Product Identifier (PID) : SPA-OC192POS-XFP
       Version Identifier (VID) : V01
       PCB Serial Number        : PRTA1304061
       Top Assy. Part Number    : 68-2190-01
       Top Assy. Revision       : A0
       Hardware Revision        : 2.0
       CLEI Code                : UNASSIGNED
       Insertion Time           : 00:00:10 (13:14:17 ago)
       Operational Status       : ok
```

Table 12 describes the significant fields shown in the display.

Table 12 show diag subslot Field Descriptions

Field	Description
Product Identifier (PID)	Product number of the SPA.
Version Identifier (VID)	Version number of the SPA.
PCB Serial Number	Serial number of the printed circuit board.
Top Assy. Part Number	Part number of the SPA.
Top Assy. Revision	Revision number (signifying a minor revision) of the SPA.
Hardware Revision	Revision number (signifying a minor revision) of the SPA hardware.
CLEI Code	Common Language Equipment Identification number.

Table 12 show diag subslot Field Descriptions (continued)

Field	Description
Insertion Time	Time when the SPA was installed, and elapsed time between that insertion time and the current time.
Operational Status	Current status of the SPA. For more information about the status field descriptions, refer to the **show hw-module subslot oir** command.

The following is sample output from the **show diag subslot details** command for the 1-Port OC-192c/STM-64c POS/RPR XFP SPA in subslot 1 of the SIP located in chassis slot 1 on a Cisco 12000 series router:

```
Router# show diag subslot 1/1 details

SUBSLOT  1/1 (SPA-OC192POS-XFP): 1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter
       EEPROM version           : 4
       Compatible Type          : 0xFF
       Controller Type          : 1100
       Hardware Revision        : 2.0
       Boot Timeout             : 400 msecs
       PCB Serial Number        : PRTA1304061
       PCB Part Number          : 73-8546-01
       PCB Revision             : A0        Fab Version              : 01
       RMA Test History         : 00
       RMA Number               : 0-0-0-0
       RMA History              : 00
       Deviation Number         : 0
       Product Identifier (PID) : SPA-OC192POS-XFP
       Version Identifier (VID) : V01
       Top Assy. Part Number    : 68-2190-01
       Top Assy. Revision       : A0        IDPROM Format Revision   : 36
       System Clock Frequency   : 00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00
       CLEI Code                : UNASSIGNED
       Base MAC Address         : 00 00 00 00 00 00
       MAC Address block size   : 0
       Manufacturing Test Data  : 00 00 00 00 00 00 00 00
       Field Diagnostics Data   : 00 00 00 00 00 00 00 00
       Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
             Calibration values :
       Power Consumption        : 11000 mWatts (Maximum)
       Environment Monitor Data : 03 30 04 B0 46 32 07 08
                                  46 32 09 C4 46 32 0C E4
                                  46 32 13 88 46 32 07 08
                                  46 32 EB B0 50 3C 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 FE 02 F6 AC
       Processor Label          : 00 00 00 00 00 00 00
       Platform features        : 00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00
       Asset ID                 :
       Asset Alias              :
       Insertion Time           : 00:00:10 (13:14:24 ago)
       Operational Status       : ok
```

SPA Interface Processor on a Cisco 12000 Series Router: Example

The following is sample output from the **show diag** command for a SIP located in chassis slot 2 on a Cisco 12000 series router:

```
Router# show diag 2

SLOT 2  (RP/LC 2 ): Modular 10G SPA Interface Card
  MAIN: type 149,  800-26270-01 rev 84
        Deviation: 0
        HW config: 0x00    SW key: 00-00-00
  PCA:  73-9607-01 rev 91 ver 1
        Design Release 1.0  S/N SAD08460678
  MBUS: Embedded Agent
        Test hist: 0x00    RMA#: 00-00-00    RMA hist: 0x00
  DIAG: Test count: 0x00000000    Test results: 0x00000000
  FRU:  Linecard/Module: 12000-SIP-650
  FRU:  Linecard/Module: 12000-SIP-650
        Processor Memory: MEM-LC5-1024=(Non-Replaceable)
        Packet Memory: MEM-LC5-PKT-256=(Non-Replaceable)
  L3 Engine: 5 - ISE OC192 (10 Gbps)
  MBUS Agent Software version 1.114 (RAM) (ROM version is 3.4)
  ROM Monitor version 255.255
  Fabric Downloader version used 3.7 (ROM version is 255.255)
  Primary clock is CSC 1
  Board is analyzed
  Board State is Line Card Enabled (IOS  RUN )
  Insertion time: 1d00h (2d08h ago)
  Processor Memory size: 1073741824 bytes
  TX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes
  RX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes
  0 crashes since restart

  SPA Information:
        subslot 2/0: SPA-OC192POS-XFP (0x44C), status is ok
        subslot 2/1: Empty
        subslot 2/2: Empty
        subslot 2/3: Empty
```

ADSL HWICs: Example

The following is sample output from the **show diag** command for a Cisco 2811 router with HWIC-1ADSL installed in slot 1 and HWIC-1ADSLI installed in slot 2. Each HWIC has a daughtercard as part of its assembly. The command results below give the output from the HWIC followed by the output from its daughtercard.

```
Router# show diag 0

Slot 0:
C2811 Motherboard with 2FE and integrated VPN Port adapter, 2 ports
        Port adapter is analyzed
        Port adapter insertion time unknown
        Onboard VPN              : v2.2.0
        EEPROM contents at hardware discovery:
        PCB Serial Number        : FOC09052HHA
        Hardware Revision        : 2.0
        Top Assy. Part Number    : 800-21849-02
        Board Revision           : B0
        Deviation Number         : 0
        Fab Version              : 06
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Processor type           : 87
```

```
        Hardware date code       : 20050205
        Chassis Serial Number    : FTX0908A0B0
        Chassis MAC Address      : 0013.1ac2.2848
        MAC Address block size   : 24
        CLEI Code                : CNMJ7N0BRA
        Product (FRU) Number     : CISCO2811
        Part Number              : 73-7214-09
        Version Identifier       :   NA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 46 4F 43 30 39 30 35 32 48 48 41 40
          0x10: 03 E7 41 02 00 C0 46 03 20 00 55 59 02 42 42 30
          0x20: 88 00 00 00 00 02 06 03 00 81 00 00 00 00 04 00
          0x30: 09 87 83 01 31 F1 1D C2 8B 46 54 58 30 39 30 38
          0x40: 41 30 42 30 C3 06 00 13 1A C2 28 48 43 00 18 C6
          0x50: 8A 43 4E 4D 4A 37 4E 30 42 52 41 CB 8F 43 49 53
          0x60: 43 4F 32 38 31 31 20 20 20 20 20 20 82 49 1C 2E
          0x70: 09 89 20 20 4E 41 D9 02 40 C1 FF FF FF FF FF FF

WIC Slot 1:
        ADSL over POTS
        Hardware Revision        : 7.0
        Top Assy. Part Number    : 800-26247-01
        Board Revision           : 01
        Deviation Number         : 0
        Fab Version              : 07
        PCB Serial Number        : FHH093600D4
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : HWIC-1ADSL
        Version Identifier       : V01
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 C8 41 07 00 C0 46 03 20 00 66 87 01
          0x10: 42 30 31 88 00 00 00 00 02 07 C1 8B 46 48 48 30
          0x20: 39 33 36 30 30 44 34 03 00 81 00 00 00 00 04 00
          0x30: CB 94 48 57 49 43 2D 31 41 44 53 4C 20 20 20 20
          0x40: 20 20 20 20 20 20 89 56 30 31 20 D9 02 40 C1 C6
          0x50: 8A FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        EM Slot 0:
        ADSL over POTS non-removable daughtercard
        Hardware Revision        : 5.0
        Part Number              : 73-9307-05
        Board Revision           : 03
        Deviation Number         : 0
        Fab Version              : 05
        PCB Serial Number        : FHH0936006E
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Fab Part Number          : 28-6607-05
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Connector Type           : 01
        Version Identifier       : V01
        Product (FRU) Number     :
        EEPROM format version 4
```

```
        EEPROM contents (hex):
          0x00: 04 FF 40 04 7A 41 05 00 82 49 24 5B 05 42 30 33
          0x10: 88 00 00 00 00 02 05 C1 8B 46 48 48 30 39 33 36
          0x20: 30 30 36 45 03 00 81 00 00 00 00 04 00 85 1C 19
          0x30: CF 05 C4 08 00 00 00 00 00 00 00 00 C5 08 00 00
          0x40: 00 00 00 00 00 00 05 01 89 56 30 31 20 FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

WIC Slot 2:
        ADSL over ISDN
        Hardware Revision        : 7.0
        Top Assy. Part Number    : 800-26248-01
        Board Revision           : 01
        Deviation Number         : 0
        Fab Version              : 07
        PCB Serial Number        : FHH093600DA
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : HWIC-1ADSLI
        Version Identifier       : V01
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 C9 41 07 00 C0 46 03 20 00 66 88 01
          0x10: 42 30 31 88 00 00 00 00 02 07 C1 8B 46 48 48 30
          0x20: 39 33 36 30 30 44 41 03 00 81 00 00 00 00 04 00
          0x30: CB 94 48 57 49 43 2D 31 41 44 53 4C 49 20 20 20
          0x40: 20 20 20 20 20 20 89 56 30 31 20 D9 02 40 C1 C6
          0x50: 8A FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        EM Slot 0:
        ADSL over ISDN non-removable daughtercard
        Hardware Revision        : 5.0
        Part Number              : 73-9308-05
        Board Revision           : 03
        Deviation Number         : 0
        Fab Version              : 05
        PCB Serial Number        : FHH0936008M
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Fab Part Number          : 28-6607-05
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Connector Type           : 01
        Version Identifier       : V01
        Product (FRU) Number     :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 7B 41 05 00 82 49 24 5C 05 42 30 33
          0x10: 88 00 00 00 00 02 05 C1 8B 46 48 48 30 39 33 36
          0x20: 30 30 38 4D 03 00 81 00 00 00 00 04 00 85 1C 19
          0x30: CF 05 C4 08 00 00 00 00 00 00 00 00 C5 08 00 00
          0x40: 00 00 00 00 00 00 05 01 89 56 30 31 20 FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

NME-AON-K9= Installed in a Cisco 3845: Example

The following is sample output of the **show diag** command for an integrated-service-engine port adapter in slot 2 on a Cisco 3845 router:

```
Slot 2:
        Integrated Service Engine Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time unknown
        EEPROM contents at hardware discovery:
        Hardware Revision        : 1.0
        Top Assy. Part Number    : 800-28152-01
        Board Revision           : 03
        Deviation Number         : 0
        Fab Version              : 01
        PCB Serial Number        : FOC101430NK
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Version Identifier       : NA
        CLEI Code                : TDB
        Product (FRU) Number     : NME-AON-K9
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 05 5B 41 01 00 C0 46 03 20 00 6D F8 01
          0x10: 42 30 33 88 00 00 00 00 02 01 C1 8B 46 4F 43 31
          0x20: 30 31 34 33 30 4E 4B 03 00 81 00 00 00 00 04 00
          0x30: 89 4E 41 00 00 D9 02 40 C1 C6 8A 54 44 42 00 00
          0x40: 00 00 00 00 00 CB 88 4E 4D 45 2D 52 56 50 4E FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Table 13 describes the significant fields shown in the display.

Table 13 show diag subslot Field Descriptions

Field	Description
Hardware Revision	Revision number (signifying a minor revision) of the SPA hardware.
Top Assy. Part Number	Part number of the SPA.
Product Identifier (PID)	Product number of the SPA.
Board Revision	Revision number of the circuit board in the module.
Deviation Number	Deviation number of the module.
Fab Version	Fabrication version of the module.
PCB Serial Number	Serial number of the printed circuit board.
Top Assy. Revision	Revision number (signifying a minor revision) of the SPA.
RMA Test History	History of RMA testing.
RMA Number	RMA number of the module.
RMA History	History of RMA on this module.
Version Identifier	Non-applicable to this module.
CLEI Code	Common Language Equipment Identification number. (non-applicable on this module)
Product (FRU) Number	Product identification number.

Table 13 show diag subslot Field Descriptions (continued)

Field	Description
EEPROM Format Version	Version of EEPROM format.
EEPROM Contents	Contents of EEPROM output.

Related Commands

Command	Description
dsl operating-mode (ADSL)	Modifies the operating mode of the digital subscriber line for an ATM interface.
show c7300	Displays the types of hardware (processors, line cards, jacket cards, and so on) installed in the Cisco 7304 router slots, including the bundled Flash, and current FPGA versions.
show c7300 errorlog	Displays error information on a Cisco 7304 router.
show dsl interface atm	Shows all of the ADSL-specific information for a specified ATM interface.
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 integrated-service-engine	Displays controller information for integrated-service-engine network modules.
show interfaces integrated-service-engine	Displays basic interface configuration information for integrated-service-engine network modules.

show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode. The resulting output varies, depending on the network for which an interface has been configured.

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

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

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

show interfaces [*type slot*/*port*] [**accounting**]

Cisco 7500 Series with Ports on VIPs

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

Cisco 7600 Series

show interfaces [*type interface-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 **async**, **bri0**, **dialer**, **ethernet**, **fastethernet**, **fddi**, **hssi**, **loopback**, **null**, **serial**, **tokenring**, and **tunnel**. For the Cisco 4500 series routers, *type* can be **atm**, **e1**, **ethernet**, **fastethernet**, **fddi**, **serial**, **t1**, and **token**. For the Cisco 7000 family, *type* can be **atm**, **e1, ethernet**, **fastethernet**, **fddi**, **serial**, **t1,** and **tokenring**. For the Cisco 7500 series *type* can also be **pos**. For the Cisco 7600 series routers, type can be **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, and **port-channel**, **atm**, and **ge-wan**. For shared port adapters, *type* can be **fastethernet**, **gigabitethernet**, **pos**, **sdcc**, **serial**, and **tengigabitethernet**, depending on the type of SPA supported on the router.
interface-number	(Optional) Port number on the selected interface.

first last	(Optional) For Cisco 2500 series routers, ISDN 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.
null *interface-number*	(Optional) Specifies the null interface; the valid value 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 SPA (for example 5/0/0:23), 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 SPA interface processor (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. • */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 SPA interface processor (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.

Defaults

No default behavior or values

Command Modes

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.

Release	Modification
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2SX release. The uplink dual-mode port information was updated.
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)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's default value was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Display Interpretation

The **show interfaces** command displays statistics for the network interfaces. 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 *interface-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 can you specify a particular interface.

Cisco 7600 Series Routers

Valid values for *interface-number* 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 CSM and the 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, while 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 Usage Guidelines

In Cisco IOS Release 12.2(33)SB, when a multilink PPP (MLPPP) interface is down/down, its default bandwidth rate is the sum of the serial interface bandwidths associated with the MLPPP 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 leads to queue length overflow. Total output drops include drops on all custom queues as well as the system queue. Fields are described with the Weighted Fair Queueing output in Table 14.

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

Table 14 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
- ARP (for IP, Frame Relay, SMDS)
- CLNS
- DEC MOP

  The routers use MOP packets to advertise their existence to Digital Equipment Corporation machines that use the MOP protocol. 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 (SDLC)
- Spanning Tree
- SR Bridge
- Transparent Bridge

Example with DWRED

The following is sample output from the **show interfaces** command when distributed weighted RED (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 ALC 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 a Synchronous Data Link Control (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 15 shows the fields relevant to all SDLC connections.

Table 15 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 16 shows other data given for each SDLC secondary interface configured to be attached to this interface.

Table 16 SDLC Field Descriptions

Field	Description
addr	Address of this secondary interface.
State	Current state of this connection. The possible values follow: • DISCONNECT—No communication is being attempted to this secondary. • CONNECT—A normal connect state exists between this router and this secondary. • DISCSENT—This router has sent a disconnect request to this secondary and is awaiting its response. • 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. • BOTHBUSY—Both sides have told each other that they are temporarily unable to receive any more information frames. • ERROR—This router has detected an error, and is waiting for a response from the secondary acknowledging this.
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 weighted RED (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 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 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 17 describes the fields shown in the display.

Table 17 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 only appears 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 17 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 or not loopback is set.
Keepalive	Indicates whether or not 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 Address Resolution Protocol (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 only applies to process-switched traffic.

Table 17 show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)

Field	Description
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 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, 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 17 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, as 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 17 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 18 describes the fields shown in the display for Gigabit Ethernet SPA interfaces.

Table 18 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 only appears 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 or not loopback is set.
Keepalive	Indicates whether or not 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 or not 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 Address Resolution Protocol (ARP) assigned and the timeout period.

Table 18 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 selective packet discard (SPD). SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it only applies 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 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).

Table 18 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
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 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 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, 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.

Table 18 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
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, as 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 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 19 describes the significant fields shown in this display.

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
```

Table 19 describes the significant fields shown in this display.

Table 19 show interfaces pos Field Descriptions—POS SPA

Field	Description
POSx/y/z 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 interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.
Scramble	Indicates whether or not 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.
(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 19 show interfaces pos 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	First-in, first-out (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 ignored count. 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 19 show interfaces pos 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, as 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 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 20 describes the significant fields shown in these displays.

Table 20 show interfaces sdcc Field Descriptions—POS SPA

Field	Description
SDCCx/y/z 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 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 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.

Table 20 show interfaces sdcc Field Descriptions—POS SPA (continued)

Field	Description
(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.
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	First-in, first-out (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 ignored count. 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.

Table 20 show interfaces sdcc Field Descriptions—POS SPA (continued)

Field	Description
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.
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, as 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.

Table 20 show interfaces sdcc Field Descriptions—POS SPA (continued)

Field	Description
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 21 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 21 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.

Table 21 show interfaces serial Field Descriptions—T3/E3 SPA (continued)

Field	Description
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 or not.
keepalive	Indicates whether keepalives are set or not.
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 ms (and less than 232 ms) ago.

Table 21 show interfaces serial Field Descriptions—T3/E3 SPA (continued)

Field	Description
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	First-in, first-out 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).
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 22 describes the fields shown in the display.

Table 22 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 only appears 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 or not loopback is set.

Table 22 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
Keepalive	Indicates whether or not 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 Address Resolution Protocol (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.
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 only applies 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 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).

Table 22 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
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.
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.

Table 22 show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA

Field	Description
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.
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, as 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 GigabitEthernet9/5

GigabitEthernet9/5 is up, line protocol is up
Hardware is C6k 1000Mb 802.3, address is 0001.64f8.3fa5 (bia 0001.64f8.3fa5)
Internet address is 172.20.20.20/24
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)
Full-duplex, 100Mb/s
Dual-mode port configured as RJ45
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, 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 1000 bits/sec, 2 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 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
300114 packets input, 27301436 bytes, 0 no buffer
Received 43458 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
15181 packets output, 1955836 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Router#
```

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
interface	Configures an interface type and enters interface configuration mode.
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 interfaces virtual-access

To display status, traffic data, and configuration information about a specified virtual access interface, use the **show interfaces virtual-access** command in privileged EXEC mode.

show interfaces virtual-access *number* [**configuration**]

Syntax Description

number	Number of the virtual access interface.
configuration	(Optional) Restricts output to configuration information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
11.3	The **configuration** keyword was added.
12.3(7)T	The output for this command was modified to indicate if the interface is a member of a multilink PPP bundle.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SB	This command was modified to no longer accept the abbreviated virtual access parameter: show interface vi2.1. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

To identify the number of the vty on which the virtual access interface was created, enter the **show users** EXEC command.

The counts of output packet bytes as reported by the L2TP access server (LAC) to the RADIUS server in the accounting record do not match those of a client. The following paragraphs describe how the accounting is done and how you can determine the correct packet byte counts.

Packet counts for client packets in the input path are as follows:

- For packets that are process-switched, virtual access input counters are incremented by the coalescing function by the PPP over Ethernet (PPPoE) payload length.
- For packets that are fast-switched, virtual access input counters are incremented by the fast-switching function by the formula:

  PPPoE payload length + PPP address&control bytes = = PPPoE payload length + 2
- For packets that are Cisco Express Forwarding (CEF)-switched, virtual access input counters are incremented by the CEF switching function by the formula:

  IP len + PPP encapbytes (4) = = PPPoE payload length + 2

Packet counts for client packets in the output path are as follows:

- For packets that are process-switched by protocols other than PPP, virtual access output counters are incremented in the upper layer protocol by the entire datagram, as follows:

  Size = PPPoE payload + PPPoE hdr (6) + Eth hdr (14) + SNAP hdr (10) + media hdr (4 for ATM)

- For packets process-switched by PPP Link Control Protocol (LCP) and Network Control Protocol (NCP), virtual access output counters are incremented by PPP, as follows:

  PPP payload size + 4 bytes of PPP hdr

- For packets that are CEF fast-switched, virtual access counters are incremented by the PPPoE payload size.

Accounting is done for PPPoE, PPPoA PTA and L2X as follows:

- For PPPoE PPP Termination Aggregation (PTA), the PPPoE payload length is counted for all input and output packets.
- For PPPoE L2X on a LAC, the PPPoE payload length is counted for all input packets. On an L2TP Network Server (LNS), the payload plus the PPP header (address + control + type) are counted.
- For PPP over ATM (PPPoA) PTA i/p packets, the payload plus the PPP address plus control bytes are counted. For PPPoA PTA o/p packets, the payload plus PPP address plus control plus ATM header are counted.
- For PPPoA L2X on a LAC for i/p packets, the payload plus PPP addr plus cntl bytes are counted. For PPPoA L2X on a LNS, the payload plus PPP header (address + control + type) are counted.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual access interface (VAI) as **vi***X.Y* in the **show pxf cpu queue** and **show interfaces** commands. Instead, you must spell out the VAI as **virtual-access**.

For example, when you enter the following commands, the router accepts the commands:

```
Router# show pxf cpu queue virtual-access2.1

Router# show interface virtual-access 2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following commands:

```
Router# show pxf cpu queue vi2.1

Router# show interface vi2.1
```

Examples

The following is sample output from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 3

Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 149760 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Link is a member of Multilink bundle Virtual-Access4
  PPPoATM vaccess, cloned from Virtual-Template1
  Vaccess status 0x44
  Bound to ATM4/0.10000 VCD:16, VPI:15, VCI:200, loopback not set
  DTR is pulsed for 5 seconds on reset
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:57:37
  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
```

```
676 packets input, 12168 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
676 packets output, 10140 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Table 23 describes the significant fields shown in the display.

Table 23 show interfaces virtual-access Field Descriptions

Field	Description
Virtual-Access ... is {up | down | administratively down}	Indicates whether the interface is currently active (whether carrier detect is present), is inactive, or has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line to be usable (that is, whether keepalives are successful).
Hardware is	Type of interface. In this case, the interface is a dynamically created virtual access interface that exists on a vty line.
Internet address | interface is unnumbered	IP address or IP unnumbered for the line. If unnumbered, the output lists the interface and IP address to which the line is assigned (Ethernet0 at 10.0.21.14 in this example).
MTU	Maximum transmission unit for packets on the virtual access interface.
BW	Bandwidth of the virtual access interface, in kbps.
DLY	Delay of the virtual access interface, in microseconds.
reliability	Reliability of the virtual access interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over five minutes.
load	Load on the virtual access interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the virtual access interface.
loopback	Test in which signals are sent and then directed back toward the source at some point along the communication path. Used to test network interface usability.
keepalive	Interval set for keepalive packets on the interface. If keepalives have not been enabled, the message is “keepalive not set.”
DTR	Data terminal ready. An RS232-C circuit that is activated to let the DCE know when the DTE is ready to send and receive data.

Table 23 show interfaces virtual-access Field Descriptions (continued)

Field	Description
LCP open | closed | req sent	Link Control Protocol (for PPP only; not for SLIP). LCP must come to the open state before any useful traffic can cross the link.
Open IPCP | IPXCP | ATCP	IPCP is the IP control protocol for PPP, IPXCP is the IPX control protocol for PPP, and ATCP is the AppleTalk control protocol for PPP. The network control protocol (NCP) is negotiated after the LCP opens. The NCP must come into the open state before useful traffic can cross the link.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by a virtual access interface. This value indicates when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by a virtual access interface.
output hang	Number of hours, minutes, and seconds (or never) since the virtual access 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 displayed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) 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. Asterisks (***) indicate that the elapsed time is too large to be displayed. Zeros (0:00:00) indicate that the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue, drops	Number of packets in input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped on account of a full queue.
Queueing strategy	Type of queueing selected to prioritize network traffic. The options are first-come-first-served (FCFS) queueing, weighted fair queueing, priority queueing, and custom queueing.
Output queue	Number of packets in output queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped on account of a full queue.
Conversations	Number of weighted fair queueing conversations.

Table 23 show interfaces virtual-access Field Descriptions (continued)

Field	Description
Reserved Conversations	Number of reserved weighted fair queueing conversations. The example shows the number of allocated conversations divided by the number of maximum allocated conversations. In this case, there have been 0 reserved conversations.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last five minutes.
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.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. 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 virtual access interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no-buffer, runts, giants, cyclic redundancy checks (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	Counter that reflects when the cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from data received. On a LAN, this often indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs often 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.

Table 23 show interfaces virtual-access Field Descriptions (continued)

Field	Description
ignored	Number of received packets ignored by the virtual access interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned in the description of the no buffer field. Broadcast storms and bursts of noise can cause the "ignored" count to be incremented.
abort	Illegal sequence of one bits on a virtual access interface. This usually indicates a clocking problem between the virtual access interface and the data link equipment.
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 far-end transmitter has been running faster than the near-end communication server's receiver can handle. Underruns may never be reported on some virtual access interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the virtual access interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams might have more than one error, and others might have errors that do not fall into any of the tabulated categories.
collisions	Number of packets colliding.
interface resets	Number of times a virtual access interface has been completely reset. A reset can happen if packets queued for transmission were not sent within several seconds. Resetting can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a virtual access 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 a virtual access interface is looped back or shut down.
output buffer failures	Number of outgoing packets dropped from the output buffer.
output buffers swapped out	Number of times that the output buffer was swapped out.
carrier transitions	Number of times that the carrier detect (CD) signal of a virtual access interface has changed state. Indicates modem or line problems if the CD line changes state often. If data carrier detect (DCD) goes down and comes up, the carrier transition counter increments two times.

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **show policy-map** command in user EXEC or privileged EXEC mode.

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.

Command Default

All existing policy map configurations are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was incorporated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was incorporated into Cisco IOS Release 12.1(1)E.
12.2(4)T	This command was modified for two-rate traffic policing to display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature.
12.2(13)T	The following modifications were made: • The output was modified for the Percentage-Based Policing and Shaping feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes can now be configured to discard packets belonging to a specified class. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.
12.0(28)S	The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms).
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.
12.2(31)SB2	This command was enhanced to display bandwidth-remaining ratios configured on traffic classes and ATM overhead accounting, and was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	Support for the Cisco 7600 series router was added.
12.4(15)T2	This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. **Note** For this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only*.
12.2(33)SB	This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added. This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE 2.1	This command integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.

Usage Guidelines

The **show policy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface. The command displays:

- ECN marking information only if ECN is enabled on the interface.
- Bandwidth-remaining ratio configuration and statistical information, if configured and used to determine the amount of unused (excess) bandwidth to allocate to a class queue during periods of congestion.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the output of the **show policy-map** command is slightly different from previous releases when the policy is an hierarchical policy.

For example, in Cisco IOS Release 12.2(33)SB output similar to the following displays when you specify a hierarchical policy in the **show policy-map** command:

```
Router# show policy-map Bronze
policy-map bronze
 class class-default
   shape average 34386000
   service-policy Child
```

In Cisco IOS Release 12.2(31)SB, output similar to the following displays when you specify a hierarchical policy in the **show policy-map** command:

```
Router# show policy-map Gold
policy-map Gold
 Class class-default
   Average Rate Traffic Shaping
   cir 34386000 (bps)
   service-policy Child2
```

In Cisco IOS Release 12.2(33)SB, the output from the **show policy-map** command displays police actions on separate lines as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P1
  priority
  police percent 50 25 ms 0 ms
   conform-action transmit
   exceed-action transmit
   violate-action drop
```

In Cisco IOS Release 12.2(31)SB, the output from the **show policy-map** command displays police actions on one line as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P2
  priority
  police percent 50 25 ms 0 ms conform-action transmit exceed-action transmit violate-
action drop
```

Examples

This section provides sample output from typical **show policy-map** commands. Depending upon the interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly from the ones shown below.

- Weighted Fair Queueing: Example, page 152
- Frame Relay Voice-Adaptive Traffic-Shaping: Example, page 154
- Traffic Policing: Example, page 155
- Two-Rate Traffic Policing: Example, page 155
- Multiple Traffic Policing Actions: Example, page 156
- Explicit Congestion Notification: Example, page 157
- Modular QoS CLI (MQC) Unconditional Packet Discard: Example, page 158
- Percentage-Based Policing and Shaping: Example, page 158
- Enhanced Packet Marking: Example, page 160
- Bandwidth-Remaining Ratio: Example, page 160
- ATM Overhead Accounting: Example, page 161
- Tunnel Marking: Example, page 161

Weighted Fair Queueing: Example

The following example displays the contents of the service policy map called po1. In this example, WFQ is enabled.

```
Router# show policy-map po1

Policy Map po1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

```
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router. Again, WFQ is enabled.

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

Table 24 describes the significant fields shown in the display.

Table 24 show policy-map Field Descriptions—Configured for WFQ

Field	Description
Policy Map	Policy map name.
Class	Class name.
Bandwidth	Amount of bandwidth in kbps allocated to class.
Max thresh	Maximum threshold in number of packets.

Frame Relay Voice-Adaptive Traffic-Shaping: Example

The following sample output for the **show-policy map** command indicates that Frame Relay voice-adaptive traffic-shaping is configured in the class-default class in the policy map "MQC-SHAPE-LLQ1" and that the deactivation timer is set to 30 seconds.

```
Router# show policy-map

  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)

  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

Table 25 describes the significant fields shown in the display.

Table 25 show policy-map Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic-Shaping

Field	Description
Strict Priority	Indicates the queueing priority assigned to the traffic in this class.
Burst	Specifies the traffic burst size in bytes.
Traffic Shaping	Indicates that Traffic Shaping is enabled.
Average Rate Traffic Shaping	Indicates the type of Traffic Shaping enabled. Choices are Peak Rate Traffic Shaping or Average Rate Traffic Shaping.
CIR	Committed Information Rate (CIR) in bps.
Max. Buffers Limit	Maximum memory buffer size in packets.

Table 25 show policy-map Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic-Shaping (continued)

Field	Description
Adapt to	Traffic rate when shaping is active.
Voice Adapt Deactivation Timer	Indicates that Frame Relay voice-adaptive traffic-shaping is configured, and that the deactivation timer is set to 30 seconds.
service-policy	Name of the service policy configured in the policy map "MQC-SHAPE-LLQ1".

Traffic Policing: Example

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy1." In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1

  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

Table 26 describes the significant fields shown in the display.

Table 26 show policy-map Field Descriptions—Configured for Traffic Policing

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of the class configured in the policy map displayed.
police	Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (Bc) and excess burst (Be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified.

Two-Rate Traffic Policing: Example

The following is sample output from the **show policy-map** command when two-rate traffic policing has been configured. As shown below, two-rate traffic policing has been configured for a class called "police." In turn, the class called police has been configured in a policy map called "policy1." Two-rate traffic policing has been configured to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following sample output shows the contents of the policy map called “policy1”:

```
Router# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
   transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

Table 27 describes the significant fields shown in the display.

Table 27 show policy-map Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (bc), peak information rate (PIR), and peak burst (BE) size used for marking packets.
conform-action	Displays the action to be taken on packets conforming to a specified rate.
exceed-action	Displays the action to be taken on packets exceeding a specified rate.
violate-action	Displays the action to be taken on packets violating a specified rate.

Multiple Traffic Policing Actions: Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The following sample output from the **show policy-map** command displays the configuration for a service policy called “police.” In this service policy, traffic policing has been configured to allow multiple actions for packets marked as conforming to, exceeding, or violating the CIR or the PIR shown in the example.

```
Router# show policy-map police

  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit

       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

Packets conforming to the specified CIR (1000000 bps) are marked as conforming packets. These are transmitted unaltered.

Packets exceeding the specified CIR (but not the specified PIR, 2000000 bps) are marked as exceeding packets. For these packets, the IP Precedence level is set to 4, the discard eligibility (DE) bit is set to 1, and the packet is transmitted.

Packets exceeding the specified PIR are marked as violating packets. For these packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

Note Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

Table 28 describes the significant fields shown in the display.

Table 28 show policy-map Field Descriptions—Configured for Multiple Traffic Policing Actions

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, BC, PIR, and BE used for marking packets.
conform-action	Displays the one or more actions to be taken on packets conforming to a specified rate.
exceed-action	Displays the one or more actions to be taken on packets exceeding a specified rate.
violate-action	Displays the one or more actions to be taken on packets violating a specified rate.

Explicit Congestion Notification: Example

The following is sample output from the **show policy-map** command when the WRED—Explicit Congestion Notification (ECN) feature has been configured. The words "explicit congestion notification" (along with the ECN marking information) included in the output indicate that ECN has been enabled.

```
Router# show policy-map

   Policy Map pol1
     Class class-default
       Weighted Fair Queueing
             Bandwidth 70 (%)
             exponential weight 9
             explicit congestion notification
             class    min-threshold    max-threshold    mark-probability
             ------------------------------------------------------------
             ------------------------------------------------------------

             0        -                -                1/10
             1        -                -                1/10
             2        -                -                1/10
             3        -                -                1/10
             4        -                -                1/10
             5        -                -                1/10
             6        -                -                1/10
             7        -                -                1/10
             rsvp     -                -                1/10
```

Table 29 describes the significant fields shown in the display.

Table 29 show policy-map Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
class	IP precedence value.
min-threshold	Minimum threshold. Minimum WRED threshold in number of packets.
max-threshold	Maximum threshold. Maximum WRED threshold in number of packets.
mark-probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.

Modular QoS CLI (MQC) Unconditional Packet Discard: Example

The following example displays the contents of the policy map called "policy1." All the packets belonging to the class called "c1" are discarded.

```
Router# show policy-map policy1

 Policy Map policy1
  Class c1
   drop
```

Table 30 describes the significant fields shown in the display.

Table 30 show policy-map Field Descriptions—Configured for MQC Unconditional Packet Discard

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

Percentage-Based Policing and Shaping: Example

The following example displays the contents of two service policy maps—one called "policy1" and one called "policy2." In policy1, traffic policing based on a CIR of 50 percent has been configured. In policy 2, traffic shaping based on an average rate of 35 percent has been configured.

```
Router# show policy-map policy1

Policy Map policy1
 class class1
    police cir percent 50

Router# show policy-map policy2

Policy Map policy2
 class class2
    shape average percent 35
```

The following example displays the contents of the service policy map called “po1”:

```
Router# show policy-map po1

Policy Map po1
 Weighted Fair Queueing
    Class class1
Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router:

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

Table 31 describes the significant fields shown in the display.

Table 31 show policy-map Field Descriptions—Configured for Percentage-Based Policing and Shaping

Field	Description
Policy Map	Name of policy map displayed.
Weighted Fair Queueing	Indicates that weighted fair queueing (WFQ) has been enabled.
Class	Name of class configured in policy map displayed.
Bandwidth	Bandwidth, in kbps, configured for this class.
Max threshold	Maximum threshold. Maximum WRED threshold in number of packets.

Enhanced Packet Marking: Example

The following sample output from the **show policy-map** command displays the configuration for policy maps called “policy1” and “policy2”.

In “policy1”, a table map called “table-map-cos1” has been configured to determine the precedence based on the class of service (CoS) value. Policy map “policy 1” converts and propagates the packet markings defined in the table map called “table-map-cos1”.

The following sample output from the **show policy-map** command displays the configuration for service polices called “policy1” and “policy2”. In “policy1”, a table map called “table-map1” has been configured to determine the precedence according to the CoS value. In “policy2”, a table map called “table-map2” has been configured to determine the CoS value according to the precedence value.

```
Router# show policy-map policy1

  Policy Map policy1
    Class class-default
      set precedence cos table table-map1

Router# show policy-map policy2

   Policy Map policy2
    Class class-default
      set cos precedence table table-map2
```

Table 32 describes the fields shown in the display.

Table 32 show policy-map Field Descriptions—Configured for Enhanced Packet Marking

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
set precedence cos table table-map1 or set cos precedence table table-map2	Name of the set command used to set the specified value. For instance, set precedence cos table-map1 indicates that a table map called “table-map1” has been configured to set the precedence value on the basis of the values defined in the table map. Alternately, set cos table table-map2 indicates that a table map called “table-map2” has been configured to set the CoS value on the basis of the values defined in the table map.

Bandwidth-Remaining Ratio: Example

The following sample output for the **show policy-map** command indicates that the class-default class of the policy map named vlan10_policy has a bandwidth-remaining ratio of 10. When congestion occurs, the scheduler allocates class-default traffic 10 times the unused bandwidth allocated in relation to other subinterfaces.

```
Router# show policy-map vlan10_policy

  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child_policy
```

Table 33 describes the fields shown in the display.

Table 33 show policy-map Field Descriptions—Configured for Bandwidth-Remaining Ratio

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
Average Rate Traffic Shaping	Indicates that Average Rate Traffic Shaping is configured.
cir	Committed information rate (CIR) used to shape traffic.
bandwidth remaining ratio	Indicates the ratio used to allocate excess bandwidth.

ATM Overhead Accounting: Example

The following sample output for the **show policy-map** command indicates that ATM overhead accounting is enabled for the class-default class. The BRAS-DSLAM encapsulation is dot1q and the subscriber encapsulation is snap-rbe for the AAL5 service.

```
Policy Map unit-test
    Class class-default
        Average Rate Traffic Shaping
        cir 10% account dot1q aal5 snap-rbe
```

Table 34 describes the significant fields shown in the display.

Table 34 show policy-map Field Descriptions—Configured for ATM Overhead Accounting

Field	Description
Average Rate	Committed burst (Bc) is the maximum number of bits sent out in each interval.
cir 10%	Committed information rate (CIR) is 10 percent of the available interface bandwidth.
dot1q	BRAS-DSLAM encapsulation is 802.1Q VLAN.
aal5	DSLAM-CPE encapsulation type is based on the ATM Adaptation Layer 5 service. AAL5 supports connection-oriented variable bit rate (VBR) services.
snap-rbe	Subscriber encapsulation type.

Tunnel Marking: Example

In this sample output of the **show policy-map** command, the character string “ip precedence tunnel 4” indicates that tunnel marking (either L2TPv3 or GRE) has been configured to set the IP precedence value to 4 in the header of a tunneled packet.

Note As of Cisco IOS Release 12.4(15)T2, GRE-tunnel marking is supported on the RPM-XF platform *only*.

```
Router# show policy-map

Policy Map TUNNEL_MARKING
    Class MATCH_FRDE
      set ip precedence tunnel 4
```

Table 35 describes the fields shown in the display.

Table 35 show policy-map Field Descriptions—Configured for Tunnel Marking

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
set ip precedence tunnel	Indicates that tunnel marking has been configured.

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class (policy map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class–map	Creates a class map to be used for matching packets to a specified class.
drop	Configures a traffic class to discard packets belonging to a specific class.
police	Configures traffic policing.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect ecn	Enables ECN.
shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
show running-config	Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show pxf cpu ipv6

To display Parallel eXpress Forwarding (PXF) IPv6 statistics, use the **show pxf cpu ipv6** command in privileged EXEC mode.

show pxf cpu ipv6 [*ipv6: address* [*prefix*] | acl-prefixes | hash | summary]

Cisco 10000 Series Router

show pxf cpu ipv6 [**acl-prefixes** | **address** | **hash** | **summary** | **table** | **vrf**]

Syntax Description

ipv6: address [*prefix*]	(Optional) Specifies the IPv6 address and optional IPv6 prefix for the information you want to display.
acl-prefixes	(Optional) Displays access control list (ACL) prefixes mapping information.
address	(Optional) Displays PXF IPv6 address-specific information.
hash	(Optional) Displays hash table summary information.
summary	(Optional) Displays a summary of the PXF IPv6 statistics.
table	(Optional) Displays detailed information about the PXF IPv6 forwarding table.
vrf	(Optional) Displays PXF IPv6 VRF information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2S	This command was introduced.
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was enhanced to provide the **address**, **table**, and **vrf** options, and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **show pxf cpu ipv6 table** command displays the global table, but does not display the leafs that correspond to the IPv6 prefixes ::1/128 (Loopback) and ::/128 (All Zero). The microcode checks for these prefixes.

The **show pxf cpu ipv6 table** command replaces the **show pxf cpu ipv6** command in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows the PXF IPv6 statistics:

```
Router# show pxf cpu ipv6

Mtrie Leaf Data: Prefix/Length

 Leaf prefix ::/0,ACL Index = 0
```

```
  Leaf elt_addr: 0x70D20001  SW_OBJ_FIB_ENTRY: 0x20A6E404 acl_index: 0
  Refcount: 514 Flags: 0x2  Parent: None
  First Covered: None
  Right Peer: None
=======================================
0 routes in Mtrie with less specific overlapping parent route


Hash Table Leaf Data: Prefix/Length

 Leaf prefix ::1/128,ACL Index = 0
  Leaf elt_addr: 0x70D20011  SW_OBJ_FIB_ENTRY: 0x0 acl_index: 0
  128-bit Table Hash Value: 0xC7F7
  Refcount: 3 Flags: 0x2  Parent: None
  First Covered: None
  Right Peer: None
 Leaf prefix ::/128,ACL Index = 0
  Leaf elt_addr: 0x70D20009  SW_OBJ_FIB_ENTRY: 0x0 acl_index: 0
  128-bit Table Hash Value: 0xC2719
  Refcount: 3 Flags: 0x2  Parent: None
  First Covered: None
  Right Peer: None
=======================================
0 routes in Hash Table with less specific overlapping parent route
```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.

show pxf cpu queue

To display parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command in privileged EXEC mode.

show pxf cpu queue [*interface* | *QID* | **summary**]

Cisco uBR10012 Universal Broadband Router

show pxf cpu queue [*interface* | *QID*]

Syntax Description

interface	(Optional) The interface for which you want to display PXF queueing statistics. This displays PXF queueing statistics for the main interface and all subinterfaces and permanent virtual circuits (PVCs). It also displays packets intentionally dropped due to queue lengths.
QID	(Optional) The queue identifier.
summary	(Optional) Displays queue scaling information such as: • Number of queues and recycled queues. • Number of available queue IDs (QIDs). • Number of packet buffers, recycled packet buffers, and free packet buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.3(23)BC1	The “Link Queues” output field for dynamic bandwidth sharing-enabled modular cable and wideband cable interfaces was added on the Cisco uBR10012 universal broadband router.
12.2(33)SB	This command was modified for virtual access interfaces (VAIs) and the output was modified for the **summary** option, and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	The output of this command has been updated or re-arranged (compared to the VTMS version) for DOCSIS Weighted Fair Queuing (WFQ) Scheduler feature and implemented on the Cisco uBR10012 router.

Usage Guidelines

When neither the interface or QID is specified, the command displays queuing statistics for the route processors (RPs).

Cisco 10000 Series Router

The Cisco 10000 series router high-speed interfaces work efficiently to spread traffic flows equally over the queues. However, using single traffic streams in a laboratory environment might result in less-than-expected performance. To ensure accurate test results, test the throughput of the Gigabit Ethernet, OC-48 POS, or ATM uplink with multiple source or destination addresses. To determine if traffic is being properly distributed, use the **show pxf cpu queue** command.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual access interface (VAI) as **vi***X.Y* in the **show pxf cpu queue** command. Instead, you must spell out the VAI as **virtual-access**.

For example, the router accepts the following command:

```
Router# show pxf cpu queue virtual-access2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following command:

```
Router# show pxf cpu queue vi2.1
```

In Cisco IOS Release 12.2(33)SB and later releases, the output from the **show pxf cpu queue** *interface* **summary** command displays only the physical interface and the number of logical links. The output does not display the number of priority queues, class queues, and so on. This modification applies to the PRE3 and PRE4.

Cisco uBR10012 Universal Broadband Router

If dynamic bandwidth sharing (DBS) is enabled, the link queue information that is displayed refers to the specific type of interface that is configured—modular cable or wideband cable. The **summary** keyword option is not supported for the Cisco uBR10012 universal broadbandrRouter for wideband cable or modular cable interfaces. The **ATM** interface output is not available for this router.

See Table 1 for descriptions of the **interface** keyword fields.

Table 36 show pxf cpu queue Interface Option Field Descriptions

Field	Description
<0-131071>	QID (queue identifier)
ATM	Asynchronous transfer mode interface **Note** The ATM interface output is not available for the Cicso uBR10012 universal broadband router.
BVI	Bridge-group virtual interface
Bundle	Cable virtual bundle interface
CTunnel	CTunnel interface
Cable	Cable modem termination service (CMTS) interface
DTI	Digital trunk interface
Dialer	Dialer interface
Ethernet	IEEE 802.3
FastEthernet	FastEthernet IEEE 802.3
GigabitEthernet	GigabitEthernet IEEE 802.3z
Group-Async	Async group interface
Loopback	Loopback interface
MFR	Multilink frame relay bundle interface

Table 36 show pxf cpu queue Interface Option Field Descriptions (continued)

Field	Description
Modular-Cable	Modular cable interface
Multilink	Multilink group interface
Null	Null interface
Port-channel	Ethernet channel of interfaces
RP	Forwarding path (FP) to route processing (RP) queues
Tunnel	Tunnel interface
Vif	Pragmatic general multicast (PGM) host interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual token ring
WB-SPA	line card to line card (LC-LC) queues
Wideband-Cable	Wideband CMTS interface

Examples

The following example shows PXF queueing statistics for an ATM interface when a QID is not specified. The sample output includes the dropped and dequeued packets for the VCs, and for classes associated with sessions that inherit queues from VCs.

```
Router# show pxf cpu queue atm 5/0/2

VCCI 2517: ATM non-aggregated VC 1/229, VCD 1, Handle 1, Rate 500 kbps

      VCCI/ClassID  ClassName      QID   Length/Max  Res  Dequeues  Drops
      0 2517/0      class-default  269   0/4096       11          3      0
      0 2517/31     pak-priority   268   0/32         11          4      0

   Queues Owned but Unused by VC (inheritable by sessions)

      ClassID       ClassName      QID   Length/Max  Res  Dequeues  Drops
            0       class-default  275   0/32         11        100      0
           31       pak-priority   268   0/32         11          4      0


VCCI 2517: ATM non-aggregated VC 1/233, VCD 4, Handle 4, Rate 50 kbps

      VCCI/ClassID  ClassName      QID   Length/Max  Res  Dequeues  Drops
      0 2517/0      class-default  269   0/4096       11          3      0
      0 2517/31     pak-priority   268   0/32         11          4      0

   Queues Owned but Unused by VC (inheritable by sessions)

      ClassID      ClassName       QID   Length/Max  Res  Dequeues  Drops
            0      class-default   274   0/32         11          0      0
           31      pak-priority    268   0/32         11          4      0


VCCI 2520: ATM non-aggregated VC 1/232, VCD 3, Handle 3, Rate 500 kbps

      VCCI/ClassID  ClassName       QID   Length/Max  Res  Dequeues  Drops
      0 2520/0      class-default   273   0/32         11          0      0
      0 2520/31     pak-priority    268   0/32         11          4      0
```

```
VCCI 2519: ATM non-aggregated VC 1/231, VCD 2, Handle 2, Rate 500 kbps

      VCCI/ClassID  ClassName       QID   Length/Max  Res  Dequeues  Drops
      0 2519/0      class-default   272   0/32         11          0      0
      0 2519/31     pak-priority    268   0/32         11          4      0
```

The following example displays PXF queuing statistics for QID 267:

```
Router# show pxf cpu queue 267

ID                                          : 267
Priority                                    : Lo
CIR (in-use/configured)                     : 0/65535
EIR (in-use/configured)                     : 0/0
MIR (in-use/configured)                     : 0/65535
Maximum Utilization configured              : no
Link                                        : 2
Flowbit (period/offset)                     : 32768/32768
Burst Size                                  : 1024 bytes
Bandwidth                                   : 133920 Kbps
Channel                                     : 0
Packet Descriptor Base                      : 0x00000100
ML Index                                    : 0
Length/Average/Alloc                        : 0/0/32
Enqueues (packets/octets)                   : 293352/9280610
Dequeues (packets/octets)                   : 293352/9280610
Drops (tail/random/max_threshold)           : 0/0/0
Drops (no_pkt_handle/buffer_low)            : 0/0
WRED (weight/avg_smaller)                   : 0/0
WRED (next qid/drop factor)                 : 0/0
WRED (min_threshold/max_threshold/scale/slope):
precedence 0                                : 0/0/0/0
precedence 1                                : 0/0/0/0
precedence 2                                : 0/0/0/0
precedence 3                                : 0/0/0/0
precedence 4                                : 0/0/0/0
precedence 5                                : 0/0/0/0
precedence 6                                : 0/0/0/0
precedence 7                                : 0/0/0/0
```

Cisco uBR10012 Universal Broadband Router

The following examples show link queue information for specific wideband cable and modular cable interfaces when dynamic bandwidth sharing is enabled.

Modular Cable Interface

```
Router(config)# interface modular-cable 1/0/0:1
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue modular-cable 1/0/0:1

Link Queues :
 QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  420   19661/19661        1/1        65535/65535      0       Inactive
```

Wideband Cable Interface

```
Router(config)# interface wideband-cable 1/0/0:0
...
Router(config-if)# cable dynamic-bw-sharing
...
Router# show pxf cpu queue wideband-cable 1/0/0:0
```

```
Link Queues :
 QID   CIR(act/conf)       EIR            MIR       RF Chan.   Status
  419   32768/32768        1/1        65535/65535      0       Inactive
  566   19661/19661        1/1        65535/65535      1       Inactive
```

The following example shows service flow queue information for modular cable interfaces.

```
Router# show pxf cpu queue modular-cable 1/2/0:0

Cable Interface Queues:

QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131147    0/255  190        0           0         1/240    0       58
131148    0/255  33820      0           0         1/10000  0       32824

Cable Service Flow Queues:

* Best Effort Queues

QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
131241    0/255  0          0           0         1/240    0       32881

* CIR Queues

QID     Len/Max  Dequeues   TailDrops   MinRt  Wt/Quantum  ShapeRt FlowId
                                        (Kbps)             (Kbps)
2049    254/255  131018     485751      99        1/1920   0       32880

* Low Latency Queues

QID     Len/Max  Dequeues   TailDrops
```

Related Commands

Command	Description
cable dynamic-bw-sharing	Enables DBS on a specific modular cable or wideband cable interface.
show pxf cable controller	Displays information about the RF channel Versatile Traffic Management System (VTMS) links and link queues.
show pxf cpu statistics queue	Displays PXF CPU queueing counters for all interfaces.

show pxf cpu statistics

To display Parallel eXpress Forwarding (PXF) CPU statistics, use the **show pxf cpu statistics** command in privileged EXEC mode.

show pxf cpu statistics [**atom** | **backwalk** | **clear** | **diversion** | **drop** [*interface* | *vcci*] | **ip** | **ipv6** | **l2tp** | **mlp** | **qos** [*interface*] | **queue** | **rx** [*vcci*] | **security** | **arp-filter** | **drl** [**cable-wan-ip** | **wan-non-ip**]]

Cisco 10000 Series Router

show pxf cpu statistics diversion [**pxf** [**interface** {*interface* | *vcci*}] | **top** *number*]

Syntax Description

atom	(Optional) Displays Any Transport over MPLS (AToM) statistics.
backwalk	(Optional) Displays backwalk requests statistics.
clear	(Optional) Clears PXF CPU statistics.
diversion	(Optional) Displays packets that the PXF diverted to the Route Processor (RP) for special handling.
drop [*interface*] [*vcci*]	(Optional) Displays packets dropped by the PXF for a particular interface or Virtual Circuit Connection Identifier (VCCI).
ip	(Optional) Displays IP statistics.
ipv6	(Optional) Displays IPv6 statistics.
l2tp	(Optional) Displays packet statistics for an L2TP Access Concentrator (LAC) (Optional) and L2TP Network Server (LNS).
mlp	(Optional) Displays multilink PPP (MLP) statistics.
pxf	(Optional) Displays packets that the PXF diverted to the Route Processor (RP). Available on the Cisco 10000 series router only.
pxf interface *interface*	(Optional) Displays per-interface PXF statistical information for the divert cause policer on a particular interface. Available on the Cisco 10000 series router only.
pxf interface *vcci*	(Optional) Displays per-VCCI PXF statistical information for the divert cause policer on a particular Virtual Circuit Connection Identifier (VCCI). Available on the Cisco 10000 series router only.
qos [*interface*]	(Optional) Displays match statistics for a service policy on an interface.
queue	(Optional) Displays queueing counters for all interfaces.
rx [*vcci*]	(Optional) Displays receive statistics for a VCCI.
security	(Optional) Displays ACL matching statistics.
top *number*	(Optional) Displays PXF statistical information for the number of top punters you specify. Available on the Cisco 10000 series router only. Valid values are from 1 to 100.
arp-filter	(Optional) Displays the ARP filter statistics.
drl	(Optional) Displays the divert rate limit.
cable-wan-ip	(Optional) Displays cable / wan-ip statistics for dropped packets.
wan-non-ip	(Optional) Displays DRL wan-non-ip statistics for dropped packets.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.2(28)SB	This command was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SB	This command was enhanced to display per-interface or per-VCCI PXF statistical information for the divert cause policer on a particular interface or VCCI, to display the top punters on an interface, and to display the provisioned burst size for any divert causes. These enhancements were implemented on the Cisco 10000 series router for the PRE2, PRE3, and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers. Support for the Cisco uBR7225VXR router was added. The **arp-filter, drl, cable-wan-ip,** and **wan-non-ip** keywords were added .

Usage Guidelines

Cisco 10000 Series Router Usage Guidelines

- The **show pxf cpu statistics diversion** command displays statistical information about diverted packets. Divert causes with the string "ipv6..." display as "v6..." in the output of all **show pxf cpu statistics diversion** commands
- The output from the **show pxf cpu statistics diversion pxf** command was enhanced in Cisco IOS Release 12.2(33)SB to display the provisioned burst size for any divert causes.
- The **show pxf cpu statistics diversion pxf interface** *interface* command displays statistical information about the divert cause policer on a specific interface. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion pxf interface** *vcci* command displays statistical information about the divert cause policer on a specific VCCI. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion top** *number* command displays the interfaces, subinterfaces, and sessions with the highest number of punter packets.

Examples The following example shows PXF queueing counters information. These are aggregate counters for all interfaces. The Total column is the total for all columns.

Note If you are troubleshooting link utilization issues, the deq_vtp_req, deq_flow_off, and deq_ocq_off counters may indicate what is causing the versatile time management scheduler (VTMS) to slow down.

If you are troubleshooting overall PXF throughput issues, look at the High Next Time, Low Next Time, High Wheel Slot, and Low Wheel Slot counters.

```
Router# show pxf cpu statistics queue

Column 6 Enqueue/Dequeue Counters by Rows:

dbg Counters         0          1          2          3          4          5          6          7
Total
=============   ========== ========== ========== ========== ========== ========== ========== ==========
==========
enq_pkt         0x0000FD9B 0x0000FC77 0x0000FE4A 0x0000FF81 0x0000FC53 0x0000FD2E 0x0000FF19 0x0000FDDE
0x0007EE55
tail_drop_pkt   0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
deq_pkt         0x0000FD47 0x0000FEF2 0x0000FCB3 0x0000FF65 0x0000FCE7 0x0000FC45 0x0000FEE7 0x0000FDF1
0x0007EE55
deq_vtp_req     0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
deq_flow_off    0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
deq_ocq_off     0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
enqdeq_conflict 0x0000003A 0x00000043 0x0000004A 0x00000039 0x0000003A 0x0000004F 0x00000036 0x00000031
0x000001F0
bndl_pkt        0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
frag_pkt        0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg_frag_drop   0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg_bndl_sem    0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
context_inhibit 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
bfifo_enq_fail  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg1            0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg2            0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg3            0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg4            0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg5            0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
dbg6            0x0000     0x0000     0x0000     0x0000     0x0000     0x0000     0x0000     0x0000
0x0000
dbg7            0x00       0x00       0x00       0x00       0x00       0x00       0x00       0x00       0x00


Column 7 Rescheduling State Counters by Rows:

dbg Counters         0          1          2          3          4          5          6          7
Total
```

```
=============   ========== ========== ========== ========== ========== ========== ========== ==========
==========
High Next Time  0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E11C0 0x524E1200 0x524E1240     -
Low Next Time   0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E1200 0x524E1200 0x524E1240     -
High Wheel Slot 0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849     -
Low Wheel Slot  0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849     -
DEQ_WHEEL       0x0001F5D0 0x0001F4BD 0x0001F56B 0x0001F6BF 0x0001F396 0x0001F3E8 0x0001F6BF 0x0001F4A7
0x000FA99B
DQ-lock Fails   0x0000039F 0x000003FD 0x000003B2 0x000003E1 0x000003CB 0x000003E2 0x000003FD 0x000003CD
0x00001EA6
TW ENQ Fails    0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_SCHED         0x0000FACD 0x0000FC6B 0x0000FA38 0x0000FCE4 0x0000FA66 0x0000F994 0x0000FC62 0x0000FB8B
0x0007DA3B
FAST_SCHED      0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_DEACT         0x0000FB03 0x0000F852 0x0000FB33 0x0000F9DB 0x0000F930 0x0000FA54 0x0000FA5D 0x0000F91C
0x0007CF60
Q_ACTIVATE      0x0000F9B6 0x0000F8D4 0x0000FA6C 0x0000FBA9 0x0000F87E 0x0000F95B 0x0000FB0A 0x0000F9DE
0x0007CF60
Q_CHANGE        0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG1          0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG2          0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG3          0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG4          0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG5          0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
```

Table 37 describes the significant fields shown in the display.

Table 37 show pxf cpu statistics queue Field Descriptions

Field	Description
Column 6 Enqueue/Dequeue Counters by Rows:	
enq_pkt	Packets the PXF enqueued.
tail_drop_pkt	Packets the PXF tails dropped.
deq_pkt	Packets the PXF dequeued.
deq_vtp_req	Number of times a dequeue was inhibited due to the virtual traffic policer.
deq_flow_off	Numbers of times a dequeue was inhibited due to a flowoff from the line card.
deq_ocq_off	Number of times a dequeue was inhibited due to link level flow control.
enqdeq_conflict	Shows a dequeue failed due to an enqueue to the same queue in progress.
bndl_pkt	Count of packets that were fragmented.
frag_pkt	Count of fragments sent.
dbg_frag_drop	Count of invalid multilink PPP (MLP) fragment handles.
dbg_bndl_sem	Count of semaphone collision (used for MLP).

Table 37 show pxf cpu statistics queue Field Descriptions (continued)

Field	Description
context_inhibit	Number of times multilink transmit fragment processing was inhibited due to a lack of DMA resources.
bfifo_enq_fail	Count of bundle FIFO (BFIFO) enqueue failures.
Column 7 Rescheduling State Counters by Rows:	
High Next Time	Current next send time for the high priority wheel.
Low Next Time	Current next send time for the low priority wheel.
High Wheel Slot	Current high priority slot number.
Low Wheel Slot	Current low priority slot number.
DEQ_WHEEL	Count of successful dequeues from the timing wheel.
DQ-lock Fails	Count of timing wheel dequeue failures (both queue empty and race conditions).
TW ENG Fails	Timing wheel enqueue failures.
Q_SCHED	Count of queues scheduled/rescheduled onto the timing wheel.
FAST_SCHED	Count of queues fast scheduled/rescheduled onto the timing wheel.
Q_DEACT	Count of queue deactivations.
Q_ACTIVATE	Count of queue activations (activate state).
Q_CHANGE	Count of queue changes; for example, Route Processor (RP) inspired rates changes.

The following example displays PXF L2TP packet statistics.

Note For L2TP Access Concentrator (LAC) operation, all statistics are applicable. For L2TP Network Server (LNS) operation, only the PPP Control Packets, PPP Data Packets, and PPP Station Packets statistics are meaningful.

```
Router# show pxf cpu statistics l2tp

LAC Switching Global Debug Statistics:
    PPP Packets           51648
    PPP Control Packets   51647
    PPP Data Packets      1
    Not IPv4 Packets      1
    IP Short Hdr Packets  1
    IP Valid Packets      0
    IP Invalid Packets    1
    DF Cleared Packets    0
    Path MTU Packets      0
    No Path MTU Packets   0
    Within PMTU Packets   0
    Fraggable Packets     0
    PMTU Pass Packets     0
    PMTU Fail Packets     0
    Encapped Packets      51648
```

```
L2TP Classification Global Debug Statistics:
    LAC or Multihop Packets  151341
    Multihop Packets         0
    PPP Control Packets      51650
    PPP Data Packets         99691
    PPP Station Packets      151341
```

The following example displays match statistics for the police_test policy on an ATM interface. The Classmap Index differentiates classes within a policy while the Match Number differentiates match statements within a class.

```
Router# show pxf cpu statistics qos atm 6/0/0.81801

               Classmap          Match         Pkts          Bytes
                Index            Number      Matched        Matched
              ------------      -----------  ------------   ----------
 police_test (Output) service-policy :
         police_class    (0)       0            0             0
                                   1            0             0
                                   2            0             0
                                   3            0             0

         class-default   (1)       0            0             0
```

Cisco 10000 Series Router

The following example displays the top 10 packet types diverted to the RP. The output displays the top punters by interface and by Layer 2 packet flow.

```
Router# show pxf cpu statistics diversion top 10

Top 10 punters by interface are:
Rate (pps)      Packets  (diverted/dropped)      vcci      Interface
        1       10/0     2606Virtual-Access2.1
        Last diverted packet type is none.

Top 10 punters by Layer 2 flow are:
Rate (pps)      Packets  (diverted/dropped)     Interface       Layer 2 info
        1       15/0    ATM2/0/3       vpi 128/vci 4096/vcci 2591
        Last diverted packet type is oam_f4.
        1       15/0    ATM2/0/3       vpi 128/vci 4096/vcci 2593
        Last diverted packet type is oam_f4.
```

Related Commands

Command	Description
platform c10k divert-policer	Configures the rate and burst size of the divert-policer.
show pxf statistics	Displays a summary of statistics in the PXF.

show vpdn tunnel

To display information about active Layer 2 tunnels for a virtual private dialup network (VPDN), use the **show vpdn tunnel** command in privileged EXEC mode.

show vpdn tunnel [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets** [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport** [*filter*]]

Syntax Description

l2f	(Optional) Specifies that only information about Layer 2 Forwarding (L2F) tunnels will be displayed.
l2tp	(Optional) Specifies that only information about Layer 2 Tunnel Protocol (L2TP) tunnels will be displayed.
pptp	(Optional) Specifies that only information about Point-to-Point Tunnel Protocol (PPTP) tunnels will be displayed.
all	(Optional) Displays summary information about all active tunnels.
filter	(Optional) One of the filter parameters defined in Table 38.
packets	(Optional) Displays packet numbers and packet byte information.
state	(Optional) Displays state information for a tunnel.
summary	(Optional) Displays a summary of tunnel information.
transport	(Optional) Displays tunnel transport information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **packet**s and **all** keywords were added.
12.3(2)T	The **l2f**, **l2tp**, and **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for L2TP congestion avoidance statistics.
12.4(11)T	The **l2f** keyword was removed.
12.2(33)SB	This command's output was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.

Usage Guidelines

Use the **show vpdn tunnel** command to display detailed information about L2TP, L2F, and PPTP VPDN tunnels.

Table 38 defines the filter parameters available to refine the output of the **show vpdn tunnel** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 38 Filter Parameters for the show vpdn tunnel Command

Syntax	Description
id *local-id*	Filters the output to display only information for the tunnel with the specified local ID. • *local-id*—The local tunnel ID number. Valid values range from 1 to 65535.
local-name *local-name remote-name*	Filters the output to display only information for the tunnel associated with the specified names. • *local-name*—The local tunnel name. • *remote-name*—The remote tunnel name.
remote-name *remote-name local-name*	Filters the output to display only information for the tunnel associated with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **show vpdn tunnel summary** command no longer displays the active PPPoE sessions. Instead, use the **show pppoe sessions** command to display the active sessions.

In Cisco IOS Release 12.2(31)SB, the **show vpdn tunnel summary** command does display the active PPPoE sessions.

Examples

The following is sample output from the **show vpdn tunnel** command for L2F and L2TP sessions:

```
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    router1       est    172.21.9.13     1701  1

L2F Tunnel
 NAS CLID HGW CLID NAS Name        HGW Name        State
 9         1        nas1           HGW1            open
                    172.21.9.4      172.21.9.232

%No active PPTP tunnels
```

Table 39 describes the significant fields shown in the display.

Table 39 show vpdn tunnel Field Descriptions

Field	Description
LocID	Local tunnel identifier.
RemID	Remote tunnel identifier.
Remote Name	Hostname of the remote peer.

Table 39 show vpdn tunnel Field Descriptions (continued)

Field	Description
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Remote address	IP address of the remote peer.
Port	Port ID.
Sessions	Number of sessions using the tunnel.
NAS CLID	A number uniquely identifying the VPDN tunnel on the network access server (NAS).
HGW CLID	A number uniquely identifying the VPDN tunnel on the gateway.
NAS Name	Hostname and IP address of the NAS.
HGW Name	Hostname and IP address of the home gateway.

The following example shows L2TP tunnel activity, including information about the L2TP congestion avoidance:

```
Router# show vpdn tunnel l2tp all

L2TP Tunnel Information Total tunnels 1 sessions 1

Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
    Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
    Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 500, Remote RWS 500
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 500
    Mode of operation is Slow Start
  Tunnel PMTU checking disabled
  Retransmission time 1, max 2 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 0, ZLB ACKs sent 2
```

```
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
Control message authentication is disabled
```

Table 40 describes the significant fields shown in the display.

Table 40 show vpdn tunnel all Field Descriptions

Field	Description
Local RWS	Size of the locally configured receive window.
Remote RWS	Size of the receive window configured on the remote peer.
Congestion Window size, Cwnd 3	Current size of the congestion window (Cwnd).
Slow Start threshold, Ssthresh 500	Current value of the slow start threshold (Ssthresh).
Mode of operation is...	Indicates if the router is operating in Slow Start or Congestion Avoidance mode.

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [permit duplicates]

Syntax Description.

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration (config-if)
Service instance configuration (config-if-srv)

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	The **permit duplicates** keyword pair was added in Cisco IOS Release 12.2(30)S.
12.3(8)T	Support for the **permit duplicates** keyword pair was integrated in Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI 0 interface:

```
Router(config)# interface bri 0
Router(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 50 ethernet
Router(config-if-srv)# snmp trap link-status
Router(config-if-srv)# exit
```

Related Commands

Command	Description
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.

virtual-template

To specify which virtual template will be used to clone virtual access interfaces, use the **virtual-template** command in VPDN group configuration mode. To remove the virtual template from a virtual private dial-up network (VPDN) group, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

template-number	Number of the virtual template that will be used to clone virtual access interfaces.

Defaults

No virtual template is enabled.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was enhanced to enable PPPoE on ATM to accept dial-in PPP over Ethernet (PPPoE) sessions.
12.2(15)T	This command was enhanced to allow IP per-user attributes to be applied to a Layer 2 Tunneling Protocol (L2TP) dial-out session.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.

Usage Guidelines

You must first enable a tunneling protocol on the VPDN group using the **protocol (VPDN)** command before you can enable the **virtual-template** command. Removing or modifying the **protocol** command will remove the **virtual-template** command from the VPDN group.

Each VPDN group can clone only virtual access interfaces using one virtual template. If you enter a second **virtual-template** command on a VPDN group, it will replace the first **virtual-template** command.

Table 41 lists the VPDN group commands under which the **virtual-template** command can be entered. Entering the VPDN group command starts VPDN group configuration mode. The table includes the command-line prompt for the VPDN group configuration mode and the type of service configured.

Table 41 VPDN Subgroups

VPDN Group Command	Command Mode Prompt	Type of Service
accept-dialin	`router(config-vpdn-acc-in)#`	Tunnel server
request-dialout	`router(config-vpdn-req-ou)#`	L2TP network server (LNS)

When the **virtual-template** command is entered under a **request-dialout** VPDN subgroup, IP and other per-user attributes can be applied to an L2TP dial-out session from an LNS. Before this command was enhanced, IP per-user configurations from authentication, authorization, and accounting (AAA) servers were not supported; the IP configuration would come from the dialer interface defined on the router.

The enhanced **virtual-template** command works in a way similar to configuring virtual profiles and L2TP dial-in. The L2TP virtual access interface is first cloned from the virtual template, which means that configurations from the virtual template interface will be applied to the L2TP virtual access interface. After authentication, the AAA per-user configuration is applied to the virtual access interface. Because AAA per-user attributes are applied only after the user has been authenticated, the LNS must be configured to authenticate the dial-out user (configuration authentication is needed for this command).

With the enhanced **virtual-template** command, all software components can now use the configuration present on the virtual access interface rather than what is present on the dialer interface. For example, IP Control Protocol (IPCP) address negotiation uses the local address of the virtual access interface as the router address while negotiating with the peer.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example enables the LNS to accept an L2TP tunnel from an L2TP access concentrator (LAC) named LAC2. A virtual access interface will be cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname LAC2
```

The following example enables PPPoE on ATM to accept dial-in PPPoE sessions. A virtual access interface for the PPP session is cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
```

The following partial example shows how to configure an LNS to support IP per-user configurations from a AAA server:

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
 request-dialout
  protocol l2tp
  rotary-group 1
  virtual-template 1
 initiate-to ip 10.0.1.194.2
 local name lns
 l2tp tunnel password 7094F3$!5^3
 source-ip 10.0.194.53
!
```

The previous configuration requires a AAA profile such as the following example to specify the per-user attributes:

```
5300-Router1-out  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "outbound:dial-number=5550121"
7200-Router1-1  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "ip:route=10.17.17.1 255.255.255.255 Dialer1 100 name 5300-Router1"
5300-Router1 Password = "cisco"
     Service-Type = Framed
     Framed-Protocol = PPP
     cisco-avpair = "lcp:interface-config=ip unnumbered loopback 0"
     cisco-avpair = "ip:outacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:outacl#2=permit ip any any"
     cisco-avpair = "ip:inacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:inacl#2=permit ip any any"
     cisco-avpair = "multilink:min-links=2"
     Framed-Route = "10.5.5.6/32 Ethernet4/0"
     Framed-Route = "10.5.5.5/32 Ethernet4/0"
     Idle-Timeout = 100
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and to create an accept-dialin VPDN subgroup.
protocol (VPDN)	Specifies the Layer 2 Tunneling Protocol that the VPDN subgroup will use.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP and to create a request-dialout VPDN subgroup.
show vtemplate	Displays information about all configured virtual templates.
vpdn-group	Defines a local, unique group number identifier.

vpdn enable

To enable virtual private dialup networking (VPDN) on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** command in global configuration mode. To disable, use the **no** form of this command.

vpdn enable

no vpdn enable

Syntax Description

This command has no arguments or keywords.

Command Default

VPDN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines below.

Usage Guidelines

The **no vpdn enable** command does not automatically disable a VPDN tunnel.

To shut down a VPDN tunnel, use the **clear vpdn tunnel** command or the **vpdn softshut** command.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, the following warning message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays the following warning message:

```
% VPDN is not enabled
```

Examples

The following example enables VPDN on the router:

```
vpdn enable
```

Related Commands

Command	Description
clear vpdn tunnel	Shuts down a specified tunnel and all sessions within the tunnel.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn softshut	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

vpdn group

To associate a virtual private dialup network (VPDN) group with a customer or VPDN profile, use the **vpdn group** command in customer profile or VPDN profile configuration mode. To disassociate a VPDN group from a customer or VPDN profile, use the **no** form of this command.

vpdn group *name*

no vpdn group *name*

Syntax Description

name	Name of the VPDN group. **Note** This name should match the name defined for the VPDN group configured with the **vpdn-group** command.

Defaults

No default behavior or values.

Command Modes

Customer profile configuration
VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines below.

Usage Guidelines

Use the **vpdn group** command in customer profile configuration mode or VPDN profile configuration mode to associate a VPDN group with a customer profile or a VPDN profile, respectively.

VPDN groups are created using the **vpdn-group** command in global configuration mode.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, the following warning message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays the following warning message:

```
% VPDN is not enabled
```

Examples

The following example creates the VPDN groups named l2tp and l2f, and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)# vpdn group l2tp
Router(config-vpdn-profile)# vpdn group l2f
```

The following example creates two VPDN groups and configures them under a customer profile named company2:

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)#
!
Router(config)# vpdn-group yourgroup
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn company2
Router(config-vpdn-profile)# vpdn group mygroup
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

Feature Information for CLI Command Changes

Table 42 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 42 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 42 Feature Information for CLI Command Changes

Feature Name	Releases	Feature Information
CLI command changes	12.2(33)SB	Modifies command behavior on the Cisco 10000 series router.