

show pxf accounting

To show Parallel eXpress Forwarding (PXF) switching statistics for individual interfaces, use the **show pxf accounting** command in user EXEC or privileged EXEC mode.

show pxf accounting *interface* [*slot/port*]

Syntax Description	<i>interface</i>	Specifies the type of interface to display.
	<i>slot/</i>	(Optional) Backplane slot number. On the Cisco 7200 VXR series routers, the value can be from 0 to 6.
	<i>port</i>	(Optional) Port number of the interface. On the Cisco 7200 VXR series routers, the value can be from 0 to 5.

Command Modes	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Usage Guidelines	You can display information about the interface types shown in Table 83 using the show pxf accounting command:

Table 83 *show pxf accounting Interface Types*

Keyword	Interface Type
atm	ATM interface
ethernet	Ethernet interface
fastethernet	FastEthernet interface
hssi	High Speed Serial interface
null	Null interface
pos	Packet-over-SONET interface
serial	Synchronous serial interface
summary	PXF summary statistics

Examples

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

```
Router# show pxf accounting ?

ATM          ATM interface
Ethernet     IEEE 802.3
FastEthernet FastEthernet IEEE 802.3
Hssi         High Speed Serial Interface
Null         Null interface
POS          Packet over Sonet
Serial       Serial
summary      PXF summary statistics
```

The following is sample output from the **show pxf accounting ethernet** command with an Ethernet interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting ethernet 4/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Ethernet4/0	0	0	122	11490	4	0

The following is sample output from the **show pxf accounting null** command with a null interface in slot 0 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting null 0/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
nu0/0	0	0	0	0	4932	0

The following is sample output from the **show pxf accounting pos** command with a Packet-over-SONET interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting pos
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
POS4/0	19	1064	0	0	44	0

The following is sample output from the **show pxf accounting serial** command with a serial interface in slot 5 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting serial 5/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Serial5/0	0	0	0	0	0	0

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

```
Router# show pxf accounting summary
```

Pkts	Dropped	RP Processed	Ignored
Total	0	48360	0

PXF Statistic:
Packets RP -> PXF:

switch ip:	0
switch raw:	30048360
qos fastsend:	0
qos enqueue:	1938
Total:	30050298

```

Packets PXF -> RP:
  qos pkts:          1938
  fast pkts:        30000000
  drops:total        0
  punts:total        48360
  "    not IP      :    40572
  "    CEF no adjacency :    7788
Total:              30050298

Packets ignored:      0 | ring space:
  shadow ring full:    0 |   shadow ring:      16384
  in ring full:        0 |   inring:           968
  PXF inactive:        0

tx credits:           16230330 | delayed credits:      0
holdq enqueues:        0 | requeue drops:        0
interrupts:            40538 | interrupt misses:     1947
interrupt packets:     53326
pending read bytes:    0

```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Fa0/0	0	0	30000000	1740000000	970	0
Et1/0	0	0	0	0	21309	0
Et1/1	0	0	0	0	0	0
Et1/2	0	0	0	0	0	0
Et1/3	0	0	0	0	0	0
Se2/0	0	0	0	0	963	0
Se2/1	0	0	0	0	0	0
Se2/2	0	0	0	0	0	0
Se2/3	0	0	0	0	0	0
Fa3/0	0	0	0	0	963	0
PO4/0	30000000	1440000000	0	0	963	0
AT5/0	0	0	0	0	23192	0
Vi1	0	0	0	0	0	0
Vt1	0	0	0	0	0	0
Vi2	0	0	0	0	0	0

Related Commands

Command	Description
show pxf crash	Displays PXF crash information.
show pxf feature	Displays the PXF routing feature tables for enabled PXF features.
show pxf interface	Displays a summary of the interfaces in the router and the PXF features or capabilities enabled on these interfaces.

show pxf cpu access-lists

To display Parallel eXpress Forwarding (PXF) memory information for access control lists (ACLs), use the **show pxf cpu access-lists** command in privileged EXEC mode.

show pxf cpu access-lists [**security** | **qos** | **pbr** | **compiled**]

Cisco 10000 Series Router

show pxf cpu access-lists [**security** [[**tcam** *acl-name* [**detail**]] | **flex-sum** | **children**] | **qos** | **pbr** | **compiled**]

Syntax Description	
security	(Optional) Displays information about the security ACLs defined in Cisco IOS and compiled to the PXF. Also displays information about split ACLs, such as how much memory has been used.
tcam <i>acl-name</i>	(Optional) Displays information about the specified security ACL stored in ternary content addressable memory (TCAM). This option is only available on the PRE3 for the Cisco 10000 series router.
detail	(Optional) Displays decoded information about the packet fields used for matching in the TCAM.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the parallel express forwarding (PXF) engine for use by the flexible key construction microcode. This information is useful for design teams. This option is only available on the PRE3 for the Cisco 10000 series router.
children	(Optional) Displays information for child policies. If an ACL is a template child, the output typically does not display the child information. Specifying the children keyword displays data for child policies, too, and shows the children and the parent policy of each child. Use caution when using the children keyword as there might be thousands of child policies configured, which could have negative effects on the command output.
qos	(Optional) Displays information about the QoS ACLs defined in Cisco IOS and compiled to the PXF.
pbr	(Optional) Displays information about ACLs for policy-based routing (PBR).
compiled	(Optional) Displays information for all compiled Turbo-ACLs. The PRE2 supports Turbo-ACLs and the compiled option. The PRE3 accepts the PRE2 compiled option, but does not implement Turbo-ACLs.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the PRE2 for the Cisco 10000 series router.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines**Cisco 10000 Series Router (PRE2)**

Because memory is shared between TurboACLs and MiniACLs, they can interfere with each other's capacities. The Mini-ACL is automatically set up with space for 8191 Mini-ACLs at router start. If more than 8191 Mini-ACLs are created, another block of MiniACLs (4096) is allocated. This process is repeated as necessary until the router is out of External Column Memory (XCM) in any one bank that the Mini-ACLs need.

Cisco 10000 Series router (PRE3)

The PRE3 implements only TCAM ACLs. Turbo-ACLs and Mini-ACLs are not supported.

Examples

The sample output from the **show pxf cpu access-lists security** command (see [Sample Output](#)) is based on the configuration of the access control list (ACL) called test_list (see [ACL Configuration](#)). The sample output is divided into several sections with a description of the type of information displayed in each.

ACL Configuration

```
Router# show pxf cpu access-lists test_list
```

```
Extended IP access list test_list (Compiled)
```

```
10 permit ip any host 10.1.1.1
20 permit ip any host 10.1.1.2
30 permit ip any host 10.1.1.3
40 permit ip any host 10.1.1.4
50 permit ip any host 10.1.1.5
60 permit ip any host 10.1.1.6
70 permit ip any host 10.1.1.7
80 permit ip any host 10.1.1.8
90 permit ip any host 10.1.1.9
100 permit ip any host 10.1.1.11
110 permit ip any host 10.1.1.12
```

Sample Output

The following sample output describes the information displayed in the first section of the command output from the **show pxf cpu access-lists security** command:

```
Router# show pxf cpu access-lists security
```

```
PIX Security ACL statistics:
```

ACL	State	Tables	Entries	Config	Fragment	Redundant	Memory	ACL_index
1	Operational	1	-	-	-	-	0Kb	1
sl_def_acl	Operational	2	-	-	-	-	0Kb	2
test	Operational	3	-	-	-	-	0Kb	3
test_list	Operational	1	12	11	0	0	7Kb	1

Table 84, Part 1, describes the significant fields shown in the display.

Table 84, Part 1 *show pxf cpu access-lists security Field Descriptions*

Field	Description
ACL	Identifies the ACL by name or number.
State	Displays the current state of the ACL: <ul style="list-style-type: none"> Copying—ACL is in the process of being created or compiled. Operational—ACL is active and filtering packets. Out of acl private mem—ACL has run out of the private memory that was allocated exclusively to it. Out of shared mem—ACL has run out of the memory that it shares with other ACLs. Unknown Failure—ACL has failed because of an uncategorized reason. Unneeded—ACL was allocated but is not currently in use.
Tables	An indicator of whether the ACL has been split into more than one PXF pass. The first three ACLs in the output are MiniACLs, and have the ACL_index duplicated in the Tables column.
Entries	The count of ACL rules as seen by the Turbo compiler. This is the sum of the Config, Fragment, and Redundant columns plus 1.
Config	The count of rules for this ACL.
Fragment	The count of extra rules added to handle fragment handling, where Layer 4 information is needed but not available in a packet fragment.
Redundant	The count of rules that are not needed because they are covered by earlier rules.
Memory	The amount of PXF XCM in use for the ACL.
ACL_index	The index of the ACL in XCM.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command:

First level lookup tables:

Block	Use	Rows	Columns	Memory used
0	TOS/Protocol	1/128	1/32	16384
1	IP Source (MS)	1/128	1/32	16384
2	IP Source (LS)	1/128	1/32	16384
3	IP Dest (MS)	2/128	1/32	16384
4	IP Dest (LS)	12/128	1/32	16384
5	TCP/UDP Src Port	1/128	1/32	16384
6	TCP/UDP Dest Port	1/128	1/32	16384
7	TCP Flags/Fragment	1/128	1/32	16384

Table 84, Part 2, describes the significant fields shown in the display.

Table 84, Part 2 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Block	Indicates the block number.
Use	Describes the IP packet field that is being matched.
Rows	An indication of where the largest variety of values are in use in the ACLs that are being applied. In the output, 12/128 means that there are 12 different values of significance in the field. If there are other rules added and the value exceeds 128, more memory will be needed to accommodate the new rules.
Columns	An indication of the number of TurboACLs in PXF memory. In the output, 1/32 means there is only one TurboACL in PXF memory. If there are more than 31 added, another chunk of memory is needed to accommodate the new ACLs.
Memory used	Displays the total amount of memory used for this particular lookup table.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command. There are 16 banks of XCM in each PXF column. This output section shows the usage level of each bank.

Banknum	Heapsize	Freesize	%Free
0	4718592	4702208	99
1	8126464	6012928	73
2	8388608	6290432	74
3	8388608	6290432	74
4	5898240	5881856	99
5	8126464	6012928	73
6	8388608	6290432	74
7	8126464	6012928	73
8	4456448	4440064	99
9	8126464	6012928	73

Table 84, Part 3, describes the significant fields shown in the display.

Table 84, Part 3 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Banknum	The block of memory used for this particular lookup table.
Heapsize	The total amount of memory, in bytes, allocated for this block.
Freesize	The amount of memory, in bytes, that is currently available for use by this block of memory.
%Free	The percentage of memory that is free and available for use for this block of memory. When the %Free drops to 0, the router cannot hold any more ACLs in PXF memory, and any new ACL will not pass traffic.

This section of the sample command output indicates the memory usage of the MiniACLs in the router. All of the rows state about the same thing. To determine the actual number of MiniACLs in play, divide the memory used in any of blocks 1 to 10 by 256, or blocks 11 to 14 by 16.

```
MiniACL XCM Tables:
Block  Use                Memory Used  %Free
0      IP Src 1                768        99
1      IP Src 2                768        99
2      IP Src 3                768        99
3      IP Src 4                768        99
4      IP Dest 1               768        99
5      IP Dest 2               768        99
6      IP Dest 3               768        99
7      IP Dest 4               768        99
8      ToS                    768        99
9      Protocol                768        99
10     TCP Flags/Fragment     768        99
11     Source Port 1          48         99
12     Source Port 2          48         99
13     Destination Port 2     48         99
14     Destination Port 2     48         99
```

The following describes the information displayed in the last section of the sample output from the **show pxf cpu access-lists security** command:

```
Available MiniACL count = 8191
Usable ranges(inclusive):
1->8191
```

Table 84, Part 4, describes the significant fields shown in the display.

Table 84, Part 4 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Available MiniACL	The number of ACLs currently available for allocation in XCM.
Usable ranges	The ACL indexes that will be assigned to MiniACLs.

PRE2 and PRE3 Security ACLs Examples (Cisco 10000 Series Router)

This section compares the output from the **show pxf cpu access-lists security** command when issued on the PRE2 and PRE3.

For the PRE2, the following sample output displays VMR (value, plus a mask and result) data for the ACL named ICMP_IGMP_MATCH:

```
Router# show pxf cpu access-lists security tcam ICMP_IGMP_MATCH detail

-----
VMR Format - handle: 524607B4
Format has 5 fields, refcount = 1
Field: Format, FIXED, start_bit = 69, end_bit = 71
Field: ACL index, FIXED, start_bit = 54, end_bit = 68
Field: Flags, FIXED, start_bit = 43, end_bit = 53
Field: L4 proto, FIXED CNV, start_bit = 16, end_bit = 23
Field: L4 source port, FIXED CNV, start_bit = 0, end_bit = 15 Total bits = 53, format = 72
GMR used: 5 Col 2 LKBP Vector: 544
-----
VMRs
----- VMR 0 -----
```



```

V: 001B0000 0000010B 00
M: FFFFC000 0000FFFF FF
R: 00010001
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00000B00/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
----- VMR 1 -----
V: 001B0000 00000103 01
M: FFFFC000 0000FFFF FF
R: 00010002
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00000301/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
----- VMR 2 -----
V: 001B0000 00000213 00
M: FFFFC000 0000FFFF 00
R: 00010003
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001300/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000
----- VMR 3 -----
V: 001B0000 00000214 00
M: FFFFC000 0000FFFF 00
R: 00010004
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001400/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000

```

For the PRE3, the following sample output displays for the **show pxf cpu access-lists security** command. Notice that the output does not include the columns shown above that are relevant to only the PRE2 and the output no longer displays first-level lookup tables.

Router# **show pxf cpu access-lists security**

```

PXF Security ACL statistics:
ACL                               State          ACL_index
STANDARD_MATCH_PERMIT           Operational    116
SRC_IP_MATCH144                 Operational    102
DST_IP_MATCH                    Operational    113
DST_IP_MATCH144                 Operational    112
PROTOCOL_MATCH                  Operational    104
PROTOCOL_MATCH144               Operational    103
FRAG_MATCH                      Operational    109
PRECEDENCE_TOS_MATCH            Operational    106
PRECEDENCE_TOS_MATCH144         Operational    105

```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf statistics	Displays a chassis-wide summary of PXF statistics.

show pxf cpu atom

To display Parallel eXpress Forwarding (PXF) CPU Any Transport over MPLS (AToM) forwarding information for an interface or Virtually Cool Common Index (VCCI), use the **show pxf cpu atom** command in privileged EXEC mode.

show pxf cpu atom [*interface-name* | *vcci*]

Syntax Description

<i>interface-name</i>	(Optional) Name of the interface.
<i>vcci</i>	(Optional) VCCI entry identifier.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB	This command was introduced on the Cisco 10000 series router.

Examples

The following example shows AToM forwarding information for Gigabit Ethernet interface 6/0/0. The fields shown in the display are self-explanatory.

Router#: **show pxf cpu atom gigabitethernet 6/0/0**

```
Imposition Information for VCCI 0x9E2:
  Output VCCI: 0x0
  Mac rewrite index: 0x0 extension: 0x0
  Ingress Flags: 0x0
  PTI Action Table: 0x0
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about AToM VCs that are enabled to route Layer 2 packets on a router.
show pxf cpu mpls	Displays PXF MPLS FIB entry information.
show pxf cpu subblocks	Displays subblocks information that includes column 0 of AToM.

show pxf cpu bba

To display information on Parallel eXpress Forwarding (PXF) CPU Broadband Aggregation (BBA) groups, use the **show pxf cpu bba** command in privileged EXEC mode.

show pxf cpu bba

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples	The following example shows BBA groups information in the PXF CPU:
-----------------	--

Router# **show pxf cpu bba**

```
6w3d: show_pxf_bba
6w3d: %IPCOIR-4-REPEATMSG: IPC handle already exists for 1/0
6w3d: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/0 is down. Notifying 4oc3atm-1 dr.
6w3d: %C10K_ALARM-6-INFO: ASSERT CRITICAL slot 1 Card Stopped Responding OIR Al
6w3d: %IPCOIR-5-CARD_DETECTED: Card type 4oc3atm-1 (0x2D8) in slot 1/0
6w3d: %IPCOIR-5-CARD_LOADING: Loading card in slot 1/0 sw version 1.1 code MD5 C
6w3d: %C10K-5-LC_NOTICE: Slot[1/0] 4oc3atm-1 Image Downloaded...Booting...
6w3d: %IPCOIR-5-CARD_DETECTED: Card type 4oc3atm-1 (0x2D8) in slot 1/0
6w3d: %C10K_ALARM-6-INFO: CLEAR CRITICAL slot 1 Card Stopped Responding OIR Ala
6w3d: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/0 is up. Notifying 4oc3atm-1 driv.
```

Related Commands	Command	Description
	bba-group pppoe	Configures a BBA group to establish PPPoE sessions.

show pxf cpu buffers

To display packet buffer memory for temporary packet storage in the Cisco Internetwork Performance Monitor (IPM) of the Parallel eXpress Forwarding (PXF), use the **show pxf cpu buffers** command in privileged EXEC mode.

show pxf cpu buffers

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines This command provides information about the number of handles that are used and available. Handles are outstanding packets in the virtual time management system (VTMS).

Examples The following example shows the number of handles that are used and available:

```
Router# show pxf cpu buffers

Cobalt2 ttc running.
Calculations could be off by (+/-) cache sizes.
      cache size
small   512
large   128

pool    # handles   available
-----
small   524288      523808
large   32768       32624
```

[Table 85](#) describes the fields shown in the display.

Table 85 *show pxf cpu buffers Field Descriptions*

Field	Description
pool	Identifies the buffer pool.
# handles	The number of handles that are currently used.
available	The number of handles that are currently available.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu cef

The **show pxf cpu cef** command is replaced by the **show ip cef platform** command on the Cisco 10000 series router. See the **show ip cef platform** command for more information.

show pxf cpu context

To display the current and historical loads on the Parallel eXpress Forwarding (PXF), use the **show pxf cpu context** command in privileged EXEC mode.

show pxf cpu context

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The **show pxf cpu context** command shows how busy the PXF forwarding process (FP) is with the current traffic load. The first section displays the number of contexts of each type that have entered the PXF engine since it was last reloaded. If counters are idle, the PXF pipeline is not operating properly.

Router# **show pxf cpu context**

```

FP context statistics      count      rate (since last time command was run)
-----
  feed_back               168635      0
  new_work_from_lc        7474477     13
  new_work_from_rp        964679      1
  new_work_from_replay    0           0
  null_context            3797097495884 6312156
-----
                               6312170
FP average context/sec    1min      5min      60min
-----
  feed_back               0          0          0      cps
  new_work_from_lc        8          8          8      cps
  new_work                 1          1          1      cps
  new_work_from_replay    0          0          0      cps
  null_context            6312260    6312261    6312250    cps
-----
  Total                   6312270    6312271    6312260    cps

FP context utilization    1min      5min      60min
-----
  Actual                  0 %       0 %       0 %
  Theoretical              0 %       0 %       0 %
  Maximum                 98 %      98 %      98 %

```

Table 85 describes the significant fields shown in the display.

Table 86 *show pxf cpu context Field Descriptions*

Field	Description
FP context statistics	
feed_back	Packets requiring additional passes through the pipeline. This counter is incremented once for each additional pass.
new_work	New packets input to the PXF pipeline. This counter represents a snapshot of the amount of incoming traffic being processed by the processor.
null_context	An indication of unused forwarding bandwidth (idle time). This counter is incremented for every context during which the PXF pipeline is not processing traffic. This counter represents the processor's potential to handle additional traffic. As the processor becomes more busy, the value for null decreases until it becomes zero, at which point the processor has reached its maximum usage.
FP average context/sec	
feed_back	Displays the rate, in terms of the number of contexts per second (cps) for the feed_back counter for the last 1-minute, 5-minute, and 60-minute time periods.
new_work	Displays the rate, in terms of the number of contexts per second (cps) for the new_work counter for the last 1-minute, 5-minute, and 60-minute time periods.
null_context	Displays the rate, in terms of the number of contexts per second (cps) for the null_counter for the last 1-minute, 5-minute, and 60-minute time periods.
FP context utilization	
Actual	Displays the actual percentage of processor usage per second, compared to the theoretical maximum, for the last 1-minute, 5-minute, and 60-minute time periods.
Theoretical	Displays the percentage of processor usage compared to the ideal theoretical capacities for the last 1-minute, 5-minute, and 60-minute time periods. The theoretical maximum for the PXF processors is 3,125,000 contexts per second (cps).
Maximum	Displays the actual maximum percentage of processor usage that has occurred for the last 1-minute, 5-minute, and 60-minute time periods.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu feedback

To display the total number of feedbacks through the Parallel eXpress Forwarding (PXF) by all packets, use the **show pxf cpu feedback** command in privileged EXEC mode.

show pxf cpu feedback

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples The following example shows feedback counters information:

Router# **show pxf cpu feedback**

Load for five secs: 5%/0%; one minute: 6%; five minutes: 2%
Time source is hardware calendar, *21:13:02.615 UTC Tue Nov 29 2005

FP column 0 feedback counts

Global packet handle retry counter = 0

Name	Current	Difference (since last show)
-----	-----	-----
bypass	= 0	0
schedule retry	= 0	0
WRED sample	= 0	0
MLPPP linkq update	= 0	0
IP frag	= 0	0
ICMP	= 0	0
layer2 divert	= 0	0
tunnel lookup	= 0	0
tunnel RX	= 0	0
tunnel TX	= 0	0
output qos	= 0	0
tag not ip	= 0	0
netflow accumulate	= 0	0
netflow age	= 0	0
netflow swap	= 0	0
netflow export	= 0	0
PBR	= 0	0
input secACL log	= 0	0
input secACL split	= 0	0
output secACL log	= 0	0
output secACL split	= 0	0
IPC response	= 0	0
IPC MLPPP flush	= 0	0
input qos split	= 0	0

```

output qos split           = 0          0
MLPPP fwd packet          = 0          0
MLPPP background          = 0          0
MLPPP flush                = 0          0
drop                       = 0          0
QPPB                      = 0          0
mcast lookup              = 0          0
mcast replicate           = 0          0
mcast rpf failed          = 0          0
mcast bypass              = 0          0
PBR split                 = 0          0
MLPPP lock retry          = 0          0
output secACL             = 0          0
qos divert split          = 0          0
qos inject split          = 0          0
secACL divert split       = 0          0
MLPPP frag                = 0          0
mpls deaggregation        = 0          0
tunnel in secACL log      = 0          0
tunnel out secACL log     = 0          0
no packet handle          = 0          0
PBR to FIB                = 0          0
MLPPP flush lock retry    = 0          0
MLPPP flush setup         = 0          0
MLPPP sync flush req      = 0          0
tail drop IP frag         = 0          0
RP inject                 = 0          0
feedback retry            = 0          0
MLPPP discard feedback    = 0          0
MLPPP stats copy IPC      = 0          0
IPM replay                = 0          0
IPM replay drop           = 0          0
IP reasm lock retry       = 0          0
IP reasm recover punt     = 0          0
IP reasm forward          = 0          0
IP reasm insertion        = 0          0
LAC switch                = 0          0
L2TP decap                = 0          0
IP reasm fb divert qos    = 0          0
keepalive                 = 0          0
drop stats redirect       = 0          0
AToM multiplexed          = 0          0
LFI reassembly            = 0          0
LFI remove entry          = 0          0
iEdge translation         = 0          0
iEdge divert              = 0          0
multiple input qos        = 0          0
multiple output qos       = 0          0
iEdge PBHK DS trans       = 0          0
LAC switch qos            = 0          0
WRED sample init          = 0          0
replay egress             = 0          0
IPV6 FIB                  = 0          0
ICMPV6                    = 0          0
IPV6 ACL                  = 0          0
IPV6 DIVERT ACL           = 0          0
Total                     = 0          0

```

Related Commands

Command	Description
show pxf cpu context	Displays the current and historical loads on the PXF.

show pxf cpu iedge

To display Parallel eXpress Forwarding (PXF) policy and template information, use the **show pxf cpu iedge** command in privileged EXEC mode.

show pxf cpu iedge [**detail** | **policy** *policy-name* | **template**]

Syntax Description	detail	(Optional) Displays detailed information about policies and templates.
	policy <i>policy-name</i>	(Optional) Displays summary policy information.
	template	(Optional) Displays summary template information.

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.

Examples The following example shows PXF template information. The fields shown in the display are self-explanatory.

Router# **show pxf cpu iedge template**

```

Super ACL name           OrigCRC   Class Count   CalcCRC
1sacl_2                  4EA94046    2             00000000
if_info 71BA3F20

```

Related Commands	Command	Description
	show pxf statistics	Displays a summary of PXF statistics.

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

<i>ipv6: address [prefix]</i>	(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 ::1/128,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 mpls

To display Parallel eXpress Forwarding (PXF) Multiprotocol Label Switching (MPLS) Forwarding Information Base (FIB) information, use the **show pxf cpu mpls** command in privileged EXEC mode.

show pxf cpu mpls [**labels** *label-value* | **vrf**]

Syntax Description	labels <i>label-value</i>	(Optional) Displays the transport type and output features associated with the specified label value or label range. The <i>label-value</i> range is 0 to 524288.
	vrf	(Optional) Displays virtual routing and forwarding (VRF) root information.

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.

Examples

The following example shows VRF root information. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu mpls vrf
VRF_ID 0      FIB_ROOT(RP) 0x72400000
```

Related Commands	Command	Description
	ping mpls	Checks MPLS LSP connectivity.
	show mpls interfaces	Displays information about the interfaces configured for label switching.
	show pxf cpu statistics	Displays PXF CPU statistics.
	trace mpls	Discovers MPLS LSP routes that packets will take when traveling to their destinations.

show pxf cpu mroute

To display Parallel eXpress Forwarding (PXF) multicast route (mroute) information, use the **show pxf cpu mroute** command in privileged EXEC mode.

show pxf cpu mroute [*ipaddress1*] [*ipaddress2*]

Syntax Description	[<i>ipaddress1</i>] [<i>ipaddress2</i>]	(Optional) Displays PXF mroute information for a particular group or range of groups.
---------------------------	--	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.

Examples

The following example shows PXF mroute information:

Router# **show pxf cpu mroute**

Shadow G/SG[5624]: s: 0.0.0.0 g: 224.0.1.40 uses: 0 bytes 0 flags: [D] LNJ

Interface	vcci	offset	rw_index	mac_header
-----------	------	--------	----------	------------

In :	0	0x000004		
------	---	----------	--	--

Shadow G/SG[3195]: s: 0.0.0.0 g: 234.5.6.7 uses: 0 bytes 0 flags: [5] NJ

Interface	vcci	offset	rw_index	mac_header
-----------	------	--------	----------	------------

In :	0	0x000008		
------	---	----------	--	--

Out: Cable5/1/0	5	0x00002C	1B	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/1/1	9	0x000028	1A	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/0/0	6	0x000024	19	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable5/0/0	3	0x000020	18	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/0/0	A	0x00001C	17	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/1/1	C	0x000018	16	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/1/0	B	0x000014	15	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/1/0	8	0x000010	14	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/0/1	7	0x00000C	13	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable5/0/1	4	0x000008	12	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

[Table 87](#) describes the fields shown in the display.

Table 87 *show pxf cpu mroute Field Descriptions*

Field	Description
Interface	Interface or subinterface.
vcci	Virtually Cool Common Index (VCCI) for the interface or subinterface.
rw index	Index used to read and write into the multicast table for this entry.
mac_header	MAC header that is used when rewriting the packet for output.

Related Commands

Command	Description
show ip mroute	Displays the Cisco IOS version of a multicast routing table entry.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu pbr action

To display policy-based routing (PBR) actions configured in the Parallel eXpress Forwarding (PXF), use the **show pxf cpu pbr action** command in privileged EXEC mode.

show pxf cpu pbr action *map-name*

Cisco 10000 Series Router (PRE3)

show pxf cpu pbr [**action** *map-name* | **tcam** *map-name* | **flex-sum**]

Syntax Description		
action <i>map-name</i>	(Optional) Displays PBR action information and redirects the command output to the route map you specify.	
tcam <i>map-name</i>	(Optional) Displays VMR (value, plus a mask and result) information stored in ternary content addressable memory (TCAM) and redirects the command output to the route map you specify.	
	Note This option is only available on the PRE3 for the Cisco 10000 series router.	
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the PXF engine for use by the flexible key construction microcode. This information is useful for design teams.	
	Note This option is only available on the PRE3 for the Cisco 10000 series router.	

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was introduced on the Cisco 10000 series router for the PRE2.
	12.2(31)SB2	This command was introduced on the Cisco 10000 series router for the PRE3.

Usage Guidelines This command is useful to determine if an adjacency has been found for a **set ip next-hop ip-address** route map configuration command.

Examples

The following example shows the PBR route maps configured in the PXF:

```
Router# show pxf cpu pbr action foo
```

```
Show PBR Action:
```

```
-----
Policy number: 1
route-map foo, permit, sequence 10
  map number      = 0
  action index    = 0
    primary action : SET_ROUTE
    secondary action : - none -
  mac-rewr index = 0x0000 0015
  vcci = 0x09D4, qos group = 0, tos prec = 0
  tt_pkt_count = 0          tt_byte_count = 0
Adjacency data 0x20D29968
XCM adjacency from 0x70000120(RP)
0xA0000120(FP) index 0x24:
```

Cisco 10000 Series Router (PRE3)

The following configuration example shows a PBR configuration in which traffic classification is based on the IP access list named `pbr_length`. The route map permits traffic based on the specified matching criteria and sets the next hop address of each packet.

```
ip access-list extended pbr_length
  permit tcp any any
!
route-map pbr_length permit 10
  match ip address pbr_length
  match length 100 200
  set ip next-hop 2.0.95.5          !
route-map pbr_length permit 20
  match ip address pbr_length
  match length 200 300
  set ip next-hop 2.0.95.5          !
route-map pbr_length permit 30
  match length 300 400
  set ip next-hop 2.0.95.5          !
```

The following sample output from the `show pxf cpu pbr` command shows the type of information that displays based on the above PBR configuration:

```
Router# show pxf cpu pbr action pbr_length
```

```
Show PBR Action:
```

```
-----
Policy number: 3

route-map pbr_length, permit, sequence 10
  map number      = 0
  action index    = 64
  map vcci out    = 0x0
  tt_pkt_count    = 0          tt_byte_count = 0

  primary action  : NULL_ACTION
  secondary action : - none -
  mac-rewr index = 0x0000 0000
  vcci = 0x0000, qos group = 0, tos prec = 0
.....

route-map pbr_length, permit, sequence 20
```

```

map number      = 1
action index    = 65
map vcci out    = 0x0
tt_pkt_count    = 0                tt_byte_count = 0

primary action   : NULL_ACTION
secondary action : - none -
mac-rewr index  = 0x0000 0000
vcci = 0x0000, qos group = 0, tos prec = 0

.....

route-map pbr_length, permit, sequence 30
map number      = 2
action index    = 66
map vcci out    = 0x0
tt_pkt_count    = 0                tt_byte_count = 0

primary action   : NULL_ACTION
secondary action : - none -
mac-rewr index  = 0x0000 0000
vcci = 0x0000, qos group = 0, tos prec = 0

```

The following sample output from the **show pxf cpu pbr tcam** command shows the type of detailed VMR (value, plus a mask and result) information that displays:

Router# **show pxf cpu pbr tcam pbr_length detail**

VMR data for Route-map pbr_length

```

-----
VMR Format - handle: 5050BC90
Format has 5 fields, refcount = 1
Field: Format, FIXED, start_bit = 69, end_bit = 71
Field: ACL index, FIXED, start_bit = 54, end_bit = 68
Field: Flags, FIXED, start_bit = 43, end_bit = 53
Field: L4 proto, FIXED CNV, start_bit = 16, end_bit = 23
Field: Unknown, FLEX, start_bit = 0, end_bit = 15 Total bits = 53, format = 72 GMR used: 0
Col 3 LKBP Vector: 96C
Status: Running

-----
VMRs
----- VMR 0 -----
V: 7000C000 00000600 70
M: FFFFD800 0000FFFF F0
R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000070/0000FFF0
----- VMR 1 -----
V: 7000C000 00000600 68
M: FFFFD800 0000FFFF F8
R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000068/0000FFF8
----- VMR 2 -----
V: 7000C000 00000600 64
M: FFFFD800 0000FFFF FC

```

```

R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000064/0000FFFC
.
.
.
----- VMR 18 -----
V: 7000C000 00000000 00
M: FFFFC000 00000000 00
R: 80000110
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000000/00000000
Flags: 00000000/00000000
Packet Length: 00000000/00000000

```

Related Commands

Command	Description
show pxf cpu policy-data	Displays QoS policy data index usage statistics.
show pxf cpu vcci	Displays VCCI to interface mapping information.

show pxf cpu police

To display all active policer policies in the Parallel eXpress Forwarding (PXF), including active interface and policing parameters, use the **show pxf cpu police** command in privileged EXEC mode.

show pxf cpu police [*policy-map-name*]

Syntax Description	<i>policy-map-name</i> (Optional) Policy for which you want to display PXF policing statistics.
---------------------------	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.

Usage Guidelines	If a policy name is not specified, the command displays policing statistics for all policy maps.
-------------------------	--

Examples	The following example shows the PXF policing statistics for a policy called policetest. The fields shown in the display are self-explanatory.
-----------------	---

```
Router# show pxf cpu police policetest
```

```
Policy policetest:
  Class: police_class
  Interface VCCI 0x9DD Output Policy:
    police 8000 8000 15000 conform-action transmit exceed-action drop violate-action drop

  Class: class-default
    *** No police action ***
```

Related Commands	Command	Description
	show pxf cpu vcci	Displays VCCI to interface mapping information.
	show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu policy-data

To display Parallel eXpress Forwarding (PXF) policy data index usage statistics, use the **show pxf cpu policy-data** command in privileged EXEC mode.

show pxf cpu policy-data

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.

Examples The following example shows PXF policy data which is information related to the number of classes in a policy and the reservation of unique indexes to support match statistics and token buckets. Policy data index statistics are related to free match statistics indexes. Exhaustion of these indexes means no more policies can be created in the router. Secondary policy data indexes are related to free token bucket indexes. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu policy-data

Service policy data index usage statistics:
Total groups = 9, pool_defragmented = TRUE.
  Group size      Chunk count
    1             0
    2             1
    4             1
    8             0
   16             1
   32             1
   64             1
  128             1
  256            1023
Total free count  = 262134.
Total chunk count = 262144.

Secondary policy data index usage statistics:
Total groups = 9, pool_defragmented = TRUE.
  Group size      Chunk count
    2             1
    4             1
    8             0
   16             1
   32             1
   64             1
  128             1
  256             1
  512            2047
Total free count  = 1048566.
Total chunk count = 1048576.
```

The Group size field is the number of policy classes. The Chunk count field is the number of blocks the group holds.

Related Commands	Command	Description
	show pxf cpu pbr action	Displays PBR actions configured in the PXF for all PBR route maps.
	show pxf cpu vcci	Displays VCCI to interface mapping information.

show pxf cpu qos

To display Parallel eXpress Forwarding (PXF) External Column Memory (XCM) contents related to a particular policy, use the **show pxf cpu qos** command in privileged EXEC mode.

show pxf cpu qos [**policy-map** *policy-name* | **vcci-maps**]

Cisco 10000 Series Router

show pxf cpu qos [*vcci* | **classifiers** | **flex-sum** | **policy-map** *policy-name* | **vcci-maps**]

Syntax Description

vcci	(Optional) Virtual Channel Circuit Identifier (VCCI). Information about this specified VCCI will be displayed.
classifiers	(Optional) Displays information about the criteria used to classify traffic.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the PXF engine for use by the flexible key construction microcode. Note This option is only available on the Cisco 10000 series router for the PRE3.
policy-map <i>policy-name</i>	(Optional) Displays per-policy map information.
vcci-maps	(Optional) Displays VCCI map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the Cisco 10000 series router for the PRE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

This command is useful in verifying the presence of a policy on interfaces and indexes programmed in the PXF.

Examples

The following example shows XCM contents related to a policy called police_test, which is defined as follows:

```
policy-map police_test
class high-priority
priority
class low-priority
set atm-clp
```



```

class class-default
  queue-limit 512

```

Router# **show pxf cpu qos police_test**

```

Output Polycmap: police_test
Vcci: A05  Flags: 4  Polycmap_index: 6  Polycmap_data_index: 12
OUT AT1/0/0.111 (0x71764660) ref_count 1
Output Action Table Contents for vcci 0xA05 - Polycmap index: 6
class-name: high-priority  class_index: 0  action_flags: 0x00
  srp_class_id: 0x01  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: low-priority  class_index: 1  action_flags: 0x10
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: class-default  class_index: 2  action_flags: 0x00
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0

```

Related Commands

Command	Description
show pxf cpu statistics qos	Displays match statistics for a service policy on an interface.

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

<i>interface</i>	(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.
<i>QID</i>	(Optional) The queue identifier.
summary	(Optional) Displays queue scaling information such as: <ul style="list-style-type: none"> • 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 **viX.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 broadband router for wideband cable or modular cable interfaces. The **ATM** interface output is not available for this router.

See [Table 88](#) for descriptions of the **interface** keyword fields.

Table 88 *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 Cisco 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 88 *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 queuing 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 (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
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 (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
131241	0/255	0	0	0	1/240	0	32881

* CIR Queues

QID	Len/Max	Dequeues	TailDrops	MinRt (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
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 VTMS links and link queues.
show pxf cpu statistics queue	Displays PXF CPU queueing counters for all interfaces.

show pxf cpu reasm_index

To display information about reassembly of IP fragmented packets in the Parallel eXpress Forwarding (PXF), use the **show pxf cpu reasm_index** command in privileged EXEC mode.

show pxf cpu reasm_index [summary]

Syntax Description	summary	(Optional) Displays summary reassembly information of IP fragmented packets in the PXF.
--------------------	---------	---

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.

Examples The following example shows reassembly summary information. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu reasm_index summary
```

```
Multilink Reassembly Index usage summary
```

```

Maximum  Used      Available
1251      0          1251
```

Related Commands	Command	Description
	ip virtual-reassembly	Enables VFR information on an interface.
	show ip virtual-reassembly	Displays VFR configuration and statistical information.

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)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
	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 .
	12.2(33)SCE	This command was modified in Cisco IOS Release 12.2(33)SCE. The cable-wan-ip keyword was removed.

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

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 89 describes the significant fields shown in the display.

Table 89 *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 semaphore collision (used for MLP).

Table 89 *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 Index	Match Number	Pkts Matched	Bytes 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	2606	Virtual-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 pxf cpu subblocks

To display Parallel eXpress Forwarding (PXF) CPU statistics for a bridged subinterface (encapsulation type), use the **show pxf cpu subblocks** command in privileged EXEC mode.

show pxf cpu subblocks *interface-name*

Syntax Description	<i>interface-name</i>	Name of the interface.
---------------------------	-----------------------	------------------------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2(28)SB	This command was introduced on the Cisco 10000 series router.
	12.3(14)T	This command was enhanced to display more information for all subblocks.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following example shows subblocks information for Gigabit Ethernet interface 7/0/0:

```
Router# show pxf cpu subblocks g7/0/0

GigabitEthernet7/0/0 is up
  ICB = 1C000, LinkId = 6, interface PXF, enabled
    link next_send:    0x37022604    channel number:    0
    link bandwidth mult: 33467          shift:          22
    link bandwidth mult: 33467          shift:          22
    link aggregate cir:  0x00000000    aggregate eir:    0x00000000
  IOS encapsulation type 1  ARPA
  Min mtu: 14      Max mtu: 1528
  VCCI mactable location = A3340000
  VCCI 9D3  (802.1Q VLAN 1)
    icmp ipaddress 0.0.0.0      timestamp 0
    fib_root 0x0, fib_root_rpf 0x0 cicb_flags 0x00, flags/netmask 0x02
  VCCI 9DB  (802.1Q VLAN 1)
    icmp ipaddress 0.0.0.0      timestamp 0
    fib_root 0x0, fib_root_rpf 0x0 cicb_flags 0x00, flags/netmask 0x02
```

The following example shows subblocks information for all interfaces:

```
Router# show pxf cpu subblocks PXF

Interface      Status  ICB   WQB_ID Fwding Enc VCCI-map VCCI VC
Control Plane  up      0     1      PXF    0   A3000000 1
ATM1/0/0       initiali 6000  3      disabl 33   A3040000 9CF
ATM1/0/1       initiali 6001  4      disabl 33   A3060000 9D0
ATM1/0/2       initiali 6002  5      disabl 33   A3080000 9D1
ATM1/0/3       initiali 6003  6      disabl 33   A30A0000 9D2
Serial2/0/0    initiali A000  7      disabl 16   A3000004 9D3
Serial2/0/1    initiali A001  8      disabl 16   A3000008 9D4
Serial2/0/2    initiali A002  9      disabl 5     A300000C 9D5
Serial2/0/3    initiali A800  10     disabl 5     A3000010 9D6
Serial2/0/4    initiali A801  11     disabl 5     A3000014 9D7
Serial2/0/5    initiali A802  12     disabl 5     A3000018 9D8
```

```

Serial2/0/6          initiali B000 13      disabl 5    A300001C 9D9
Serial2/0/7          initiali B001 14      disabl 5    A3000020 9DA
POS3/0/0             up        E000 15      PXF      5    A3000024 9DB
Serial4/0/0.1/1/1/1:0 up      12000 27     PXF     16    A3000040 9E7
Serial4/0/0.1/1/1/1:1 up      12001 28     PXF     16    A3000044 9E8
POS5/0/0             down     16000 16     disabl 5    A3000028 9DC
POS5/0/1             down     16001 17     disabl 5    A300002C 9DD
POS5/0/2             down     16002 18     disabl 5    A3000030 9DE
POS5/0/3             down     16003 19     disabl 5    A3000034 9DF
POS5/0/4             down     16004 20     disabl 5    A3000038 9E0
POS5/0/5             down     16005 21     disabl 5    A300003C 9E1
GigabitEthernet6/0/0 down     1A000 22     disabl 1    A32C0000 9E2 1
GigabitEthernet6/0/0.100 down 1A000 22     disabl 1    A32C0000 9EB 100
ATM8/0/0             up       22000 23     PXF     33    A33C0000 9E3
ATM8/0/0.1           up       22000 23     PXF     33    A33C0000 0   0/33
ATM8/0/0.2           up       22000 23     PXF     33    A33C0000 0   0/34
ATM8/0/0.100         up       22000 23     PXF     33    A33C0000 9EC 30/32
ATM8/0/0.200         up       22000 23     PXF     33    A33C0000 9ED 0/32
ATM8/0/1             down     22001 24     disabl 33   A33E0000 9E4
ATM8/0/2             down     22002 25     disabl 33   A3400000 9E5
ATM8/0/3             down     22003 26     disabl 33   A3420000 9E6
Multilink1           up        0    29     PXF     16    A3000048 2
Multilink2           down     0    36     disabl 16   A300005C 4
Multilink20          up        0    30     PXF     16    A300004C 3
Multilink60230       down     0    31     disabl 16   A3000050 9E9
Multilink60130       down     0    32     disabl 16   A3000054 9EA

```

Table 87 describes the fields shown in the display.

Table 90 *show pxf cpu subblocks Field Descriptions*

Field	Description
Interface	Identifies the interface or subinterface.
Status	Displays the status of the interface: <ul style="list-style-type: none"> Administ—The interface has been shut down and is in the administrative down state. Deleted—The subinterface has been removed from the router's configuration. Down—The interface is down because of a cable or other connectivity problem. Initiali—The interface is in the process of initializing. Reset—The interface is currently being reset. Up—The interface is up and passing traffic.
ICB	Displays the Interface Control Block (ICB) that is mapped to this interface.
WQB_ID	Displays the Work Queue Block (WQB) identifier for the interface.
Fwding	Displays whether traffic is being forwarded (PXF) or not (disable).

Table 90 *show pxf cpu subblocks Field Descriptions (continued)*

Field	Description
Enc	<p>Identifies the type of encapsulation used on the interface. The most common encapsulation types are:</p> <ul style="list-style-type: none"> 0 = None 1 = Ethernet ARPA 2 = Ethernet SAP 3 = 802.2 SNAP 5 = Serial, raw HDLC 8 = Serial, LAPB 9 = Serial, X.25 20 = Frame Relay 21 = SMDS 22 = MAC-level packets 27 = Logical Link Control (LLC) 2 28 = Serial, SDLC (primary) 30 = Async SLIP encapsulation 33 = ATM interface 35 = Frame Relay with IETF encapsulation 42 = Dialer encapsulation 46 = Loopback interface 51 = ISDN Q.921 59 = DOCSIS (previously known as MCNS) 61 = Transparent Mode 62 = TDM clear channel 64 = PPP over Frame Relay 65 = IEEE 802.1Q 67 = LAPB terminal adapter 68 = DOCSIS Cable Modem
VCCI-map	Displays the memory address for the Virtually Cool Common Index (VCCI) map table for this particular VCCI.
VCCI	Identifies the VCCI, in hexadecimal, assigned to the interface or subinterface.
VC	Identifies the virtual circuit (VC).

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
debug pxf	Displays PXF debugging output.
show ip mroute	Displays the contents of the IP multicast routing table.
show pxf cpu tbridge	Displays PXF CPU statistics for transparent bridging.
show pxf microcode	Displays identifying information for the microcode currently loaded on the PXF.

show pxf cpu vcci

To display Virtually Cool Common Index (VCCI) to interface mapping information on the Parallel eXpress Forwarding (PXF), use the **show pxf cpu vcci** command in privileged EXEC mode.

show pxf cpu vcci [summary]

Syntax Description	summary (Optional) Displays VCCI allocation information.
---------------------------	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.

Usage Guidelines	<p>The VCCI is an index that uniquely identifies each interface or subinterface in the PXF and it maps that interface to the appropriate set of services and features. This command is useful to verify the number of VCCIs that are used and available.</p> <p>The Cisco 10000 series router has 65,536 VCCIs. A VCCI is assigned to each individual routed interface. A VCCI is not assigned to virtual template interfaces and loopbacks.</p>
-------------------------	--

Examples	The following example shows how to display the number of used and available VCCIs. The fields shown in the display are self-explanatory.
-----------------	--

```
Router# show pxf cpu vcci summary

VCCI usage summary

          Maximum  Used    Available
Multilink VCCI   2500     0        2500
Other VCCI       63023   14       63009
```

Related Commands	Command	Description
	show pxf cpu policy-data	Displays QoS policy data index usage statistics.

show pxf crash

To display Parallel eXpress Forwarding (PXF) crash information, use the **show pxf crash** command in privileged EXEC mode.

show pxf crash

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.1(1)E	This command was introduced on the Cisco 10000 series router.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
	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.

Examples The following example shows crash information as a result of a PXF direct memory access (DMA) error. The PXF crash information is typically stored in bootflash.

```
Router# show pxf crash

Summary of bootflash:pxf_crashinfo_20060117-152035

Time of crash was 15:20:35 UTC Tue Jan 17 2006

PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted

Current microcode:
  file=system:pxf/c10k2-11-ucode.108.0.0.0,
  version=108.0.0.0,
  description=Nightly Build Software created Sat 19-Nov-05 00:12
```

[Table 89](#) describes the significant fields shown in the display.

Table 91 *show pxf crash Field Descriptions*

Field	Description
Summary of bootflash:	Displays the filename in bootflash where the PXF crash information is stored. The filename format includes the date and time of the PXF crash.
Time of crash	Displays the date of the PXF crash.

Table 91 *show pxf crash Field Descriptions (continued)*

Field	Description
UTC	Displays the Universal Coordinated Time (UTC) of the PXF crash.
Current microcode	Displays identifying information for the microcode currently running on the PXF.

Related Commands

Command	Description
show pxf statistics	Displays a summary of PXF statistics.

show pxf dma

To display the current state of direct memory access (DMA) buffers, error counters, and registers on the Parallel eXpress Forwarding (PXF), use the **show pxf dma** command in privileged EXEC mode.

show pxf dma [**buffers** | **counters** | **reassemble** | **registers**]

Cisco 10000 Series Router (PRE3 only)

show pxf dma [**buffers** | **counters** | **reassemble** | **registers**] [**brief** | **config** | **errors** | **status**]

Syntax Description	
buffers	(Optional) Displays PXF DMA buffers information.
counters	(Optional) Displays packet and error counters for the PXF DMA engine.
reassemble	(Optional) Displays PXF reassembly table usage information.
registers	(Optional) Displays PXF DMA registers information.
brief	(Optional) Displays PXF DMA information, including the initialization state of each block in the PXF API and any errors that occurred. Note This option is available on the PRE3 only.
config	(Optional) Displays a configuration summary of the registers in each of the PXF DMA blocks. Note This option is available on the PRE3 only.
errors	(Optional) Displays the errors that occurred in each of the PXF DMA blocks. Note This option is available on the PRE3 only.
status	(Optional) Displays the initialization state of each PXF DMA block. In normal operation, all blocks display the enabled state. Note This option is available on the PRE3 only.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series router for the PRE2.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router for the PRE3.

Examples

The following example shows PXF DMA buffers information:

Router# **show pxf dma buffers**

PXF To-RP DMA Ring Descriptors & Buffers:

	Descriptor Address	Buffer Address	Buffer Length(b)	Descriptor Flags
0	0x0CA06340	0x0AC097C0	512	0x0002
1	0x0CA06350	0x0AC088C0	512	0x0002
2	0x0CA06360	0x0AC07C40	512	0x0002
3	0x0CA06370	0x0AC0B5C0	512	0x0002
4	0x0CA06380	0x0AC0CC40	512	0x0002
5	0x0CA06390	0x0AC08640	512	0x0002
6	0x0CA063A0	0x0AC0C240	512	0x0002
7	0x0CA063B0	0x0AC08B40	512	0x0002
8	0x0CA063C0	0x0AC0AE40	512	0x0002
9	0x0CA063D0	0x0AC0BAC0	512	0x0002
10	0x0CA063E0	0x0AC0C9C0	512	0x0002
11	0x0CA063F0	0x0AC09CC0	512	0x0002
12	0x0CA06400	0x0AC0C740	512	0x0002
13	0x0CA06410	0x0AC0A6C0	512	0x0002
14	0x0CA06420	0x0AC0B0C0	512	0x0002
15	0x0CA06430	0x0AC09040	512	0x0002
16	0x0CA06440	0x0AC0A440	512	0x0002
17	0x0CA06450	0x0AC065C0	512	0x0002
18	0x0CA06460	0x0AC06FC0	512	0x0002
19	0x0CA06470	0x0AC06340	512	0x0002
20	0x0CA06480	0x0AC07240	512	0x0002
21	0x0CA06490	0x0AC092C0	512	0x0002
22	0x0CA064A0	0x0AC0D140	512	0x0002
23	0x0CA064B0	0x0AC0C4C0	512	0x0002
24	0x0CA064C0	0x0AC07740	512	0x0002
25	0x0CA064D0	0x0AC09540	512	0x0002
26	0x0CA064E0	0x0AC0A940	512	0x0002
27	0x0CA064F0	0x0AC06840	512	0x0002
28	0x0CA06500	0x0AC08140	512	0x0002
29	0x0CA06510	0x0AC06D40	512	0x0002
30	0x0CA06520	0x0AC07EC0	512	0x0002
31	0x0CA06530	0x0AC0ABC0	512	0x0003

PXF From-RP DMA Ring Descriptors & Buffers:

	Descriptor Address	Buffer Address	Buffer Length(b)	Descriptor Flags	Context Bit
0	0x0CA06580	0x00000000	0	0x0000	Not set
1	0x0CA06590	0x00000000	0	0x0000	Not set
2	0x0CA065A0	0x00000000	0	0x0000	Not set
3	0x0CA065B0	0x00000000	0	0x0000	Not set
4	0x0CA065C0	0x00000000	0	0x0000	Not set
5	0x0CA065D0	0x00000000	0	0x0000	Not set
6	0x0CA065E0	0x00000000	0	0x0000	Not set
7	0x0CA065F0	0x00000000	0	0x0000	Not set
8	0x0CA06600	0x00000000	0	0x0000	Not set
9	0x0CA06610	0x00000000	0	0x0000	Not set
10	0x0CA06620	0x00000000	0	0x0000	Not set
11	0x0CA06630	0x00000000	0	0x0000	Not set
12	0x0CA06640	0x00000000	0	0x0000	Not set
13	0x0CA06650	0x00000000	0	0x0000	Not set
14	0x0CA06660	0x00000000	0	0x0000	Not set
15	0x0CA06670	0x00000000	0	0x0001	Not set

Table 87 describes the fields shown in the display.

Table 92 *show pxf dma Field Descriptions*

Field	Description
Descriptor Address	Memory address pointing to the descriptor for this buffer.
Buffer Address	Address of this buffer in memory.
Buffer Length	Length, in bytes, of this particular buffer.
Descriptor Flags	Internal flags identifying this buffer's use and status.
Context Bit	State of the context bit which is set when the buffer is currently in use by a context (the basic unit of packet processing).

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu	Displays PXF CPU statistics.
show pxf microcode	Displays the microcode version running on the PXF.

show pxf feature cef

To display Parallel eXpress Forwarding (PXF) routing feature tables for Cisco Express Forwarding, use the **show pxf feature cef** command in user EXEC or privileged EXEC mode.

show pxf feature cef *entry*

Syntax Description

<i>entry</i>	Display the PXF entry.
--------------	------------------------

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Examples

The following is sample output from the **show pxf feature cef** command. The fields shown in the display are self-explanatory.

Router# **show pxf feature cef entry**

```
Shadow 16-4-4-8 PXF Mtrie:
  41 leaves, 1968 leaf bytes, 15 nodes, 267000 node bytes
  5 invalidations
  46 prefix updates
  refcounts: 66746 leaf, 66720 node
```

Prefix/Length	Refcount	Parent
0.0.0.0/0	62282	
0.0.0.0/32	3	0.0.0.0/0
171.22.12.128/27	34	0.0.0.0/0
171.22.12.128/32	3	171.22.12.128/27
171.22.12.129/32	3	171.22.12.128/27
171.22.12.130/32	3	171.22.12.128/27
171.22.12.131/32	3	171.22.12.128/27
171.22.12.147/32	3	171.22.12.128/27

Related Commands

Command	Description
show pxf feature nat	Displays PXF routing feature tables for NAT.

show pxf feature cef vrf

To display the routing feature tables for Virtual Private Network (VPN) routing and forwarding instances (VRFs) on the Parallel eXpress Forwarding (PXF) path, use the **show pxf feature cef vrf** command in privileged EXEC mode.

show pxf feature cef vrf *vpn-name*

Syntax Description	<i>vpn-name</i>	Name of the VPN to display.
--------------------	-----------------	-----------------------------

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.2(15)B	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines	Use this command to display VRF PXF routing feature tables for a specified VPN for Cisco Express Forwarding. This command also displays information about prefix and MTRIE resource usage.
------------------	--

Examples	The following is sample output for the show pxf feature cef vrf command when it is used to display information about VRF vpn1:
----------	---

Router# **show pxf feature cef vrf vpn1**

```
Shadow 8-8-4-4-8 PXF Mtrie:
  51 leaves, 2448 leaf bytes, 92 nodes, 56352 node bytes
  10 invalidations
  61 prefix updates
  refcounts: 3666 leaf, 3733 node
```

Prefix/Length	Refcount	Parent	Address	Shadow
0.0.0.0/32	3		0xC0047218	0x62CAF2E8
10.5.0.0/16	558		0xC0047278	0x62CAF108
10.5.0.0/32	3	10.5.0.0/16	0xC0047268	0x62CAEE08
10.5.0.1/32	3	10.5.0.0/16	0xC0047260	0x62CAEA18
10.5.0.2/32	3	10.5.0.0/16	0xC0047388	0x62CAEA48
10.5.0.255/32	3	10.5.0.0/16	0xC0047270	0x62CAF0D8
10.30.1.0/16	288		0xC0047360	0x62CAEB38
10.30.1.1/32	3	10.30.1.0/16	0xC0047350	0x62CAEB98
10.70.0.0/32	3		0xC00472C0	0x62CAEEF8
10.70.1.1/32	3		0xC0047358	0x62CAEB68
10.70.1.2/32	3		0xC0047368	0x62CAEB08
10.70.1.3/32	3		0xC0047370	0x62CAEAD8
10.70.1.4/32	3		0xC0047378	0x62CAEA88
70.1.1.5/32	3		0xC0047380	0x62CAEA78
224.0.0.0/24	3		0xC0047228	0x62CAF288
255.255.255.255/32	3		0xC0047220	0x62CAF2B8

=====

5 routes with less specific overlapping parent route

Table 93 describes the significant fields shown in the display.

Table 93 *show pxf feature cef vrf Field Descriptions*

Field	Description
Shadow 8-8-4-4-8 PXF Mtrie	MTRIE lookup table index structures.
51 leaves	All created leaves for all MTRIEs.
2448 leaf bytes	Leaf byte counter. When a new leaf is created, the leaf byte counter is incremented by the size of the leaf structure.
92 nodes	All created nodes for all MTRIEs.
56352 node bytes	Node byte counter. When a new node is created, the node byte counter is incremented.
10 invalidations	Invalidations counter. When a route (represented by a leaf) is deleted from an MTRIE, the invalidations counter is incremented. This counter includes all MTRIEs.
61 prefix updates	IP prefix counter. When an IP prefix (represented by a leaf) is added to the MTRIE, the IP prefix counter is incremented. This counter includes all MTRIEs.
refcounts	Counters associated with references between leaves.
3666 leaf	MTRIEs have a leaf lock and a leaf free function. The leaf lock function increments the leaf refcount. The leaf free function decrements the leaf refcount. The leaf lock and leaf free functions prevent a leaf from being freed (deleted) while the leaf is still being referenced. This counter includes all MTRIEs.
3733 node	Node counter. When a child node is added to another node, the node to which the child node is added becomes a parent node. The node counter is decremented when a child node is deleted. This counter includes all MTRIEs.
Prefix/Length	The IP address and subnet mask of a leaf.
Refcount	The number of leaves that reference a specified leaf. The refcount counter is incremented when the leaf lock function is called and decremented when the leaf free function is called.
Parent	When you add a less specific route to a more specific route, the more specific route has a back pointer that points to the less specific route.
Address	The address of the memory for the specified leaf.
Shadow	The shadow address in Route Processor memory for the specified leaf.

Related Commands

Command	Description
show pxf feature cef	Displays PXF routing feature tables for CEF.
show pxf feature nat	Displays PXF routing feature tables for NAT.

show pxf feature nat

To display Parallel eXpress Forwarding (PXF) routing tables for Network Address Translation (NAT), use the **show pxf feature nat** command in user EXEC or privileged EXEC mode.

show pxf feature nat [**entry** | **stat** | **tcp**]

Syntax Description	entry	Displays NAT information.
	stat	Displays NAT processing information.
	tcp	Displays NAT TCP logging information.

Command Modes	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Examples The following is sample output from the **show pxf feature nat** command. The fields shown in the display are self-explanatory.

Router# **show pxf feature nat**

```

--- 171.22.12.175      192.168.0.129      ---      ---
--- 171.22.12.163      192.168.0.7        ---      ---
--- 171.22.12.161      192.168.0.13       ---      ---
--- 171.22.12.162      192.168.0.3        ---      ---
--- 171.22.12.165      192.168.0.8        ---      ---
--- 171.22.12.168      192.168.0.14       ---      ---
--- 171.22.12.170      192.168.0.12       ---      ---
--- 171.22.12.166      192.168.0.15       ---      ---
--- 171.22.12.164      192.168.0.16       ---      ---

```

Related Commands	Command	Description
	show pxf feature cef	Displays PXF routing feature tables for Cisco Express Forwarding.

show pxf interface

To display a summary of the interfaces on the router and the Parallel eXpress Forwarding (PXF) features and capabilities enabled on these interfaces, use the **show pxf interface** command in privileged EXEC mode.

```
show pxf interface interface-name [detail]
```

Syntax Description	<i>interface-name</i>	Name of the interface.
	detail	(Optional) Displays detailed information for all PXF interfaces on the router.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	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.

Usage Guidelines If you do not specify an interface, the command displays a summary of the statistics for all PXF interfaces on the router.

Examples The following example shows PXF statistics for serial interface 1/0/0. The significant fields shown in the display are self-explanatory.

```
Router# show pxf interface s1/0/0

ed10#sho pxf interface s1/0/0
Serial1/0/0 is up, enabled, PXF enabled, IOS encap PPP      (16)
  Last clearing of Serial1/0/0 counters: 00:06:29
    91 packets input, (1934 bytes)

Total PXF input errors (pkts/bytes):           0/0

PXF output queues:
      Class      ID    Length/Max    Outputs (pkts/bytes)    Drops
    0 class-default  276    0/1024         0/0                0
    15              -   275    0/32        91/1953                0

Slot 1/0:  FBB Rx:0x00000000 OCQ debug:0x00001040, qN_entry_cnt[5:0]: 0
           PXF DMA RE drops: 0/0, Null config drops: 0/0
           Last clearing of slot 1/0 counters: 00:06:29
```

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf microcode

To display identifying information for the microcode currently loaded on the Parallel eXpress Forwarding (PXF), use the **show pxf microcode** command in privileged EXEC mode.

show pxf microcode

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples The following example shows the microcode version that is currently loaded on the PXF:

```
Router# show pxf microcode

PXF complex: 4 Toasters 8 Columns total
PXF processor tmc0 is running.
PXF processor tmc1 is running.
PXF processor tmc2 is running.
PXF processor tmc3 is running.

Loaded microcode: system:pxf/c10k2-11-ucode.6.1.3
    Version: 6.1.3
    Release Software created Sun 20-Nov-05 14:06
    Signature: 0d2b395c1083872793586f9cec47d7b3
    Microcode load attempted 1 time(s), latest 2w6d ago
    tmc0 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc1 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc2 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc3 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=154
```

[Table 94](#) describes the fields shown in the display.

Table 94 *show pxf microcode Field Descriptions*

Field	Description
PXF complex	The number of PXF processors, their associate memory columns, and their current status.
Loaded microcode	The source and filename for the microcode that is currently loaded on the PXF processor.
Version	The microcode version.

Table 94 *show pxf microcode Field Descriptions (continued)*

Field	Description
Release Software created	The time and date the current microcode was compiled.
Signature	The signature in the microcode version.
Microcode load attempted	The number of times the PXF processor has loaded the microcode since the Cisco IOS image was loaded at system boot. Also, shows the time (in days and hours) since the last successful load of the microcode.
tmc#	The current program counters and configuration for the PXF processors.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf dma	Displays PXF DMA information.

show pxf netflow

To display the NetFlow Parallel eXpress Forwarding (PXF) counters, use the **show pxf netflow** command in privileged EXEC mode.

show pxf netflow

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples	The following example shows the NetFlow PXF statistics. The fields shown in the display are self-explanatory.
-----------------	---

```
Router# show pxf netflow

NetFlow debug counters
  timeout activity:    0
  timeout inactivity: 9785
  forced age:         0
  export busy:        1
  export locked:      62
  export noswap:      2
  accumulate:         1296898
  new flow:           9808

(unreliable) ICM counters
  records pending :   0
  live flows :       0

NetFlow PXF Config Registers
  PXF Inactive Timeout: 90000
  PXF Active Timeout:  90000
```

Related Commands	Command	Description
	show pxf cpu statistics	Displays PXF CPU statistics.
	show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf stall-monitoring

To display the configuration and operating status details of the PXF stall monitor (PSM), use the **show pxf stall-monitoring** command in privileged EXEC mode. The **show pxf stall-monitoring** command also displays the number of stalls on the PSM after it was last enabled.

```
show pxf stall-monitoring [counters | reset { active-status | cob-fib | cob-tib | pxf-drop } subslot
sub-slot]
```

Syntax Description		
counters		Displays statistical information for all counters.
reset		Displays the following counters:
		<ul style="list-style-type: none"> active-status—Displays the active status on the specified subslot. cob-fib—Displays the Cobalt FIB counter on the specified subslot. cob-tib—Displays the Cobalt TIB counter on the specified subslot. pxf-drop—Displays the PXF per RSRC drop counter on the specified subslot. subslot sub slot—Displays information about the specified subslot.

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.2(33)XNE	This command was introduced.

Examples The following example displays a sample output of the **show pxf stall-monitoring** command:

```
Router# show pxf stall-monitoring

pxf stall-monitoring : Enabled
Stall History
=====
Stall Threshold Configuration
=====
Primary Action = LC-reset Threshold = 3 (default)
Primary Action = HT-reset Threshold = 3 (default)

Secondary action = SSO SwitchOverRouter#
```

The fields displayed are self-explanatory.

The following example displays a sample output of the **show pxf stall-monitoring counters** command:

```
Router# show pxf stall-monitoring counters

To RP Counters
=====
IOS To RP Counter = 20665
PXF To RP Drop Counter = 0
Current Counter Values
```

```

=====
Slot 0 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 0 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 1 Subslot 0 Cob TIB = 2368 Cob FIB = 0 PXF Drop = 0
Slot 1 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 2 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 2 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 3 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 3 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 4 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 4 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 5 Subslot 0 Cob TIB = 6162 Cob FIB = 6204 PXF Drop = 0
Slot 5 Subslot 1 Cob TIB = 6101 Cob FIB = 6065 PXF Drop = 0
Slot 5 Subslot 2 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 5 Subslot 3 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 7 Subslot 0 Cob TIB = 8402 Cob FIB = 8402 PXF Drop = 0
Slot 7 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 8 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 8 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Line Card Participant Status
=====
Slot 1 Subslot 0 = 1
Slot 1 Subslot 1 = 0
Slot 2 Subslot 0 = 0
Slot 2 Subslot 1 = 0
Slot 3 Subslot 0 = 0
Slot 3 Subslot 1 = 0
Slot 4 Subslot 0 = 0
Slot 4 Subslot 1 = 0
Slot 5 Subslot 0 = 0
Slot 5 Subslot 1 = 1
Slot 5 Subslot 2 = 0
Slot 5 Subslot 3 = 0
Slot 7 Subslot 0 = 1
Slot 7 Subslot 1 = 0
Slot 8 Subslot 0 = 1
Slot 8 Subslot 1 = 0
Line Card Active Status
=====
Slot 1 Subslot 0 = 0
Slot 1 Subslot 1 = 0
Slot 2 Subslot 0 = 0
Slot 2 Subslot 1 = 0
Slot 3 Subslot 0 = 0
Slot 3 Subslot 1 = 0
Slot 4 Subslot 0 = 0
Slot 4 Subslot 1 = 0
Slot 5 Subslot 0 = 0
Slot 5 Subslot 1 = 1
Slot 5 Subslot 2 = 0
Slot 5 Subslot 3 = 0
Slot 7 Subslot 0 = 0
Slot 7 Subslot 1 = 0
Slot 8 Subslot 0 = 0
Slot 8 Subslot 1 = 0

```

The fields displayed are self-explanatory.

The following example displays a sample output of the **show pxf stall-monitoring reset** command:

```

Router# show pxf stall-monitoring reset active-status subslot 1/0

pxf stall-monitoring : Enabled
0

```

Related Commands

Command	Description
hw-module pxf stall-monitoring	Enables PXF stall monitor on the Cisco 10000 series router and configures default threshold values before the LC and HTDP resets.

show pxf statistics

To display summary Parallel eXpress Forwarding (PXF) statistics, use the **show pxf statistics** command in privileged EXEC mode.

show pxf statistics { context | diversion | drop [detail] | ip | ipv6 }

Syntax Description		
	context	Displays context statistics.
	diversion	Displays traffic diverted from the PXF.
	drop [detail]	Displays packets dropped by the PXF. The detail option provides detailed information.
	ip	Displays IP and ICMP statistics.
	ipv6	Displays IPv6 statistics.

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.0(22)S	This command was introduced on the Cisco 10000 series router.
	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.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following example shows a summary of PXF IP statistics:

```
Router# show pxf statistics ip

Chassis-wide PXF forwarding counts
  IP inputs 0, forwarded 0, punted 0
  IP dropped 0, no adjacency 0, no route 0
  IP unicast RPF 0, unresolved 0

  ICMP created 0, Unreachable sent 0, TTL expired sent 0
  ICMP echo requests 0, replies sent 0
  ICMP checksum errors 0

  IP packets fragmented 0, total fragments 0, failed 0
  IP don't-fragment 0, multicast don't-fragment 0

  IP mcast total 0, switched 0, punted 0, failed 0
  IP mcast drops 0, RPF 0, input ACL 0, output ACL + taildrops 0
Last clearing of PXF forwarding counters:never
```

The following example shows a summary of PXF statistics for dropped packets:

```
Router# show pxf statistics drop

PXF input drops:
  Unassigned drops (pkts/bytes):                0/0
Last clearing of drop counters: never
```

The following example shows detailed PXF statistics for dropped packets:

Router# **show pxf statistics drop detail**

PXF input drops:

Unassigned drops (pkts/bytes): 0/0

PXF Unassigned input drop details:

(These input drops are not assigned to a particular PXF interface.)

	packets	bytes
generic	0	0
mpls_no_eos	0	0
fib_zero_dest	0	0
fib_drop_null	0	0
fib_icmp_no_adj	0	0
fib_icmp_bcast_dst	0	0
mfib_ttl_0	0	0
mfib_disabled	0	0
mfib_rpf_failed	0	0
mfib_null_oif	0	0
tfib_rp_flag	0	0
tfib_eos_violation	0	0
tfib_nonip_expose	0	0
tfib_label_invalid	0	0
tfib_path_unknown	0	0
tfib_nonip_ttl_exp	0	0
icmp_unrch_interval	0	0
icmp_on_icmp	0	0
icmp_bad_hdr	0	0
icmp_multicast	0	0
icmp_frag	0	0
macr_bad_tag_num	0	0
no_touch	0	0
eng_id_0	0	0
no_pkt_handles	0	0
l2_unsupp_drop	0	0
ipm_replay_full	0	0
bad_atm_arp	0	0
nested_fragmentation	0	0
l2less drop packets	0	0
l2tp_payload_encap	0	0
re_bit[00]	0	0
[01]	0	0
[02]	0	0
[03]	0	0
[04]	0	0
[05]	0	0
[06]	0	0
[07]	0	0
[08]	0	0
[09]	0	0
[10]	0	0

.
.
.

The following example shows summarized statistics for traffic diverted from the PXF:

Router# **show pxf statistics diversion**

```

Diversion Cause Stats:
  divert      = 0
  encap       = 0
  clns_isis   = 0
  clns        = 0
  cdp         = 0
  cgmpp       = 0
  arp         = 1
  rarp        = 0
  mpls_ctl    = 0
  keepalive   = 0
  ppp_cntrl   = 449
  fr_lmi      = 0
  atm ilmi    = 0
  oam f4      = 0
  oam f5 ete  = 0
  oam f5 seg  = 0
  mlfr lip    = 0
.
.
.
```

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu statistics	Displays PXF CPU statistics.

show pxf xcm

To display Parallel eXpress Forwarding (PXF) External Column Memory (XCM) information, use the **show pxf xcm** command in privileged EXEC mode.

show pxf xcm

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples The following example shows XCM information for each PXF processor:

```
Router# show pxf xcm

Toaster 0:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
  XCM1 type:FCRAM, size = 67108864
  ECC is enabled for column 1
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
Toaster 1:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
```

```

XCM0 type:FCRAM, size = 67108864
ECC is enabled for column 0
  XCM AB Config Register: 0x024703B9
  XCM CD Config Register: 0x024703B9
  XCM Exception Type Register: 0x00000000
  FCRAM-A Counters
    Number of ECC single bit errors: 0
  FCRAM-B Counters
    Number of ECC single bit errors: 0
  FCRAM-C Counters
    Number of ECC single bit errors: 0
  FCRAM-D Counters
    Number of ECC single bit errors: 0
XCM1 type:FCRAM, size = 67108864
ECC is enabled for column 1
  XCM AB Config Register: 0x024703B9
  XCM CD Config Register: 0x024703B9
  XCM Exception Type Register: 0x00000000
  FCRAM-A Counters
    Number of ECC single bit errors: 0

  FCRAM-B Counters
    Number of ECC single bit errors: 0
  FCRAM-C Counters
    Number of ECC single bit errors: 0
  FCRAM-D Counters
    Number of ECC single bit errors: 0
Toaster 2:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
  XCM1 type:FCRAM, size = 67108864
  ECC is enabled for column 1
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
Toaster 3:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9

```



```

XCM CD Config Register: 0x024703B9
XCM Exception Type Register: 0x00000000
FCRAM-A Counters
Number of ECC single bit errors: 0
FCRAM-B Counters
Number of ECC single bit errors: 0
FCRAM-C Counters
Number of ECC single bit errors: 0
FCRAM-D Counters
Number of ECC single bit errors: 0
XCM1 type:FCRAM, size = 67108864
ECC is enabled for column 1
XCM AB Config Register: 0x024703B9
XCM CD Config Register: 0x024703B9
XCM Exception Type Register: 0x00000000
FCRAM-A Counters
Number of ECC single bit errors: 0
FCRAM-B Counters
Number of ECC single bit errors: 0
FCRAM-C Counters
Number of ECC single bit errors: 0
FCRAM-D Counters
Number of ECC single bit errors: 0

```

Table 95 describes the fields shown in the display.

Table 95 *show pxf xcm Field Descriptions*

Field	Description
The following fields appear for each PXF processor.	
Toaster #	Identifies the PXF processor.
Number of Columns	Displays the number of memory columns on the PXF processor.
Proc ID	Displays the processor type (TMC is Toaster Memory Column).
ASIC Revision	Displays the internal version number of the PXF processor.
The following fields appear for each XCM memory column.	
XCM type	Displays the type and size, in bytes, of memory used in this particular column.
ECC is enabled for column	Displays whether Error Code Correction (ECC) checking is enabled or disabled for this memory column.
XCM Config Register and XCM Exception Type Register	Displays the contents of these two registers for the memory column.
Number of ECC single bit errors	Displays the number of single-bit errors detected in memory.

Related Commands

Command	Description
show pxf cpu	Displays PXF CPU statistics.
show pxf microcode	Displays the microcode version currently loaded on the PXF.

show route-map ipc

To display counts of the one-way route map interprocess communication (IPC) messages sent from the rendezvous point (RP) to the Versatile Interface Processor (VIP) when NetFlow policy routing is configured, use the **show route-map ipc** command in privileged EXEC mode.

show route-map ipc

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.0(3)T	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.

Usage Guidelines This command displays the counts of one-way route map IPC messages from the RP to the VIP when NetFlow policy routing is configured. If you execute this command on the RP, the messages are shown as “Sent.” If you execute this command on the VIP console, the IPC messages are shown as “Received.”

Examples The following is sample output of the **show route-map ipc** command when it is executed on the RP:

```
Router# show route-map ipc

Route-map RP IPC Config Updates Sent
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

The following is sample output of the **show route-map ipc** command when it is executed on the VIP:

```
Router# show route-map ipc

Route-map LC IPC Config Updates Received
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

Table 96 describes the significant fields shown in the display.

Table 96 *show route-map ipc Field Descriptions*

Field	Description
Route-map RP IPC Config Updates Sent	Indicates that IPC messages are being sent from the RP to the VIP.
Name	Number of IPC messages sent about the name of the route map.
Match access-list	Number of IPC messages sent about the access list.
Match length	Number of IPC messages sent about the length to match.
Set precedence	Number of IPC messages sent about the precedence.
Set tos	Number of IPC messages sent about the type of service (ToS).
Set nexthop	Number of IPC messages sent about the next hop.
Set interface	Number of IPC messages sent about the interface.
Set default nexthop	Number of IPC messages sent about the default next hop.
Set default interface	Number of IPC messages sent about the default interface.
Clean all	Number of IPC messages sent about clearing the policy routing configuration from the VIP. When dCEF is disabled and reenabled, the configuration related to policy routing must be removed (cleaned) from the VIP before the new information is downloaded from the RP to the VIP.

Related Commands

Command	Description
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to that next hop.

show xdr

To display details about eXternal Data Representation (XDR), use the **show xdr** command in user EXEC or privileged EXEC mode.

```
show xdr {client {client-name | all} [statistics] | linecard [linecard-number] [internal] |
          multicast-group | timers}
```

Syntax Description	<div> client {<i>client-name</i> all} Displays client basic information or statistics for a client or all clients. </div> <div> statistics (Optional) Displays XDR statistics. </div> <div> linecard (Line cards only) (Route/Switch Processor (RSP) on Cisco 7500 series and Route Processor (RP) on Cisco 10000 series) Displays XDR information for all XDR line card peer instances or the specified XDR line card peer instance. </div> <div> <i>linecard-number</i> (Optional) Specifies the line card slot number. </div> <div> internal (Optional) (RSP only) Displays internal information. </div> <div> multicast-group Displays XDR multicast groups. </div> <div> timers Displays XDR timers. </div>
--------------------	---

Command Default XDR details are not displayed.

Command Modes
User EXEC (>)
Privileged EXEC (#)

Command History	<div> <div>Release</div> <div>Modification</div> </div> <div> 12.2(25)S This command was introduced. </div> <div> 12.2(28)SB This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers. </div> <div> 12.2(33)SRA This command was integrated into Cisco IOS Release 12.2(33)SRA. </div> <div> 12.2(33)SXH This command was integrated into Cisco IOS Release 12.2(33)SXH. </div> <div> 12.4(20)T This command was integrated into Cisco IOS Release 12.4(20)T. </div>
-----------------	---

Usage Guidelines
This command is available only on distributed platforms (such as the Cisco 7500 series) and on the Cisco 10000 series routers.

Examples
The following example shows how to display XDR information for all clients:

```
Router# show xdr client all

XDR Interrupt P(0) flag:1 decode:0x413B9804 pull:0x413B9AE8 context:8
XDR Process Pri(1) flag:1 decode:0x413B99A0 pull:0x413B9D3C context:6
FIBHWIDB broker(2) flag:1 decode:0x0 pull:0x413A7B7C context:2
```

```

FIBIDB broker (3) flag:1 decode:0x0 pull:0x413A844C context:2
FIBHWIDB Subblo(4) flag:1 decode:0x0 pull:0x413A8E20 context:2
FIBIDB Subblock(5) flag:1 decode:0x0 pull:0x413A97DC context:2
XDR High Queue (6) flag:3 decode:0x4031AFC pull:0x4031B934 context:1
Adjacency updat(7) flag:1 decode:0x413B266C pull:0x413B261C context:2
XDR Medium Queue(8) flag:3 decode:0x4031B004 pull:0x4031B95C context:1
IPv4 table brok(9) flag:1 decode:0x0 pull:0x413B21F0 context:6
IPv6 table brok(10) flag:1 decode:0x0 pull:0x413ECA90 context:6
XDR Low Queue (11) flag:3 decode:0x4031B00C pull:0x4031B984 context:1
MFI RP Pull (12) flag:1 decode:0x0 pull:0x413E1174 context:1
Push Client One(13) flag:1 decode:0x413BA300 pull:0x0 context:4
CEF push (14) flag:1 decode:0x413A3D74 pull:0x0 context:124
MFI non-RP Push(15) flag:1 decode:0x413DFA34 pull:0x0 context:4
XDR ping (16) flag:1 decode:0x413BABB4 pull:0x0 context:1

```

The following example shows how to display XDR information for all XDR line card peer instances:

```
Router# show xdr linecard
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send      21
  Maximum sequence number expected 36

XDR slot number 2, status PEER UP
  IPC messages sent 52
  Next sequence number to send      31
  Maximum sequence number expected 46

XDR slot number 3, status PEER UP
  IPC messages sent 55
  Next sequence number to send      17
  Maximum sequence number expected 32

```

The following example shows how to display XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send      21
  Maximum sequence number expected 36

```

The following example shows how to display internal XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1 internal
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send      21
  Maximum sequence number expected 36

```

	Tx	bytes	Rx	bytes	
XDR Interrupt Priority:					
	0	0	2391	11955	Window Message
	21	336	0	0	Time Message
	2	8	0	0	Resequenece Message
	0	0	1	6	CEF LC state
XDR Process Priority:					
	0	0	1	3	Registration Signal
	2	10	0	0	CEF running
FIBHWIDB broker :					
	90	33570	0	0	fibhwwidb update

```

FIBIDB broker      :
      80      30960      0      0      fibidb update
FIBIDB Subblock brok:
      10      315      0      0      fibswsb update
Adjacency update   :
      2       6       0      0      Adjacency update me
      3       9       0      0      Adjacency repopulat
IPv4 table broker  :
      16      558      0      0      prefix
      4       24      0      0      epoch
      2       36      0      0      table
      4       44      0      0      multicast prefix
IPv6 table broker  :
      1       18      0      0      table
CEF push           :
      12      72      19     114     repopulation req
      0       0       1      12     isl table update rq
      0       0       1      12     dot1q table updateq
      2      10       0      0      state
      9     452       0      0      control
      1       3       0      0      flow features deace
      1      22       0      0      flow cache config
      1      40       0      0      flow export config
      6     470       0      0      access-list config
      2      10       0      0      access-list delete
      1      12       0      0      route-map
      1      16       0      0      icmp limit
      1       8       0      0      SSM RP to LC commas
XDR ping           :
      3      12      3      12     ping message

```

The following is sample output from the **show xdr multicast-group** command:

```

Router# show xdr multicast-group

0x4300DC00  READY      Window: 15  Linecards: 2
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

0x4414BC60  READY      Window: 15  Linecards: 1
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

0x44159420  READY      Window: 15  Linecards: 3
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

```

The following is sample output from the **show xdr timers** command:

```

Router# show xdr timers

XDR multicast timers
  Expiration      Type
  |      0.000    (parent)

XDR RP ping timers
  Expiration      Type
  |      0.000    (parent)

XDR RP timers
  Expiration      Type

```

```

|      1:19.236  (parent)
|      1:19.236   Sending Time
|      4:59.236   Keepalive timer slot: 2
|      4:59.236   Keepalive timer slot: 1
|      4:59.248   Keepalive timer slot: 3

```

Cisco 10000 Series Router Examples

The following example shows how to display XDR information for all clients:

```
Router# show xdr client all
```

```

XDR Interrupt P(0) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Process Pri(1) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBHWIDB broker(2) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBIDB broker  (3) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBHWIDB Subblo(4) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBIDB Subblock(5) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR High Queue (6) flag:RP|LC
Adjacency updat(7) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Medium Queu(8) flag:RP|LC
IPv4 table brok(9) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Low Queue  (11) flag:RP|LC
MFI Pull        (12) flag:RP|ISSU aware
  ISSU capable slot(s): 1
Push Client One(13) flag:RP
CEF push        (14) flag:RP|ISSU aware
  ISSU capable slot(s): 1
MFI Push        (15) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR ping        (16) flag:RP
MPLS Embedded M(17) flag:RP

```

The following example shows how to display XDR information for all XDR line card peer instances:

```
Router# show xdr linecard
```

```

XDR slot number 1, status  PEER UP
  IPC messages sent 569
  This is the secondary RP
  Next sequence number to send      116
  Maximum sequence number expected 160
  ISSU state: Nego done, version 2, mtu 7, sid 31

```

The following example shows how to display XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1
```

```

XDR slot number 1, status  PEER UP
  IPC messages sent 570
  This is the secondary RP
  Next sequence number to send      116
  Maximum sequence number expected 160
  ISSU state: Nego done, version 2, mtu 7, sid 31

```

The following example shows how to display internal XDR information for the XDR line card peer instance in slot number 1:

Router# **show xdr linecard 1 internal**

```

XDR slot number 1, status  PEER UP
IPC maximum mtu  1478
IPC messages sent 570
This is the secondary RP
Next sequence number to send      116
Maximum sequence number expected 160
ISSU state: Nego done, version 2, mtu 7, sid 31

```

	Tx	bytes	Rx	bytes	
XDR Interrupt Priori:					
	0	0	10427	52135	Window Message
	87	1392	0	0	Time Message
	1	4	0	0	Resequence Message
	19	444	11	264	ISSU nego
XDR Process Priority:					
	17	51	11	33	Reg Signal
	1	2	0	0	CEF running
	0	0	1	4	CEF reload request
	15	348	9	216	ISSU nego
FIBHWIDB broker :					
	32	3588	0	0	fibhwidb update
	7	156	5	120	ISSU nego
FIBIDB broker :					
	49	6429	0	0	fibidb update
	7	156	5	120	ISSU nego
FIBHWIDB Subblock br:					
	7	156	5	120	ISSU nego
FIBIDB Subblock brok:					
	41	1533	0	0	fibswsb update
	13	300	8	192	ISSU nego
Adjacency update :					
	62	3089	0	0	adj update
	4	8	0	0	adj epoch
	17	396	10	240	ISSU nego
IPv4 table broker :					
	285	28557	0	0	prefix
	8	48	0	0	epoch
	5	78	0	0	table
	5	55	0	0	multicast prefix
	45	1068	24	576	ISSU nego
MFI Pull :					
	12	456	0	0	pull update
	75	1788	39	936	ISSU nego
CEF push :					
	8	48	14	84	repopulation req
	5	10	0	0	state
	12	816	0	0	control
	2	0	0	0	mpls_access-list delete
	2	32	0	0	icmp limit
	9	204	6	144	ISSU nego
MFI Push :					
	3	101	0	0	service reply
	2	34	0	0	client request
	0	0	4	106	service request
	2	16	0	0	enable/redist redistribution
client					
	153	3660	78	1872	ISSU nego
XDR ping :					
	6	24	6	24	ping message

Related Commands

Command	Description
show cef broker	Displays Cisco Express Forwarding information related to a selected update broker.

snmp mib cef throttling-interval

To set the throttling interval for the CEF-MIB inconsistency notifications, use the **snmp mib cef throttling-interval** command in global configuration mode. To remove the throttling interval, use the **no** form of this command.

snmp mib cef throttling-interval *seconds*

no snmp mib cef throttling-interval *seconds*

Syntax Description	<i>seconds</i>	The time to allow before an inconsistency notification is sent during the process of updating forwarding information from the Routing Information Base (RIB) to the Route Processor (RP) and the line card databases. The valid values are from 0 to 3600 seconds.
---------------------------	----------------	--

Command Default	Throttling is disabled by default (throttling interval is set to 0 seconds).
------------------------	--

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	12.2(31)SB	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines	<p>Use this command in conjunction with the snmp-server enable traps cef inconsistency command to set the time that elapsed between the occurrence of a Cisco Express Forwarding database inconsistencies and the time when you want to receive an inconsistency notification.</p> <p>If you set the throttling interval to 0 seconds, throttling is disabled.</p>
-------------------------	---

Examples	<p>The following example shows how to set the throttling interval for CEF-MIB inconsistency notification to 300 seconds:</p> <pre>configure terminal ! snmp-server enable traps cef inconsistency snmp mib cef throttling-interval 300</pre>
-----------------	--

Related Commands

Command	Description
snmp-server enable traps cef	Enables CEF-MIB notifications that correspond to Cisco Express Forwarding events.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps cef

To enable Cisco Express Forwarding support of Simple Network Management Protocol (SNMP) notifications on a network management system (NMS), use the **snmp-server enable traps cef** command in global configuration mode. To disable Cisco Express Forwarding support of SNMP notifications, use the **no** form of this command.

snmp-server enable traps cef [**peer-state-change**] [**resource-failure**] [**inconsistency**]
[**peer-fib-state-change**]

no snmp-server enable traps cef [**peer-state-change**] [**resource-failure**] [**inconsistency**]
[**peer-fib-state-change**]

Syntax Description

peer-state-change	(Optional) Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of Cisco Express Forwarding peers.
resource-failure	(Optional) Enables the sending of CEF-MIB SNMP notifications for resource failures that affect Cisco Express Forwarding operations.
inconsistency	(Optional) Enables the sending of CEF-MIB SNMP notifications for inconsistencies that occur when routing information is updated from the Routing Information Base (RIB) to the Cisco Express Forwarding Forwarding Information Base (FIB) on the Route Processor (RP) and to the Cisco Express Forwarding FIB on the line cards.
peer-fib-state-change	(Optional) Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of the Cisco Express Forwarding peer FIB.

Command Default

All CEF-MIB notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

You can use this command to enable CEF-MIB SNMP notifications that correspond to specific Cisco Express Forwarding events. To send the notifications to an NMS or host system, you must configure the **snmp-server host** command with the **cef** keyword.

You can enable all CEF-MIB SNMP notifications if you enter the **snmp-server enable traps cef** command without entering an optional keyword.

Examples

The following example shows how to enable a router to send Cisco Express Forwarding peer state changes and forwarding inconsistencies as informs to the NMS with IP address 10.56.125.47 and to use the community string defined as public:

```
configure terminal
!  
snmp-server enable traps cef peer-state-change inconsistency  
snmp-server host 10.56.125.47 informs version 2c public
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} [vrf vrf-name] [informs | traps] [version {1 | 2c | 3  
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

```
no snmp-server host {hostname | ip-address} [vrf vrf-name] [informs | traps] [version {1 | 2c | 3  
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

```
snmp-server host ip-address {community-string | {informs | traps} {community-string |  
version {1 | 2c | 3 {auth | noauth}} community-string | version {1 | 2c | 3 {auth | noauth}}  
community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c | 3 {auth  
| noauth}} community-string}} [notification-type]
```

```
no snmp-server host ip-address {community-string | {informs | traps} {community-string |  
version {1 | 2c | 3 {auth | noauth}} community-string | version {1 | 2c | 3 {auth | noauth}}  
community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c | 3 {auth  
| noauth}} community-string}} [notification-type]
```

Command Syntax on Cisco 7600 Series Router

```
snmp-server host ip-address {community-string | {informs | traps} {community-string |  
version {1 | 2c | 3 {auth | noauth | priv}} community-string | version {1 | 2c | 3 {auth | noauth  
| priv}} community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c  
| 3 {auth | noauth | priv}} community-string}} [notification-type]
```

```
no snmp-server host ip-address {community-string | {informs | traps} {community-string |  
version {1 | 2c | 3 {auth | noauth | priv}} community-string | version {1 | 2c | 3 {auth | noauth  
| priv}} community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c  
| 3 {auth | noauth | priv}} community-string}} [notification-type]
```

Syntax Description

<i>hostname</i>	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
<i>ip-address</i>	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the vrf keyword is required.
<i>vrf-name</i>	(Optional) VPN VRF instance used to send SNMP notifications. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the <i>vrf-name</i> argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the informs keyword is required.

traps	<p>(Optional) Specifies that notifications should be sent as traps. This is the default.</p> <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the traps keyword is required.
version	<p>(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1.</p> <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the version keyword is required and the priv keyword is not supported. <p>If you use the version keyword, one of the following keywords must be specified:</p> <ul style="list-style-type: none"> 1—SNMPv1. 2c—SNMPv2C. 3—SNMPv3. The most secure model because it allows packet encryption with the priv keyword. The default is noauth. <p>One of the following three optional security level keywords can follow the 3 keyword:</p> <ul style="list-style-type: none"> auth—Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. noauth—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. priv—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	<p>Password-like community string sent with the notification operation.</p> <p>Note You can set this string using the snmp-server host command by itself, but Cisco recommends that you define the string using the snmp-server community command prior to using the snmp-server host command.</p> <p>Note The “at” sign (@) is used for delimiting the context information.</p>
udp-port	<p>(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host.</p> <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the udp-port keyword is not supported.
<i>port</i>	<p>(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162.</p> <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the <i>port</i> argument is not supported.
<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the “Notification-Type Keywords” section on page 455 in the “Usage Guidelines” section for more information about the keywords available.</p>

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	<ul style="list-style-type: none"> The version 3 [auth noauth priv] syntax was added as part of the SNMPv3 Support feature. The hsrp notification-type keyword was added. The voice notification-type keyword was added.
12.1(3)T	The calltracker notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	<ul style="list-style-type: none"> The vrf <i>vrf-name</i> keyword and argument combination was added. The ipmobile notification-type keyword was added. Support for the vsimaster notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	<ul style="list-style-type: none"> The pim notification-type keyword was added. The ipsec notification-type keyword was added.
12.2(8)T	<ul style="list-style-type: none"> The mpls-traffic-eng notification-type keyword was added. The director notification-type keyword was added.
12.2(13)T	<ul style="list-style-type: none"> The srp notification-type keyword was added. The mpls-ldp notification-type keyword was added.
12.3(2)T	<ul style="list-style-type: none"> The flash notification-type keyword was added. The l2tun-session notification-type keyword was added.
12.3(4)T	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added. The ospf notification-type keyword was added.
12.3(8)T	The iplocalpool notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The vrrp keyword was added.
12.3(14)T	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The eigrp notification-type keyword was added.
12.4(20)T	The license notification-type keyword was added.
15.0(1)M	<ul style="list-style-type: none"> The nhrp notification-type keyword was added. The automatic insertion of the snmp-server community command into the configuration, along with the community string specified in the snmp-server host command, was changed. The snmp-server community command must be manually configured.
Cisco IOS Release 12.0S	
12.0(17)ST	The mpls-traffic-eng notification-type keyword was added.
12.0(21)ST	The mpls-ldp notification-type keyword was added.

Release	Modification
12.0(22)S	<ul style="list-style-type: none"> All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. The mpls-vpn notification-type keyword was added.
12.0(23)S	The l2tun-session notification-type keyword was added.
12.0(26)S	The memory notification-type keyword was added.
12.0(27)S	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The vrf vrf-name keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The l2tun-pseudowire-status notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The cef notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	<ul style="list-style-type: none"> The dhcp-snooping notification-type keyword was added. The errdisable notification-type keyword was added.
12.2(54)SE	This command was modified. See the “Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches” section on page 450 for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The public storm-control notification-type keyword was added.
12.2(50)SY	This command integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS Release 15S	
15.0(1)S	This command was modified. The flowmon notification-type keyword was added.
Cisco IOS XE	
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

**Note**

If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command **help ?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific virtual routing and forwarding (VRF) VPN. The VRF defines a VPN membership of a user so that data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but that does not have a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The notification type can be one or more of the following keywords:



Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server**—Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adsl**—Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm**—Sends ATM notifications.
- **authenticate-fail**—Sends an SNMP 802.11 Authentication Fail trap.
- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge**—Sends SNMP STP Bridge MIB notifications.
- **bstun**—Sends Block Serial Tunneling (bstun) event notifications.
- **bulkstat**—Sends Data-Collection-MIB notifications.
- **c6kxbar**—Sends SNMP crossbar notifications.
- **callhome**—Sends Call Home MIB notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **casa**—Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme**—Sends SNMP Cisco netManager Event (CCME) traps.
- **cef**—Sends notifications related to Cisco Express Forwarding.
- **chassis**—Sends SNMP chassis notifications.
- **cnpd**—Sends Cisco network-based application recognition (NBAR) Protocol Discovery (CNPD) traps.
- **config**—Sends configuration change notifications.
- **config-copy**—Sends SNMP config-copy notifications.
- **config-ctid**—Sends SNMP config-ctid notifications.
- **cpu**—Sends CPU-related notifications.
- **csg**—Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate**—Sends an SNMP 802.11 Deauthentication trap.
- **dhcp-snooping**—Sends Dynamic Host Configuration Protocol (DHCP) snooping MIB notifications.
- **director**—Sends notifications related to DistributedDirector.
- **disassociate**—Sends an SNMP 802.11 Disassociation trap.
- **dls**—Sends data-link switching (DLSW) notifications.
- **dnis**—Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x**—Sends 802.1X notifications.
- **dot11-mibs**—Sends dot11 traps.
- **dot11-qos**—Sends SNMP 802.11 QoS Change trap.

- **ds1**—Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback**—Sends ds1-loopback traps.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise**—Sends SNMP energywise notifications.
- **entity**—Sends Entity MIB modification notifications.
- **entity-diag**—Sends SNMP entity diagnostic MIB notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable**—Sends error disable notifications.
- **ethernet-cfm**—Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager**—Sends SNMP Embedded Event Manager notifications.
- **firewall**—Sends SNMP Firewall traps.
- **flash**—Sends flash media insertion and removal notifications.
- **flexlinks**—Sends FLEX links notifications.
- **flowmon**—Sends flow monitoring notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **fru-ctrl**—Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu**—Sends SNMP ICSUDSU traps.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipmulticast**—Sends IP multicast notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isakmp**—Sends SNMP ISAKMP notifications.
- **isdn**—Sends ISDN notifications.
- **l2tc**—Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **license**—Sends licensing notifications as traps or informs.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification**—Sends SNMP MAC notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **module**—Sends SNMP module notifications.
- **module-auto-shutdown**—Sends SNMP module autosutdown MIB notifications.
- **mpls-fast-reroute**—Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.

- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **msdp**—Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn**—Sends multicast VPN notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **port-security**—Sends SNMP port-security notifications.
- **power-ethernet**—Sends SNMP power Ethernet notifications.
- **public storm-control**—Sends SNMP public storm-control notifications.
- **pw-vc**—Sends SNMP pseudowire virtual circuit (VC) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **resource-policy**—Sends CISCO-ERM-MIB notifications.
- **rf**—Sends SNMP RF MIB notifications.
- **rogue-ap**—Sends an SNMP 802.11 Rogue AP trap.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb**—Sends SNMP server load balancer (SLB) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.



Note To enable RFC 2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet**—Sends SNMP SONET notifications.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stp**—Sends SNMP STP MIB notifications.
- **srst**—Sends SNMP Survivable Remote Site Telephony (SRST) traps.
- **stun**—Sends serial tunnel (STUN) notifications.
- **switch-over**—Sends an SNMP 802.11 Standby Switch-over trap.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.

- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **udp-port**—Sends the notification host's UDP port number.
- **vlan-mac-limit**—Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate**—Sends SNMP VLAN created notifications.
- **vlandelete**—Sends SNMP VLAN deleted notifications.
- **voice**—Sends SNMP voice traps.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **vswitch**—Sends SNMP virtual switch notifications.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep**—Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.
- **x25**—Sends X.25 event notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands.

[Table 97](#) maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 97 *SNMP-server enable traps Commands and Corresponding Notification Keywords*

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	l2tun-session
snmp-server enable traps mpls ldp	mpls-ldp
snmp-server enable traps mpls traffic-eng ¹	mpls-traffic-eng
snmp-server enable traps mpls vpn	mpls-vpn

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

**Note**

The “at” sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.

switchover pxf restart

To configure the number of parallel express forwarding (PXF) restarts that are allowed before a switchover to a redundant Performance Routing Engine (PRE) module, use the **switchover pxf restart** command in redundancy configuration (main-cpu) mode. To disable switchovers due to PXF restarts, use the **no** form of this command.

switchover pxf restart *number-of-restarts* *time-period*

no switchover pxf restart

Syntax Description	<i>number-of-restarts</i>	The number of PXF restarts that are allowed within the specified time period. If the PXF processors restart this many times within the given time period, the router switches over to the redundant PRE module. The valid range is 1 to 25. The default is 2 PXF restarts within 5 hours.
	<i>time-period</i>	Time period, in hours, that PXF restart counts are monitored. The valid range is 0 to 120 hours.
	Note	A value of 0 specifies that a switchover occurs on the configured <i>number-of-restarts</i> regardless of the time period.

Command Default If this command is not configured, the default is 2 PXF restarts within 5 hours.

Command Modes Redundancy configuration, main-cpu mode (config-r-mc)

Command History	Release	Modification
	12.2(15)BC2	This command was introduced on the Cisco uBR10012 router.
	12.3(7)	This command was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.3(7).
	12.2SB	This command was integrated into Cisco IOS Release 12.2SB.

Usage Guidelines The startup and running configurations of the standby PRE are synchronized with the active PRE, ensuring the fastest possible cut-over time if the active PRE fails. A second switchover is prevented for 2 hours if a PXF restart occurs on the new active PRE.

A PXF restart following a PXF fault may restore service more quickly when the features in use are not configured for nonstop forwarding with stateful switchover (NSF/SSO), or when SSO mode is not configured on the router. Conversely, a PRE switchover in response to a PXF restart may restore service more quickly when NSF/SSO is configured on the router and all configured features support NSF/SSO.

When a switchover occurs because of repeated PXF restarts, the router displays the following system message:

```
C10KEVENTMGR-3-PXF_FAIL_SWITCHOVER: Multiple PXF failures, switchover to redundant PRE initiated.
```

Examples

The following example shows how to configure the router so that if five PXF restarts occur within a one-hour period, the router initiates a switchover to the redundant PRE module.

```
Router(config)# redundancy  
Router(config-red)# main-cpu  
Router(config-r-mc)# switchover pxf restart 5 1
```

Related Commands

Command	Description
main-cpu	Enters main-cpu redundancy configuration mode to configure the synchronization of the active and standby PRE modules.
redundancy	Configures the synchronization of system files between the active and standby PRE modules.
redundancy force-failover main-cpu	Forces a manual switchover between the active and standby PRE modules.
show redundancy	Displays the current redundancy status.

test cef table consistency

To test the Cisco Express Forwarding Forwarding Information Base (FIB) for prefix consistency, use the **test cef table consistency** command in privilege EXEC mode.

test cef table consistency [detail]

Syntax Description	detail	(Optional) Displays detailed information about the consistency of prefixes in the Cisco Express Forwarding FIB table.
---------------------------	---------------	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2(25)S	This command was introduced. This command replaces the show ip cef inconsistency command .
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	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.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines	<p>This command displays recorded Cisco Express Forwarding consistency records found by the lc-detect, scan-rib-ios, scan-ios-rib, scan-lc-rp, and scan-rp-lc detection mechanisms. The scan-lc-rp and scan-rp-lc detection mechanisms are available only on routers with line cards.</p>
-------------------------	---

You can configure the Cisco Express Forwarding prefix consistency-detection mechanisms using the **cef table consistency-check** command.

Examples	The following is sample output from the test cef table consistency command:
-----------------	--

```
Router# test cef table consistency

full-scan-rib-ios: Checking IPv4 RIB to FIB consistency
full-scan-ios-rib: Checking IPv4 FIB to RIB consistency
No IPv4 inconsistencies found, check took 00:00:00.000
```

The following is sample output from the **test cef table consistency detail** command:

```
Router# test cef table consistency detail

full-scan-rib-ios: Checking IPv4 RIB to FIB consistency
full-scan-rib-ios: FIB checked 12 prefixes, and found 0 missing.
full-scan-ios-rib: Checking IPv4 FIB to RIB consistency
full-scan-ios-rib: Checked 12 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 26 IPv4 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv4 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv4 check completed on linecards..1..0..4..
full-scan-rp-lc: Linecard 4 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
```

```

full-scan-rp-lc: Linecard 0 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rib-ios: Checking IPv6 RIB to FIB consistency
full-scan-rib-ios: FIB checked 16 prefixes, and found 5 missing.
full-scan-ios-rib: Checking IPv6 FIB to RIB consistency
full-scan-ios-rib: Checked 11 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 11 IPv6 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv6 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv6 check completed on linecards..1..4..0..
full-scan-rp-lc: Linecard 4 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 0 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
No IPv4 inconsistencies found, check took 00:00:01.444
Warning: 5 IPv6 inconsistencies found, check took 00:00:01.240

```

Table 98 describes the significant fields shown in the display.

Table 98 *test cef consistency detail Field Descriptions*

Field	Description
FIB checked 12 prefixes, and found 0 missing	The scan-rib-ios consistency checker checked 12 prefixes in the FIB against the FIB and found 0 missing.
Checked 12 FIB prefixes in 1 pass, and found 0 extra.	The scan-ios-rib consistency checker checked 12 prefixes in the RIB and found no extra prefixes in one pass.
Linecard 4 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.	The scan-rp-lc consistency checker found no inconsistencies on line card 4 after checking 26 IPv4 prefixes.

Related Commands

Command	Description
cef table consistency check	Enables Cisco Express Forwarding table consistency checker types and parameters.