



# Cisco IOS Switching Commands

---

This chapter documents commands used to configure switching and NetFlow in Cisco IOS software. For guidelines on configuring switching and NetFlow, refer to the *Cisco IOS Switching Services Configuration Guide*.

---

**Note** In Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on Cisco 7000 series routers.

---

## clear ip flow stats

To clear the NetFlow statistics, use the **clear ip flow stats** EXEC command.

**clear ip flow stats**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CA.

The **show ip cache flow** command displays the NetFlow statistics. Use the **clear ip flow** command to clear the NetFlow statistics.

### Example

The following example clears the NetFlow statistics on the router:

```
clear ip flow stats
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show ip cache**

## encapsulation isl

Use the **encapsulation isl** subinterface configuration command to enable the Inter-Switch Link (ISL). ISL is a Cisco protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.

**encapsulation isl** *vlan-identifier*

### Syntax Description

*vlan-identifier* Virtual LAN identifier. The allowed range is 1 to 1000.

### Default

Disabled

### Command Mode

Subinterface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

ISL encapsulation is configurable on Fast Ethernet interfaces.

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between switches.

### Example

The following example enables ISL on Fast Ethernet subinterface 2/1.20:

```
interface FastEthernet 2/1.20
 encapsulation isl 400
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**bridge-group**

**debug vlan**

**show bridge vlan**

**show interfaces**

**show vlans**

## encapsulation sde

Use the **encapsulation sde** subinterface configuration command to enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs. IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.

**encapsulation sde** *said*

### Syntax Description

*said* Security association identifier. This value is used as the virtual LAN identifier. The valid range is 0 through 0xFFFFFFFFE.

### Default

Disabled

### Command Mode

Subinterface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

SDE encapsulation is configurable only on the following interface types:

#### IEEE 802.10 Routing

- FDDI

#### IEEE 802.10 Transparent Bridging

- Ethernet
- FDDI
- HDLC Serial
- Transparent mode
- Token Ring

### Example

The following example enables SDE on FDDI subinterface 2/0.1 and assigns a VLAN identifier of 9999:

```
interface fddi 2/0.1
 encapsulation sde 9999
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**bridge-group**  
**debug vlans**  
**show bridge vlan**  
**show interfaces**  
**show vlans**

## ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** global configuration command. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

```
ip cache-invalidate-delay [minimum maximum quiet threshold]  
no ip cache-invalidate-delay
```

### Syntax Description

<i>minimum</i>	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
<i>maximum</i>	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
<i>quiet</i>	(Optional) Length of quiet period (in seconds) before invalidation.
<i>threshold</i>	(Optional) Maximum number of invalidation requests considered to be quiet.

### Defaults

*minimum* = 2 seconds

*maximum* = 5 seconds, and 3 seconds with no more than zero invalidation requests

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

All cache invalidation requests are honored immediately.

This command should typically not be used except under the guidance of technical support personnel. Incorrect settings can seriously degrade network performance.

The IP fast-switching and autonomous-switching features maintain a cache of IP routes for rapid access. When a packet is to be forwarded and the corresponding route is not present in the cache, the packet is process-switched and a new cache entry is built. However, when routing table changes occur (such as when a link or an interface goes down), the route cache must be flushed so that it can be rebuilt with up-to-date routing information.

This command controls how the route cache is flushed. The intent is to delay invalidation of the cache until after routing has settled down. Because route table changes tend to be clustered in a short period of time, and the cache may be flushed repeatedly, a high CPU load might be placed on the router.

When this feature is enabled, and the system requests that the route cache be flushed, the request is held for at least *minimum* seconds. Then the system determines whether the cache has been “quiet” (that is, less than *threshold* invalidation requests in the last *quiet* seconds). If the cache has been quiet, the cache is then flushed. If the cache does not become quiet within *maximum* seconds after the first request, it is flushed unconditionally.

Manipulation of these parameters trades off CPU utilization versus route convergence time. Timing of the routing protocols is not affected, but removal of stale cache entries is affected.

### Example

The following example sets a minimum delay of 5 seconds, a maximum delay of 30 seconds, and a quiet threshold of no more than 5 invalidation requests in the previous 10 seconds:

```
ip cache-invalidate-delay 5 30 10 5
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ip route-cache**  
**show ip cache**

## ip flow-cache entries

Use the **ip flow-cache entries** global configuration command to change the number of entries maintained in the NetFlow cache. Use the **no** form of this command to return to the default number of entries.

**ip flow-cache entries** *number*  
**no ip flow-cache entries**

### Syntax Description

*number*                      Number of entries to maintain in the NetFlow cache. Range is 1024 to 524288 entries. The default is 65536 (64K).

### Default

65536 entries (64K)

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CA.

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow** command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.



**Caution** Cisco recommends that you do not change the NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

### Example

The following example increases the number of entries in the NetFlow cache to 131072 (128K):

```
ip flow-cache entries 131072
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show ip cache**

## ip flow-export

To enable the exporting of information in NetFlow cache entries, use the **ip flow-export** global configuration command. To disable the exporting of information, use the **no** form of this command.

```
ip flow-export ip-address udp-port [version 1 | version 5 [origin-as | peer-as]]
no ip flow-export
```

### Syntax Description

<i>ip-address</i>	IP address of the workstation to which you want to send the NetFlow information.
<i>udp-port</i>	UDP protocol-specific port number.
<b>version 1</b>	(Optional) Specifies that the export packet uses the version 1 format. This is the default. The version field occupies the first two bytes of the export record. The number of records stored in the datagram is a variable between 1 and 24 for version 1.
<b>version 5</b>	(Optional) Specifies export packet uses the version 5 format. The number of records stored in the datagram is a variable between 1 and 30 for version 5.
<b>origin-as</b>	(Optional) Specifies that export statistics includes the origin autonomous system (AS) for the source and destination.
<b>peer-as</b>	(Optional) Specifies that export statistics includes the peer AS for the source and destination.

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command was modified to include the **version** keyword in Cisco IOS Release 11.1 CA.

There is a lot of information in a NetFlow cache entry. When NetFlow is enabled with the **ip route-cache flow** command, you can use the **ip flow-export** command to configure the router to export the flow cache entry to a workstation when a flow expires. This feature can be useful for purposes of statistics, billing, and security.

Version 5 format includes the source and destination AS addresses, source and destination prefix masks, and a sequence number. Because this change may appear on your router as a maintenance release, support for version 1 format is maintained with the **version 1** keyword.

For more information on version 1 and version 5 data format, refer to the “NetFlow Data Format” section in “Configuring NetFlow” chapter of the *Cisco IOS Switching Services Configuration Guide*.

### Examples

The following example configures the router to export the NetFlow cache entry to UDP port 125 on the workstation at 134.22.23.7 when the flow expires using version 1 format:

```
ip flow-export 134.22.23.7 125
```

The following example configures the router to export the NetFlow cache entry to UDP port 2048 on the workstation at 134.22.23.7 when the flow expires using version 5 format and including the peer AS information:

```
ip flow-export 134.22.23.7 2048 version 5 peer-as
```

### Related Command

You can use the master indexes or search online to find documentation of related commands.

### **ip route-cache flow**

## ip route-cache

Use the **ip route-cache** interface configuration command to control the use of high-speed switching caches for IP routing. To disable any of these switching modes, use the **no** form of this command.

```

ip route-cache [cbus]
no ip route-cache [cbus]

ip route-cache same-interface
no ip route-cache same-interface

ip route-cache [optimum | flow]
no ip route-cache [optimum | flow]

ip route-cache distributed
no ip route-cache distributed

```

### Syntax Description

<b>cbus</b>	(Optional) Enables both autonomous switching and fast switching.
<b>same-interface</b>	Enables fast-switching packets back out the interface on which they arrived.
<b>optimum</b>	(Optional) Enables optimum fast switching on the Cisco 7500 series. This feature is enabled by default for IP on all supported interfaces (Ethernet, FDDI, and serial). For serial interfaces, it is supported for HDLC encapsulation only.
<b>flow</b>	(Optional) Enables NetFlow on the interface.
<b>distributed</b>	Enables VIP distributed switching on the interface. This feature can be enabled on Cisco 7500 series routers with an RSP and Versatile Interface Processor (VIP) controllers.

### Defaults

IP autonomous switching is disabled.  
 Fast switching varies by interface and media.  
 Optimum switching is enabled on supported interfaces.  
 Distributed switching is disabled.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **optimum** keyword first appeared in Cisco IOS Release 11.1. The **distributed** keyword first appeared in Cisco IOS Release 11.2.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis.

The **ip route-cache** command with no additional keywords enables fast switching and disables.

Cisco routers generally offer better packet transfer performance when fast switching is enabled, with one exception. On networks using slow serial links (64K and below), disabling fast switching to enable the per-packet load sharing is usually the best choice.

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This normally is not recommended, though it is useful when you have partially meshed media, such as Frame Relay. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection.

On Cisco 7500 series routers with RSP and Versatile Interface Processor (VIP) controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

Not all switching methods are available on all platforms. Refer to the *Cisco Product Catalog* for information about features available on the platform you are using.

### Examples

The following example enables both fast switching and autonomous switching:

```
ip route-cache cbus
```

The following example disables both fast switching and autonomous switching:

```
no ip route-cache
```

The following example turns off autonomous switching only:

```
no ip route-cache cbus
```

The following example enables VIP distributed NetFlow on the interface:

```
interface ethernet 0/5/0
ip address 17.252.245.2 255.255.255.0
ip route-cache distributed
ip route-cache flow
```

The following example returns the system to its defaults (fast switching enabled; autonomous switching disabled):

```
ip route-cache
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ip cache-invalidate-delay**  
**show ip cache**

## ip route-cache flow

To enable NetFlow for IP routing, use the **ip route-cache flow** interface configuration command. To disable NetFlow, use the **no** form of this command.

**ip route-cache flow**  
**no ip route-cache flow**

### Syntax Description

This command has no arguments or keywords.

### Defaults

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

NetFlow captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service information that can be used for a wide variety of purposes such as network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export** global configuration command.

NetFlow is supported on IP and IP encapsulated traffic over all interface types and encapsulations except for ISL/VLAN, ATM and Frame Relay interfaces when more than one input access control list is used on the interface, and ATM LANE.

A network flow is identified as a unidirectional stream of packets between a source and destination—both defined by a network-layer IP address and transport-layer port number. Specifically, a flow is identified as the combination of the following fields:

- source IP address
- destination IP address
- source port number
- destination port number
- protocol type
- type of service
- input interface

NetFlow operates by creating a flow cache. The cache includes entries for traffic statistics. Flow information is maintained within the NetFlow cache for all active flows. With NetFlow you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow does not involve any connection-setup protocol either between routers or to any other networking device or end station and does not require any change externally—either to the traffic or packets themselves or to any other networking device. Thus, NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, because NetFlow is performed independently on each internetworking device, it

does not need to be operational on each router in the network. Network planners can selectively invoke NetFlow (and NetFlow data export) on a router/interface basis to gain traffic performance, control, or accounting benefits in specific network locations.

---

**Note** NetFlow does consume additional memory and CPU resources; therefore, it is important to understand the resources required on your router before enabling NetFlow.

---

### Examples

The following example enables NetFlow on the interface:

```
interface ethernet 0/5/0
 ip address 17.252.245.2 255.255.255.0
 ip route-cache flow
```

The following example returns the interface to its defaults (fast switching enabled; autonomous switching disabled):

```
interface ethernet 0/5/0
 ip route-cache
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ip flow-export**  
**show ip cache**

## show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache EXEC** command.

```
show ip cache [prefix mask] [type number]
```

### Syntax Description

<i>prefix</i>	(Optional) Display only the entries in the cache that match the prefix and mask combination.
<i>mask</i>	(Optional) Display only the entries in the cache that match the prefix and mask combination.
<i>type</i>	(Optional) Display only the entries in the cache that match the interface type and number combination.
<i>number</i>	(Optional) Display only the entries in the cache that match the interface type and number combination.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The arguments *prefix*, *mask*, *type*, and *number* first appeared in Cisco IOS Release 10.0. The **show ip cache** display shows MAC headers up to 92 bytes.

### Sample Displays

The following is sample output from the **show ip cache** command:

```
Router# show ip cache

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length      Age           Interface     MAC Header
131.108.1.1/32     0:01:09      Ethernet0/0   AA000400013400000C0357430800
131.108.1.7/32     0:04:32      Ethernet0/0   00000C01281200000C0357430800
131.108.1.12/32    0:02:53      Ethernet0/0   00000C029FD000000C0357430800
131.108.2.13/32    0:06:22      Fddi2/0       00000C05A3E000000C035753AAAA0300
00000800
131.108.2.160/32   0:06:12      Fddi2/0       00000C05A3E000000C035753AAAA0300
00000800
131.108.3.0/24     0:00:21      Ethernet1/2   00000C026BC600000C03574D0800
131.108.4.0/24     0:02:00      Ethernet1/2   00000C026BC600000C03574D0800
131.108.5.0/24     0:00:00      Ethernet1/2   00000C04520800000C03574D0800
131.108.10.15/32   0:05:17      Ethernet0/2   00000C025FF500000C0357450800
131.108.11.7/32    0:04:08      Ethernet1/2   00000C010E3A00000C03574D0800
131.108.11.12/32   0:05:10      Ethernet0/0   00000C01281200000C0357430800
131.108.11.57/32   0:06:29      Ethernet0/0   00000C01281200000C0357430800
```

Table 1 describes significant fields shown in the display.

**Table 1 Show IP Cache Field Descriptions**

Field	Description
IP routing cache version	Version number of this table. This number is incremented any time the table is flushed.
entries	Number of valid entries.
bytes	Number of bytes of processor memory for valid entries.
hash overflows	Number of times autonomous switching cache overflowed.
Minimum invalidation interval	Minimum time delay between cache invalidation request and actual invalidation.
maximum interval	Maximum time delay between cache invalidation request and actual invalidation.
quiet interval	Length of time between cache flush requests before the cache will be flushed.
threshold <i>n</i> requests	Maximum number of requests that can occur while the cache is considered quiet.
Invalidation rate <i>n</i> in last <i>m</i> seconds	Number of cache invalidations during the last <i>m</i> seconds.
0 in last 3 seconds	Number of cache invalidation requests during the last quiet interval.
Last full cache invalidation occurred <i>hh:mm:ss</i> ago	Time since last full cache invalidation was performed.
Prefix/Length	Network reachability information for cache entry.
Age	Age of cache entry.
Interface	Output interface type and number.
MAC Header	Layer 2 encapsulation information for cache entry.

The following is sample output from the **show ip cache** command with a prefix and mask specified:

```
Router# show ip cache 131.108.5.0 255.255.255.0

IP routing cache version 4490, 119 entries, 17464 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:11:56 ago

Prefix/Length      Age      Interface      MAC Header
131.108.5.0/24    0:00:34  Ethernet1/2    0000C0452080000C03574D0800
```

The following is sample output from the **show ip cache** command with an interface specified:

```
Router# show ip cache e0/2

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length      Age      Interface      MAC Header
131.108.10.15/32   0:05:17  Ethernet0/2    0000C025FF500000C0357450800
```

## show ip cache flow

To display a summary of the NetFlow statistics, use the **show ip cache flow EXEC** command.

**show ip cache flow**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command was modified to update the display with the latest information in Cisco IOS Release 11.1 CA.

### Sample Display

The following is a sample output from the **show ip cache flow** command.

```
Router# show ip cache flow
IP packet size distribution (12718M total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
    .000 .554 .042 .017 .015 .009 .009 .009 .013 .030 .006 .007 .005 .004 .004

    512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
    .003 .007 .139 .019 .098 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456448 bytes
65509 active, 27 inactive, 820628747 added
955454490 aged polls, 0 flow alloc failures
Exporting flows to 1.1.15.1 (2057)
820563238 flows exported in 34485239 udp datagrams, 0 failed
last clearing of statistics 00:00:03
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	2656855	4.3	86	78	372.3	49.6	27.6
TCP-FTP	5900082	9.5	9	71	86.8	11.4	33.1
TCP-FTPD	3200453	5.1	193	461	1006.3	45.8	33.4
TCP-WWW	546778274	887.3	12	325	11170.8	8.0	32.3
TCP-SMTP	25536863	41.4	21	283	876.5	10.9	31.3
TCP-X	116391	0.1	231	269	43.8	68.2	27.3
TCP-BGP	24520	0.0	28	216	1.1	26.2	39.0
TCP-Frag	56847	0.0	24	952	2.2	13.1	33.2
TCP-other	49148540	79.7	47	338	3752.6	30.7	32.2
UDP-DNS	117240379	190.2	3	112	570.8	7.5	34.7
UDP-NTP	9378269	15.2	1	76	16.2	2.2	38.7
UDP-TFTP	8077	0.0	3	62	0.0	9.7	33.2
UDP-Frag	51161	0.0	14	322	1.2	11.0	39.4
UDP-other	45502422	73.8	30	174	2272.7	8.5	37.8
ICMP	14837957	24.0	5	224	125.8	12.1	34.3
IGMP	40916	0.0	170	207	11.3	197.3	13.5
IPINIP	3988	0.0	48713	393	315.2	644.2	19.6
GRE	3838	0.0	79	101	0.4	47.3	25.9
IP-other	77406	0.1	47	259	5.9	52.4	27.0

## show ip cache flow

```

Total:          820563238 1331.7          15  304 20633.0          9.8          33.0
SrcIf  SrcIPAddress  DstIf  DstIPAddress  Pr SrcP DstP Pkts B/Pk Active
Fd0/0  80.0.0.3        Hs1/0  200.1.9.1     06 0621 0052   7  87  5.9
Fd0/0  80.0.0.3        Hs1/0  200.1.8.1     06 0620 0052   7  87  1.8
Hs1/0  200.0.0.3       Fd0/0  80.1.10.1    06 0052 0621   6  58  1.8
Hs1/0  200.0.0.3       Fd0/0  80.1.1.1     06 0052 0620   5  62  5.9
Fd0/0  80.0.0.3        Hs1/0  200.1.3.1    06 0723 0052  16  68  0.3
Hs1/0  200.0.0.3       Fd0/0  80.1.2.1     06 0052 0726   6  58 11.8
Fd0/0  80.0.0.3        Hs1/0  200.1.5.1    06 0726 0052   6  96  0.3
Hs1/0  200.0.0.3       Fd0/0  80.1.4.1     06 0052 0442   3  76  0.3
Hs1/0  200.0.0.3       Fd0/0  80.1.7.1     06 0052 D381  11 1171 0.6

```

Table 2 describes the fields in the packet size distribution lines of the output.

**Table 2 Packet Size Distribution Field Descriptions**

Field	Description
IP packet size distribution	The two lines below this banner show the percentage distribution of packets by size range. In this display, 55.4% of the packets fall in the size range 33 to 64 bytes.

Table 3 describes the fields in the flow switching cache lines of the output.

**Table 3 Flow Switching Cache Display Field Descriptions**

Field	Description
bytes	Number of of bytes of memory the NetFlow cache uses,
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive,	Number of flow buffers allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command was entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to expire entries (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Exporting flows	IP address and UDP port number of the workstation to which flows are exported.
flows exported in udp datagrams	Total number of flows exported and the total number of UDP datagrams used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the clear ip flow stats command was executed. This time output changes to hours and days after the time exceed 24 hours

Table 4 describes the fields in the activity-by-protocol lines of the output.

**Table 4 Activity-By-Protocol Display Field Descriptions**

Field	Description
Protocol	IP protocol and the “well known” port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to Total Packets for this protocol or number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol) or the total number of seconds for this summary period).
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, time-out, and so forth) in seconds or total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time this command was entered, in seconds or total flows for this protocol for this summary period.

Table 5 describes the fields in the current flow lines of the output.

**Table 5 Current Flow Display Field Descriptions**

Field	Description
SrcIf	Internal port name for the source interface.
SrcIPAddress	Source IP address for this flow.
DstIf	Router’s internal port name for the destination interface.
DstIPAddress	Destination IP address for this flow.
Pr	IP protocol; for example, 6=TCP, 17=UDP, ... as defined in RFC 1340.
SrcP	Source port address, TCP/UDP “well known” port number, as defined in RFC 1340.
DstP	Destination port address, TCP/UDP “well known” port number, as defined in RFC 1340.
Pkts	Number of packets observed for this flow.
B/Pkt	Average observed number of bytes per packet for this flow.
Active	Number of seconds between first and last packet of a flow.

## Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ip route-cache**  
**clear ip flow stats**

