

NetFlow Switching Enhancements

Description

The NetFlow switching commands have been modified to provide added functionality and improved performance under heavy traffic conditions. Netflow switching is a high-performance, network-layer switching path that captures as part of its switching function 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.

NetFlow switching 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.

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow switching, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a “connection-oriented” basis as part of the flow, where access list checks are bypassed and packet switching and statistics capture are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a give 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 switching operates by creating a flow cache that contains the information needed to switch and perform access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard switching path (fast or optimum). As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created,

packets identified as belonging to an existing flow can be switched based on the cached information and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

Benefit

NetFlow switching provides network administrators with access to “call detail recording” information from their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting and departmental chargebacks, ISP billing, data warehousing/mining for marketing purposes, etc. NetFlow also provides a highly efficient mechanism with which to process security access lists without paying as much of a performance penalty as is incurred with other available switching methods.

Platforms

This feature is supported on these platforms:

- Cisco 7200 series
- Cisco 7500 series
- Cisco 7000 series routers with RSP7000 and RSP7000CI

Configuration Tasks

The following sections describe how to configure and maintain NetFlow switching on the router.

Configure NetFlow Switching

NetFlow switching is one of the four available switching modes. When you configure NetFlow on an interface, the other switching modes are not used on that interface. Optimum switching remains the most efficient switching mode and results in the highest throughput when extensive access list processing is not required. NetFlow comes in a close second (within 15 to 20% of optimum switching throughput, possibly higher when access lists are involved). Fast switching is third fastest, with process switching the slowest of all. Also, with NetFlow switching you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow switching is based on identifying packet flows and performing switching and access list processing within a router. It 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 switching is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, because NetFlow switching 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 switching (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 compared to other switching modes; therefore, it is important to understand the resources required on your router before enabling NetFlow.

To configure NetFlow switching, first configure the router for IP routing as described in the “Configuring IP” and the “Configuring IP Routing Protocols” chapters. After you configure IP routing, perform the following tasks beginning in global configuration mode:

Task	Command
Step 1 Specify the interface, and enter interface configuration mode.	interface <i>type slot/port-adapter lport</i> (Cisco 7500 series and Cisco 7000 series routers with the RSP7000) interface <i>type slot/port</i> (Cisco 7200 series routers)
Step 2 Specify flow switching.	ip route-cache flow

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 NetFlow traffic rates. 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 4 MB 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.

To customize the number of entries in the NetFlow cache, perform the following task in global configuration mode:

Task	Command
Change the number of entries maintained in the NetFlow cache. The number of entries can be 1024 to 524288. The default is 65536.	ip flow-cache entries <i>number</i>



Caution We recommend that you 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.

Configure NetFlow Data Export

NetFlow switching information can also be exported to network management applications. The information is exported to a specified workstation. When using the NetFlow Collector application on the workstation, you can also specify the NetFlow Collector version format that the exported packets uses. For more information on the NetFlow version, refer to the “NetFlow Data Format” section later in this document.

To configure the router to export NetFlow switching statistics maintained in the NetFlow cache to a workstation when a flow expires, perform the following tasks in global configuration mode:

Task	Command
Step 1 Configure the router to export NetFlow cache entries to a workstation.	ip flow-export destination { <i>hostname</i> <i>ip-address</i> } <i>udp-port</i>

Task	Command
Step 2 If you are using version 5 of the NetFlow Collector on the workstation, configure the router to use version 5. The default is version 1. Optionally, for version 5, specify origin or peer autonomous system (AS). The default is to export neither AS and provides improved performance.	ip flow-export version { 1 5 [origin-as peer-as]}
Step 3 Configure the source interface used by NetFlow to indicate the source of the exported NetFlow data.	ip flow-export source <i>interface</i>

By default, the active flows timeout after 30 minutes, at which time the router exports the active flow cache entries to a workstation. To increase or decrease the timeout period for active flows, perform the following task in global configuration mode:

Task	Command
Change the timeout period for the active flows. The time can be 1 to 60 minutes. The default is 30 minutes.	ip flow-cache active-timeout <i>minutes</i>

Manage NetFlow Switching Statistics

You can display and clear NetFlow switching statistics. NetFlow statistics consist of IP packet size distribution, IP flow switching cache information, and flow information such as the protocol, total flow, flows per second, etc. The resulting information can be used to find out information about your router traffic. These tasks are summarized below. Perform any of the following tasks in privileged EXEC mode:

Task	Command
Display the NetFlow switching statistics.	show ip cache flow
Clear the NetFlow switching statistics.	clear ip flow stats

Configuration Examples

The following example shows how to configure NetFlow switching on serial interface 5/0:0 and enable exporting of flow statistics for further processing to UDP port 9995 on a workstation with the IP address of 1.1.15.1. The NetFlow Collector on the workstation uses the source IP address to determine which router sent the flow data. Because the source address can change depending on the route the data takes, you must specify a loopback interface. The source interface is specified as a loopback interface 0 and the serial interface is assigned to loopback 0 interface.

In this example, existing NetFlow statistics are cleared to ensure accurate information when the **show ip cache flow** command is executed to view a summary of the NetFlow switching statistics.

```
router# configure terminal
router(config)# interface loopback0
router(config-if)# ip address 4.0.0.1 255.0.0.0
router(config-if)# exit
router(config)# interface serial 5/0:0
router(config-if)# ip unnumbered loopback0
router(config-if)# no ip mroute-cache
router(config-if)# encapsulation ppp
router(config-if)# ip route-cache flow
router(config-if)# exit
router(config)# ip flow-export destination 1.1.15.1 9995
router(config)# ip flow-export source loopback0
router(config)# ip flow-export version 5 peer-as
router(config)# exit
router# clear ip flow stats
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.1 command references.

- **clear ip flow stats**
- **ip flow-cache active-timeout**
- **ip flow-cache entries**
- **ip flow-export destination**
- **ip flow-export source**
- **ip flow-export version**
- **ip route-cache flow**
- **show ip cache flow**

Note The **ip flow-export destination**, **ip flow-export source**, and **ip flow-export version** commands replace the **ip flow-export** command. Refer to the documentation of the **ip flow-export destination**, **ip flow-export source**, and **ip flow-export version** commands for more information.

clear ip flow stats

To clear the NetFlow switching 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 switching statistics. Use the **clear ip flow** command to clear the NetFlow switching statistics.

Example

The following example clears the NetFlow switching statistics on the router:

```
router# clear ip flow stats
```

Related Command

show ip cache flow

ip flow-cache active-timeout

To specify when the active flows should timeout, use the **ip flow-cache active-timeout** global configuration command. To return to the default timeout period, use the **no** form of this command.

ip flow-cache active-timeout *minutes*
no ip flow-cache active-timeout

Syntax Description

minutes Timeout period for the active flows. Range is 1 to 60 minutes. The default is 30 minutes.

Default

30 minutes

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CA.

You can increase or decrease the timeout period for the active flows, and the router will export active flow cache entries to a workstation when the active flows reach this timeout value. To obtain information on your flow timeout, use the **show ip cache flow** command.

Example

The following example increases the timeout period for the active flows to be exported after 45 minutes:

```
router# configure terminal
router(config)# ip flow-cache active-timeout 45
router(config)# exit
```

Related Commands

ip flow-cache entries
show ip cache flow

ip flow-cache entries

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

```
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 4 MB 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 We recommend 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):

```
router# configure terminal  
router(config)# ip flow-cache entries 131072  
router(config)# exit
```

Related Command

show ip cache flow

ip flow-export destination

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

```
ip flow-export destination {hostname | ip-address} udp-port
no ip flow-export destination
```

Syntax Description

<i>hostname</i>	IP hostname of the workstation to which you want to send the NetFlow information.
<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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

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

There is a lot of information in a NetFlow cache entry. When flow switching is enabled with the **ip route-cache flow** command, you can use the **ip flow-export destination** 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, security, for example.

To specify the source IP address of the data, use the **ip flow-export source** command. To specify the version used on the workstation that receives the NetFlow data, use the **ip flow-export version** command.

Example

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 (the default):

```
router# configure terminal
router(config)# ip flow-export destination 134.22.23.7 125
router(config)# exit
```

Related Commands

```
ip flow-export source
ip flow-export version
ip route-cache flow
```

ip flow-export source

To specify the source interface IP address used in the NetFlow export datagram, use the **ip flow-export source** global configuration command. To remove the source address, use the **no** form of this command.

```
ip flow-export source interface  
no ip flow-export source
```

Syntax Description

interface Interface type to use as the source interface.

Default

No source interface is specified.

Command Mode

Global configuration

Usage Guidelines

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

After you configure NetFlow data export, you can also specify the source interface used in the UDP datagram containing the export data. The NetFlow Collector on the workstation uses the IP address of the source interface to determine which router sent the information. The NetFlow Collector also performs SNMP queries to the router using the IP address of the source interface. Because the IP address of the source interface can change (for example, the interface might flap so a different interface is used to send the data), we recommend you configure a loopback source interface. A loopback interface is always up and can respond to SNMP queries from the NetFlow Collector on the workstation.

Example

The following example shows the configuration for a loopback source interface. The loopback interface has the IP address 4.0.0.1 and is used by the serial interface in slot 5, port 0.

```
router# configure terminal  
router(config)# interface loopback0  
router(config-if)# ip address 4.0.0.1 255.0.0.0  
router(config-if)# exit  
router(config)# interface serial 5/0:0  
router(config-if)# ip unnumbered loopback0  
router(config-if)# no ip mroute-cache  
router(config-if)# encapsulation ppp  
router(config-if)# ip route-cache flow  
router(config-if)# exit  
router(config)# ip flow-export source loopback0  
router(config)# exit
```

Related Commands

```
ip flow-export destination  
ip flow-export version  
ip route-cache flow
```

ip flow-export version

To specify the version format used by the NetFlow export packets, use the **ip flow-export version** global configuration command. To disable the exporting of information, use the **no** form of this command.

```
ip flow-export version {1 | 5 [origin-as | peer-as]}
no ip flow-export version
```

Syntax Description

1	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.
5	Specifies that the 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.
origin-as	(Optional) For version 5, specifies that export statistics include the origin autonomous system (AS) for the source and destination.
peer-as	(Optional) For version 5, specifies that export statistics include the peer AS for the source and destination.

Default

Version 1

Command Mode

Global configuration

Usage Guidelines

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

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

For more information on version 1 and version 5 data format, refer to the “NetFlow Data Format” section at the end of this chapter.

Example

The following example configures the router to export the data using version 5 format and include the peer AS information:

```
router# configure terminal
router(config)# interface loopback0
router(config-if)# ip address 4.0.0.1 255.0.0.0
router(config-if)# exit
router(config)# interface serial 5/0:0
router(config-if)# ip unnumbered loopback0
router(config-if)# no ip mroute-cache
router(config-if)# encapsulation ppp
router(config-if)# ip route-cache flow
router(config-if)# exit
router(config)# ip flow-export version 5 peer-as
router(config)# exit
```

Related Commands

ip flow-export destination

ip flow-export source

ip route-cache flow

ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** interface configuration command. To disable NetFlow switching, 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 CA.

Netflow switching is a high-performance, network-layer switching path that captures as part of its switching function 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 switching 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.

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow switching, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a “connection-oriented” basis as part of the flow, where access list checks are bypassed and packet switching and statistics capture are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a give 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 switching operates by creating a flow cache that contains the information needed to switch and perform access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard switching path (fast or optimum). As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created, packets identified as belonging to an existing flow can be switched based on the cached information and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

NetFlow switching is one of the four available switching modes. When you configure NetFlow on an interface, the other switching modes are not used on that interface. Optimum switching remains the most efficient switching mode and results in the highest throughput when extensive access list processing is not required. NetFlow comes in a close second (within 15 to 20% of optimum switching throughput, possibly higher when access lists are involved). Fast switching is third fastest, with process switching the slowest of all. Also, with NetFlow switching you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow switching is based on identifying packet flows and performing switching and access list processing within a router. It 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 switching is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, because NetFlow switching 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 switching (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 compared to other switching modes; therefore, it is important to understand the resources required on your router before enabling NetFlow

Examples

The following example enables NetFlow switching on the interface:

```
router# configure terminal
router(config)# interface ethernet 0/5/0
router(config-if)# ip address 17.252.245.2 255.255.255.0
router(config-if)# ip route-cache flow
router(config-if)# exit
```

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

```
router# configure terminal
router(config)# interface ethernet 0/5/0
router(config-if)# ip route-cache
router(config-if)# exit
```

Related Commands

ip flow-export destination
show ip cache flow

show ip cache flow

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

show ip cache flow

Syntax Description

This command has no keywords and arguments.

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 (0 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Exporting flows to 200.0.0.2 (9996)
  Exporting using source interface Loopback0
  Version 5 flow records, peer-as
  Active flows timeout in 10 minutes
  0 flows exported in 0 udp datagrams, 0 failed
  last clearing of statistics never

Protocol          Total  Flows  Packets Bytes  Packets Active(Sec) Idle(Sec)
-----          Flows  /Sec   /Flow /Pkt   /Sec   /Flow   /Flow
SrcIf   SrcIPAddress  DstIf   DstIPAddress  Pr SrcP DstP Pkts B/Pk Activ
```

Table 20 describes the fields in the packet size distribution lines of the output.

Table 20 Show IP Cache Flow Field Descriptions—Packet Size Distribution

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 21 describes the fields in the flow switching cache lines of the output.

Table 21 Show IP Cache Flow Field Descriptions—Flow Switching Cache

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 to	IP address and UDP port number of the workstation to which flows are exported.
Exporting using source interface	Interface type used as the source IP address.
Version 5 flow records, peer-as	Exported packets use version 5 format and the export statistics includes the peer AS for the source and destination. The number of records stored in the datagram is a variable between 1 and 30 for version 5.
Active flows timeout in	Timeout period for active flows in the NetFlow cache.
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 22 describes the fields in the activity-by-protocol lines of the output.

Table 22 Show IP Cache Flow Field Descriptions—NetFlow Activity by Protocol

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 /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 /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) / The total number of seconds for this summary period).

Table 22 Show IP Cache Flow Field Descriptions—NetFlow Activity by Protocol

Field	Description
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/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/Total Flows for this protocol for this summary period.

Table 23 describes the fields in the current flow lines of the output.

Table 23 Show IP Cache Flow Field Descriptions—Current Flow

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

ip route-cache flow
clear ip flow stats

NetFlow Data Format

NetFlow exports flow information in UDP datagrams in one of two formats: the version 1 format was the initial released version, and version 5 is a later enhancement to add BGP AS information and flow sequence numbers. Versions 2 through 4 were not released.

In version 1 and version 5 format, the datagram consists of a header and one or more flow records. The first field of the header contain the version number of the export datagram. Typically a receiving application that accepts either format allocates a buffer big enough for the biggest possible datagram from either format and uses the version from the header to determine how to interpret the datagram. The second field in the header is the number of records in the datagram and should be used to index through the records.

All fields in either version 1 or version 5 formats are in network byte order. Table 24 and Table 25 describe the data format for version 1, and Table 26 and Table 27 describe the data format for version 5.

We recommend that receiving applications sanity check datagrams to ensure that the datagrams are from a valid Netflow source. We recommend you first check the size of the datagram to make sure it is at least long enough to contain the version and count fields. Next we recommend you verify that the version is valid (1 or 5) and that the number of received bytes is enough for the header and count flow records (using the appropriate version).

Because Netflow export uses UDP to send export datagrams, it is possible for datagrams to be lost. To determine whether or not flow export information is lost, the version 5 header format contains a flow sequence number. The sequence number is equal to the previous datagram's sequence number plus the number of flows in the previous datagram. After receiving a new datagram, the receiving application can subtract the expected sequence number from the sequence number in the header to get the number of missed flows.

Table 24 **Version 1 Header Format**

Bytes	Content	Description
0-1	version	Netflow export format version number.
2-3	count	Number of flows exported in this packet (1-24).
4-7	SysUptime	Current time in milliseconds since router booted.
8-11	unix_secs	Current seconds since 0000 UTC 1970.
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970.

Table 25 **Version 1 Flow Record Format**

Bytes	Content	Description
0-3	srcaddr	Source IP address.
4-7	dstaddr	Destination IP address.
8-11	nexthop	Next hop router's IP address.
12-13	input	Input interface's SNMP index.
14-15	output	Output interface's SNMP index.
16-19	dPkts	Packets in the flow.
20-23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24-27	First	SysUptime at start of flow.
28-31	Last	SysUptime at the time the last packet of flow was received.
32-33	srcport	TCP/UDP source port number or equivalent.
34-35	dstport	TCP/UDP destination port number or equivalent.
36-37	pad1	Unused (zero) byte.
38	prot	IP protocol (for example, 6=TCP, 17=UDP).
39	tos	IP type-of-service.
40	flags	Cumulative OR of tcp flags.
41-43	,pad2and pad3	Unused (zero) bytes.
44-47	reserved	Unused (zero) bytes.

Table 26 **Version 5 Header Format**

Bytes	Content	Description
0-1	version	Netflow export format version number.
2-3	count	Number of flows exported in this packet (1-30).
4-7	SysUptime	Current time in milliseconds since router booted.
8-11	unix_secs	Current seconds since 0000 UTC 1970.
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970.
16-19	flow_sequence	Sequence counter of total flows seen.
20-23	reserved	Unused (zero) bytes.

Table 27 **Version 5 Flow Record Format**

Bytes	Content	Description
0-3	srcaddr	Source IP address.
4-7	dstaddr	Destination IP address.
8-11	nexthop	Next hop router's IP address.
12-13	input	Input interface's SNMP index.
14-15	output	Output interface's SNMP index.
16-19	dPkts	Packets in the flow.
20-23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24-27	First	SysUptime at start of flow.
28-31	Last	SysUptime at the time the last packet of flow was received.
32-33	srcport	TCP/UDP source port number or equivalent.
34-35	dstport	TCP/UDP destination port number or equivalent.
36	pad1	Unused (zero) bytes.
37	tcp_flags	Cumulative OR of tcp flags.
38	prot	IP protocol (for example, 6=TCP, 17=UDP).
39	tos	IP type-of-service.
40-41	src_as	AS of the source, either origin or peer.
42-43	dst_as	AS of the destination, either origin or peer.
44	src_mask	Source address prefix mask bits.
45	dst_mask	Destination address prefix mask bits.
46-47	pad2	Unused (zero) bytes.

What to Do Next

For more information on NetFlow, refer to the *NetFlow FlowCollector Installation and User's Guide* and the *NetFlow FlowAnalyzer Installation and User's Guide* publications.

