

Configuring NetFlow

This chapter describes NetFlow. For a complete description of NetFlow commands used in this chapter, refer to the *Cisco IOS Switching Services Command Reference*. For documentation of other commands that appear in this chapter, you can use the command reference master index or search online. This chapter contains these sections:

- Understanding NetFlow
- Configure NetFlow
- NetFlow Configuration Example

Understanding NetFlow

NetFlow 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 and data mining for marketing purposes.

This chapter describes NetFlow and how to configure NetFlow features. It contains these sections:

- NetFlow Support
- Accounting Statistics
- NetFlow Data Format
- Configure NetFlow

NetFlow Support

NetFlow is supported on Cisco 7200 series routers and Cisco 7500 series routers.

Accounting Statistics

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.

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.

Capturing Traffic Data

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 Cache

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.

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 Border Gateway Protocol (BGP) autonomous system (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 2 and Table 3 describe the data format for version 1, and Table 4 and Table 5 describe the data format for version 5.

Cisco recommends 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 User Datagram Protocol (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 sequence number of the previous 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 2 lists the bytes for version 1 header format.

Table 2 Version 1 Header Format

Bytes	Content	Description
0-3	version and count	Netflow export format version number and 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 3 lists the byte definitions for version 1 flow record format.

Table 3 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.
12-15	input and output	Input and 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.
32-35	srcport and dstport	TCP/UDP source and destination port number or equivalent.
36-39	pad1, prot, and tos	Unused (zero) byte, IP protocol (for example, 6=TCP, 17=UDP), and IP type-of-service.
40-43	flags, pad2, and pad3	Cumulative OR of TCP flags. Pad 2 and pad 3 are unused (zero) byte.
44-47	reserved	Unused (zero) bytes.

Table 4 lists the byte definitions for version 5 header format.

Table 4 Version 5 Header Format

Bytes	Content	Description
0-3	version and count	Netflow export format version number and 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 5 lists the byte definitions for version 5 flow record format.

Table 5 **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.
12-15	input and output	Input and 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.
32-35	srcport and dstport	TCP/UDP source and destination port number or equivalent.
36-39	pad1, tcp_flags, prot, and tos	Unused (zero) byte, Cumulative OR of TCP flags, IP protocol (for example, 6=TCP, 17=UDP), and IP type-of-service.
40-43	src_as and dst_as	AS of the source and destination, either origin or peer.
44-47	src_mask, dst_mask, and pad2	Source and destination address prefix mask bits, pad 2 is unused (zero) bytes.

Configure NetFlow

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 or 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.

To configure NetFlow, first configure the router for IP routing as described in the IP configuration chapters in the *Network Protocols Configuration Guide, Part 1*. 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 routers) interface <i>type slot/port</i> (Cisco 7200 series routers)
Step 2 Specify NetFlow.	ip route-cache flow

NetFlow information can also be exported to network management applications. To configure the router to export NetFlow statistics maintained in the NetFlow cache to a workstation when a flow expires, perform one of the following tasks in global configuration mode:

Task	Command
Configure the router to export NetFlow cache entries to a workstation if you are using receiving software that requires version 1. Version 1 is the default.	ip flow-export <i>ip-address udp-port</i> [version 1]
Configure the router to export NetFlow cache entries to a workstation if you are using receiving software that accepts version 5. Optionally specify origin or peer autonomous system (AS). The default is to export neither AS which provides improved performance.	ip flow-export <i>ip-address udp-port version 5</i> [origin-as peer-as]

Normally the 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 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.

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 Cisco recommends 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.

Manage NetFlow Statistics

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution, IP flow cache information, and flow information such as the protocol, total flow, flows per second, and so forth. The resulting information can be used to find out information about your router traffic. To manage NetFlow statistics, perform any of the following tasks in privileged EXEC mode:

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

Configure IP Distributed Switching and NetFlow on VIP Interfaces

On Cisco 7500 series routers with a Route Switch Processor (RSP) and with 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. This process is called *distributed switching*. Distributed switching decreases the demand on the RSP.

The VIP hardware can also be configured for NetFlow, a new feature that identifies initiation of traffic flow between internet endpoints and caches information about the flow. NetFlow data can also be exported to network management applications.

Refer to the Cisco Product Catalog for information about VIP port adapters used for distributed switching.

To configure distributed switching on the VIP, first configure the router for IP routing as described in this chapter and the various routing protocol chapters, depending on the protocols you use.

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>
Step 2 Enable VIP distributed switching of IP packets on the interface.	ip route-cache distributed
Step 3 Specify optimum switching or NetFlow.	ip route-cache [flow optimum]

To export NetFlow cache entries to a workstation when a flow expires, perform the following task in global configuration mode:

Task	Command
Configure the router to export NetFlow cache entries to a workstation.	ip flow-export <i>ip-address udp-port</i>

To improve performance, fragmented IP packets are optimum switched rather than being process switched by default on Cisco 7500 series routers.

NetFlow Configuration Example

The following example shows how to modify the configuration of serial interface 3/0/0 to enable NetFlow and to export the flow statistics for further processing to UDP port 0 on a workstation with the IP address of 1.1.15.1. 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 statistics.

```
configure terminal
interface serial 3/0/0
 ip route-cache flow
 exit
 ip flow-export 1.1.15.1 0 version 5 peer-as
 exit
 clear ip flow stats
```

