

# NetFlow Overview

---

This chapter describes NetFlow.

## 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. It contains these sections:

- NetFlow Support
- Accounting Statistics
- NetFlow Data Format

## 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 5 and Table 6 describe the data format for version 1, and Table 7 and Table 8 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 5 lists the bytes for version 1 header format.

**Table 5**            **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 6 lists the byte definitions for version 1 flow record format.

**Table 6**      **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 7 lists the byte definitions for version 5 header format.

**Table 7**      **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 8 lists the byte definitions for version 5 flow record format.

**Table 8**      **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.

---

<b>Bytes</b>	<b>Content</b>	<b>Description</b>
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.