NetFlow Export Datagram Formats

NetFlow exports flow information in UDP datagrams in one of four formats:

- Version 1
- Version 5
- Version 7
- Version 8

The Version 1 (V1) format is the original format supported in the initial NetFlow releases. The Version 5 (V5) format is an enhancement that adds Border Gateway Protocol (BGP) autonomous system information and flow sequence numbers. The Version 7 (V7) format is an enhancement that exclusively supports NetFlow with Cisco Catalyst 5000 series switches equipped with a NetFlow feature card (NFFC). V7 is not compatible with Cisco routers. The Version 8 (V8) format is an enhancement that adds router-based aggregation schemes. Versions 2, 3, 4, and 6 either were not released or are not supported by FlowCollector.

In Versions 1, 5, and 7, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts any of the format versions allocates a buffer large enough for the largest possible datagram from any of the format versions and then uses the header to determine how to interpret the datagram. The second field in the header contains the number of records in the datagram and should be used to search through the records.

All fields described in the format version tables are in network byte order.

- Table B-1 and Table B-2 describe the V1 header and flow record format, respectively
- Table B-3 and Table B-4 describe the V5 header and flow record format, respectively
- Table B-5 and Table B-6 describe the V7 header and flow record format, respectively
- Table B-7 describes the V8 header format
- Table B-8 describes the V8 RouterAS flow record format
- Table B-9 describes the V8 RouterProtoPort flow record
- Table B-10 describes the V8 RouterDstPrefix flow record
- Table B-11 describes the RouterSrcPrefix flow record
- Table B-12 describes the RouterPrefix flow record format
- Table B-13 describes the TosAS flow record format
- Table B-14 describes the TosProtoPort flow record format
- Table B-15 describes the PrePortProtocol flow record format

- Table B-16 describes the TosSrcPrefix flow record format
- Table B-17 describes the TosDstPrefix flow record format
- Table B-18 describes the TosPrefix flow record format
- Table B-19 describes the DestOnly flow record format
- Table B-20 describes the SrcDst flow record format
- Table B-21 describes the FullFlow flow record format.

Note V8 data consists of header information that follows the same format as the other versions. However, the V8 flow record formats are separated based on the aggregation schemes that support router-based aggregation. Instead of one flow record table, you see five tables that describe the V8 flow record format for each individual aggregation scheme.

We recommend that receiving applications perform a *sanity check* on datagrams to ensure that the datagrams are from a valid NetFlow source. You should first check the size of the datagram to verify that it is at least long enough to contain the version and count fields. You should next verify that the version is valid (1, 5, 7, or 8) 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 flow export information has been lost, Version 5, Version 7, and

Version 8 headers contain a flow sequence number. The sequence number is equal to the sequence number of the previous datagram 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 derive the number of missed flows.

Datagram format Version 8 offers five router-based aggregation schemes allowing you to summarize FlowCollector export data on the router before the data is exported to the FlowCollector. The result is lower bandwidth requirements and reduced platform requirements for NetFlow data collection devices.

Router-based aggregation enables on-router aggregation by maintaining one or more extra NetFlow caches with different combinations of fields that determine which traditional flows are grouped together. These extra caches are called aggregation caches. As flows expire from the main flow cache, they are added to each enabled aggregation cache. The normal flow ager process runs on each active aggregation cache the same way it runs on the main cache. On-demand aging is also supported.

Table B-1 describes the V1 header format.

Table B-1 Version 1 Header Format

Bytes	Contents	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 the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-16	unix_nsecs	Residual nanoseconds since 0000 UTC 1970

Table B-2 describes the V1 flow record format.

Table B-2 Version 1 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the 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) bytes
38	prot	IP protocol type (for example, TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40	flags	Cumulative OR of TCP flags
41-43	pad1, pad2, pad3	Unused (zero) bytes
44-48	reserved	Unused (zero) bytes

Table B-3 describes the V5 header format.

Table B-3 Version 5 Header Format

Bytes	Contents	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 the export device booted
8-11	unix_secs	Current count of 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	engine_type	Type of flow-switching engine
21	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

Table B-4 describe the V5 flow record format.

Table B-4 Version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the 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 type (for example, TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number 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

Table B-5 and describes the V7 header format.

Table B-5 Version 7 (Catalyst 5000) Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this flow frame (protocol data unit, or PDU)
4-7	SysUptime	Current time in milliseconds since the export device 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 B-6 describe the V7 flow record format.

Table B-6 Version 7 (Catalyst 5000) Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address; in case of destination-only flows, set to zero.
4-7	dstaddr	Destination IP address.
8-11	nexthop	Next hop router; always set to zero.
12-13	input	SNMP index of input interface; always set to zero.
14-15	output	SNMP index of output interface.
16-19	dPkts	Packets in the flow.
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow.
24-27	First	SysUptime, in milliseconds, at start of flow.
28-31	Last	SysUptime, in milliseconds, at the time the last packet of the flow was received.
32-33	srcport	TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination.
34-35	dstport	TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination.
36	flags	Flags indicating, among other things, what flow fields are invalid.
37	tcp_flags	TCP flags; always set to zero.
38	prot	IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination.
39	tos	IP type of service; switch sets it to the ToS of the first packet of the flow.
40-41	src_as	Source autonomous system number, either origin or peer; always set to zero.
42-43	dst_as	Destination autonomous system number, either origin or peer; always set to zero.
44	src_mask	Source address prefix mask; always set to zero.
45	dst_mask	Destination address prefix mask; always set to zero.
46-47	flags	Flags indicating, among other things, what flows are invalid.
48-51	router_sc	IP address of the router that is bypassed by the Catalyst 5000 series switch. This is the same address the router uses when it sends NetFlow export packets. This IP address is propagated to all switches bypassing the router through the FCP protocol.

Table B-7 describes the V8 header format.

Note Version 7 AS information is not supported in current implementations of the Catalyst 5000 series switch.

Table B-7 Version 8 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this flow frame (protocol data unit, or PDU)
4-7	SysUptime	Current time in milliseconds since the export device 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	engine_type	Type of flow switching engine
21	engine_id	ID number of the flow switching engine
22	aggregation	Aggregation method being used
23	agg_version	Version of the aggregation export
24-27	reserved	Unused (zero) bytes

Table B-8 describes the V8 RouterAS flow record format.

Table B-8 Version 8 RouterAS Flow Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-21	src_as	Source autonomous system number, either origin or peer; always set to zero
22-23	dst_as	Destination autonomous system number, either origin or peer; always set to zero
24-25	input	SNMP index of input interface; always set to zero
26-27	output	SNMP index of output interface

Table B-9 describes the V8 **RouterProtoPort** flow record.

Table B-9 Version 8 RouterProtoPort Flow Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20	prot	IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination
21	pad	Unused (zero) bytes
22-23	reserved	Unused (zero) bytes
24-25	srcport	TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination
26-27	dstport	TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination

Table B-10 describes the V8 **RouterDstPrefix** flow record.

Table B-10 Version 8 RouterDstPrefix Flow Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	dst_prefix	Destination IP address prefix
24	dst_mask	Destination address prefix mask; always set to zero
25	pad	Unused (zero) bytes
26-27	dst_as	Destination autonomous system number, either origin or peer; always set to zero
28-29	output	SNMP index of output interface
30-31	reserved	Unused (zero) bytes

Table B-11 describes the **RouterSrcPrefix** flow record.

Table B-11 Version 8 RouterSrcPrefix Flow Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	src_prefix	Source IP address prefix
24	src_mask	Source address prefix mask; always set to zero
25	pad	Unused (zero) bytes
26-27	src_as	Source autonomous system number, either origin or peer; always set to zero
28-29	input	SNMP index of input interface; always set to zero
30-31	reserved	Unused (zero) bytes

Table B-12 describes the **RouterPrefix** flow record format.

Table B-12 Version 8 RouterPrefix Flow Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	src_prefix	Source IP address prefix
24-27	dst_prefix	Destination IP address prefix
28	dst_mask	Source address prefix mask; always set to zero
29	src_mask	Destination address prefix mask; always set to zero
30-31	reserved	Unused (zero) bytes
32-33	src_as	Source autonomous system number, either origin or peer; always set to zero
34-35	dst_as	Destination autonomous system number, either origin or peer; always set to zero
36-37	input	SNMP index of input interface; always set to zero
38-39	output	SNMP index of output interface

Table B-13 describes the **TosAS** flow record format.

Table B-13 Version 8 TosAS Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-21	src_as	Source autonomous system number, either origin or peer; always set to zero
22-23	dst_as	Destination autonomous system number, either origin or peer; always set to zero
24-25	input	SNMP index of input interface; always set to zero
26-27	output	SNMP index of output interface
28	tos	Type of service
29	pad	Unused (zero) bytes
30-31	reserved	Unused (zero) bytes

Table B-14 describes the **TosProtoPort** flow record format.

Table B-14 Version 8 TosProtoPort Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20	prot	IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination
21	Tos	IP Type of Service
22-23	reserved	Unused (zero) bytes
24-25	srcport	TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination
26-27	dstport	TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination
28-29	input	SNMP index of input interface
30-31	output	SNMP index of output interface

Table B-15 describes the **PrePortProtocol** flow record format.

Table B-15 Version 8 PrePortProtocol Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dpkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	src_prefix	Source IP address prefix
24-27	dst_prefix	Destination IP address prefix
28	dst_mask	Destination address prefix mask
29	src_mask	Source address prefix mask
30	Tos	IP Type of Service
31	prot	IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination
32-33	srcport	TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination
34-35	dstport	TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination
36-37	input	SNMP index of input interface
38-39	output	SNMP index of output interface

Table B-16 describes the **TosSrcPrefix** flow record format.

Table B-16 Version 8 TosSrcPrefix Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	src_prefix	Source IP address prefix
24	src_mask	Source address prefix mask
25	Tos	IP Type of Service
26-27	src_as	Source autonomous system number, either origin or peer
28-29	input	SNMP index of input interface
30-31	reserved	Reserved for future use

Table B-17 describes the **TosDstPrefix** flow record format.

Table B-17 Version 8 TosDstPrefix Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	dst_prefix	Destination IP address prefix
24	dst_mask	Destination address prefix mask
25	Tos	IP Type of Service
26-27	dst_as	Destination autonomous system number, either origin or peer
28-29	output	SNMP index of output interface
30-31	reserved	Unused (zero) bytes

Table B-18 describes the **TosPrefix** flow record format.

Table B-18 Version 8 TosPrefix Record Format

Bytes	Contents	Description
0-3	flows	Number of flows
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-23	src_prefix	Source IP address prefix
24-27	dst_prefix	Destination IP address prefix
28	dst_mask	Destination address prefix mask
29	src_mask	Source address prefix mask
30	Tos	IP Type of Service
31	pad	Unused (zero) bytes
32-33	src_as	Source autonomous system number, either origin or peer
34-35	dst_as	Destination autonomous system number, either origin or peer
36-37	input	SNMP index of input interface
38-3	output	SNMP index of output interface

Table B-19 describes the **DestOnly** flow record format.

Note This Flow statistic record is only used in Catalyst 6000 Series **DestOnly** aggregation.

Table B-19 Version 8 DestOnly Record Format

Bytes	Contents	Description
0-3	dstaddr	Destination IP address
4-7	dPkts	Packets in the flow
8-11	dOctets	Total number of Layer 3 bytes in the packets of the flow
12-15	First	SysUptime, in seconds, at start of flow
16-19	Last	SysUptime, in seconds, at the time the last packet of the flow was received
20-21	Output	SNMP index of output interface
22	Tos	IP Type of Service
23	marked_tos	Type of Service of the packets that exceeded the contract
24-27	extraPkts	Packets that exceed the contract
28-31	router_sc	IP address of the router that is bypassed by the Catalyst 5000 series switch. This is the same address the router uses when it sends NetFlow export packets. This IP address is propagated to all switches bypassing the router through the FCP protocol.

Table B-20 describes the **SrcDst** flow record format.

Note This Flow statistic record is used in Catalyst 6000 Series only **SrcDst** aggregation.

Table B-20 Version 8 SrcDst Record Format

Bytes	Contents	Description
0-3	dstaddr	Destination IP address
4-7	srcaddr	Source IP address; in case of destination-only flows, set to zero
8-11	dPkts	Packets in the flow
12-15	dOctets	Total number of Layer 3 bytes in the packets of the flow
16-19	First	SysUptime, in seconds, at start of flow
20-23	Last	SysUptime, in seconds, at the time the last packet of the flow was received
24-25	Output	SNMP index of output interface
26-27	Input	SNMP index of input interface
28	Tos	IP Type of Service
29	marked_tos	Type of Service of the packets that exceeded the contract
30-31	reserved	Unused (zero) bytes

Table B-20 Version 8 SrcDst Record Format (continued)

Bytes	Contents	Description
32-35	extraPkts	Packets that exceed the contract
36-39	router_sc	IP address of the router that is bypassed by the Catalyst 5000 series switch. This is the same address the router uses when it sends NetFlow export packets. This IP address is propagated to all switches bypassing the router through the FCP protocol.

Table B-21 describes the **FullFlow** flow record format.

Note This Flow statistic record is used in Catalyst 6000 Series only **FullFlow** aggregation.

Table B-21 Version 8 FullFlow Record Format

Bytes	Contents	Description
0-3	dstaddr	Destination IP address
4-7	srcaddr	Source IP address; in case of destination-only flows, set to zero
8-9	dstport	TCP/UDP destination port number; set to zero if flow mask is destination-only or source-destination
10-11	srcport	TCP/UDP source port number; set to zero if flow mask is destination-only or source-destination
12-15	dPkts	Packets in the flow
16-19	dOctets	Total number of Layer 3 bytes in the packets of the flow
20-23	First	SysUptime, in seconds, at start of flow
24-27	Last	SysUptime, in seconds, at the time the last packet of the flow was received
28-29	Output	SNMP index of output interface
30-31	Input	SNMP index of input interface
32	Tos	IP Type of Service
33	prot	IP protocol type (for example, TCP = 6; UDP = 17); set to zero if flow mask is destination-only or source-destination
34	marked_tos	Type of Service of the packets that exceeded the contract
35	pad	Unused (zero) bytes
36-39	extraPkts	Packets that exceed the contract
40-43	router_sc	IP address of the router that is bypassed by the Catalyst 5000 series switch. This is the same address the router uses when it sends NetFlow export packets. This IP address is propagated to all switches bypassing the router through the FCP protocol.