

Cisco IOS NetFlow Version 9 Flow-Record Format

Last updated: May 2011

Overview

Cisco IOS® NetFlow services provide network administrators with access to information concerning IP flows within their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting, and departmental chargebacks, Internet Service Provider (ISP) billing, data warehousing, combating Denial of Service (DoS) attacks, and data mining for marketing purposes.

The basic output of NetFlow is a **flow record**. Several different formats for flow records have evolved as NetFlow has matured. The most recent evolution of the NetFlow flow-record format is known as Version 9. The distinguishing feature of the NetFlow Version 9 format is that it is **template based**. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Using templates provides several key benefits:

- Third-party business partners who produce applications that provide collector or display services for NetFlow will not be required to recompile their applications each time a new NetFlow feature is added; instead, they may be able to use an external data file that documents the known template formats
- New features can be added to NetFlow more quickly, without breaking current implementations
- NetFlow is “future-proofed” against new or developing protocols, because the Version 9 format can be adapted to provide support for them

Terminology Used in This Document

One of the difficulties in describing the NetFlow Version 9 packet format occurs because many distinctly different, but similar-sounding, terms are used to describe portions of the NetFlow output. To eliminate any confusion, these terms are described below:

- **Export packet**—Built by a device (for example, a router) with NetFlow services enabled, this type of packet is addressed to another device (for example, a NetFlow collector). This other device processes the packet (parses, aggregates, and stores information on IP flows).
- **Packet header**—the first part of an export packet, the packet header provides basic information about the packet, such as the NetFlow version, number of records contained within the packet, and sequence numbering, enabling lost packets to be detected.
- **FlowSet**—following the packet header, an export packet contains information that must be parsed and interpreted by the collector device. A FlowSet is a generic term for a collection of records that follow the packet header in an export packet. There are two different types of FlowSets: **template** and **data**. An export packet contains one or more FlowSets, and both template and data FlowSets can be mixed within the same export packet.
- **Template FlowSet**—a template FlowSet is a collection of one or more **template records** that have been grouped together in an export packet.

- **Template record**—a template record is used to define the format of subsequent data records that may be received in current or future export packets. It is important to note that a template record within an export packet does not necessarily indicate the format of data records within that same packet. A collector application must cache any template records received, and then parse any data records it encounters by locating the appropriate template record within the cache.
- **Template ID**—the template ID is a unique number that distinguishes this template record from all other template records produced by the same export device. A collector application that is receiving export packets from several devices should be aware that uniqueness is not guaranteed **across** export devices. Thus, the collector should also cache the address of the export device that produced the template ID in order to enforce uniqueness.
- **Data FlowSet**—a data FlowSet is a collection of one or more **data records** that have been grouped together in an export packet.
- **Data record**—A data record provides information about an IP flow that exists on the device that produced an export packet. Each group of data records (that is, each data FlowSet) references a previously transmitted template ID, which can be used to parse the data contained within the records.
- **Options template**—an options template is a special type of template record used to communicate the format of data related to the NetFlow process.
- **Options data record**—the options data record is a special type of data record (based on an options template) with a reserved template ID that provides information about the NetFlow process itself.

NetFlow Version 9 Packet Layout

The NetFlow Version 9 record format consists of a packet header followed by at least one or more template or data FlowSets. A template FlowSet provides a description of the fields that will be present in future data FlowSets. These data FlowSets may occur later within the same export packet or in subsequent export packets.

Template and data FlowSets can be intermingled within a single export packet, as illustrated in Table 1.

Table 1. NetFlow Version 9 Export Packet

Packet Header	Template FlowSet	Data FlowSet	Data FlowSet	Template FlowSet	Data FlowSet
---------------	------------------	--------------	--------------	-------	------------------	--------------

The possible combinations that can occur in an export packet follow:

- An export packet that consists of interleaved template and data FlowSets—A collector device should not assume that the template IDs defined in such a packet have any specific relationship to the data FlowSets within the same packet. The collector must always cache any received templates, and examine the template cache to determine the appropriate template ID to interpret a data record.
- An export packet consisting entirely of data FlowSets—after the appropriate template IDs have been defined and transmitted to the collector device, most of the export packets will consist solely of data FlowSets.
- An export packet consisting entirely of template FlowSets—although this case is the exception, it is possible to receive packets containing only template records. Ordinarily, templates are “piggybacked” onto data FlowSets. However, in some instances only templates are sent. When a router first boots up or reboots, it attempts to synchronize with the collector device as quickly as possible. The router may send template FlowSets at an accelerated rate so that the collector device has sufficient information to interpret

any subsequent data FlowSets. Also, template records have a limited lifetime, and they must be periodically refreshed. If the refresh interval for a template occurs and there is no appropriate data FlowSet that needs to be sent to the collector device, an export packet consisting solely of template FlowSets is sent.

The format of both template and data FlowSets is discussed later in this document.

NetFlow Version 9 Packet Header Format

The format of the NetFlow Version 9 packet header remains relatively unchanged from previous versions. It is based on the NetFlow Version 5 packet header and is illustrated in Table 2. Table 3 gives field descriptions.

Table 2. NetFlow Version 9 Packet Header Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version										Count																					
System Uptime																															
UNIX Seconds																															
Package Sequence																															
Source ID																															

Table 3. NetFlow Version 9 Packet Header Field Descriptions

Field Name	Value
Version	The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009
Count	Number of FlowSet records (both template and data) contained within this packet
System Uptime	Time in milliseconds since this device was first booted
UNIX Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970
Sequence Number	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to identify whether any export packets have been missed Note: This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented "total flows."
Source ID	The Source ID field is a 32-bit value that is used to guarantee uniqueness for all flows exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow Version 5 and Version 8 headers). The format of this field is vendor specific. In the Cisco implementation, the first two bytes are reserved for future expansion, and will always be zero. Byte 3 provides uniqueness with respect to the routing engine on the exporting device. Byte 4 provides uniqueness with respect to the particular line card or Versatile Interface Processor on the exporting device. Collector devices should use the combination of the source IP address plus the Source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

Other values that existed in the NetFlow Version 5 and Version 8 packet headers (such as sampling interval and aggregation scheme) are sent in a reserved "options" data record. The format of the options template and options data record is discussed later in this document.

NetFlow Version 9 Template FlowSet Format

One of the key elements in the new NetFlow Version 9 format is the template FlowSet. Templates greatly enhance the flexibility of the NetFlow record format, because they allow a NetFlow collector or display application to process NetFlow data **without necessarily knowing the format of the data in advance**. Templates are used to describe the type and length of individual fields within a NetFlow data record that match a template ID.

The format of the template FlowSet is described in Table 4, and the field descriptions are given in Table 5.

Table 4. NetFlow Version 9 Template FlowSet Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = 0															
Length															
Template ID															
Field Count															
Field 1 Type															
Field 1 Length															
Field 2 Type															
Field 2 Length															
.															
.															
.															
Field N Type															
Field N Length															
Template ID															
Field Count															
Field 1 Type															
Field 1 Length															
Field 2 Type															
Field 2 Length															
.															
.															
.															
Field N Type															
Field N Length															

Table 5. NetFlow Version 9 Template FlowSet Field Descriptions

Field Name	Value
FlowSet ID	The FlowSet ID is used to distinguish template records from data records. A template record always has a FlowSet ID in the range of 0-255. Currently, the template record that describes flow fields has a FlowSet ID of zero and the template record that describes option fields (described below) has a FlowSet ID of 1. A data record always has a nonzero FlowSet ID greater than 255.
Length	Length refers to the total length of this FlowSet. Because an individual template FlowSet may contain multiple template IDs (as illustrated above), the length value should be used to determine the position of the next FlowSet record, which could be either a template or a data FlowSet. Length is expressed in Type/Length/Value (TLV) format, meaning that the value includes the bytes used for the FlowSet ID and the length bytes themselves, as well as the combined lengths of all template records included in this FlowSet.
Template ID	As a router generates different template FlowSets to match the type of NetFlow data it will be exporting, each template is given a unique ID. This uniqueness is local to the router that generated the template ID. Templates that define data record formats begin numbering at 256 since 0-255 are reserved for FlowSet IDs.
Field Count	This field gives the number of fields in this template record. Because a template FlowSet may contain multiple template records, this field allows the parser to determine the end of the current template record and the start of the next.

Field Name	Value
Field Type	This numeric value represents the type of the field. The possible values of the field type are vendor specific. Cisco supplied values are consistent across all platforms that support NetFlow Version 9. At the time of the initial release of the NetFlow Version 9 code (and after any subsequent changes that could add new field-type definitions), Cisco provides a file that defines the known field types and their lengths. The currently defined field types are detailed in Table 6.
Field Length	This number gives the length of the above-defined field, in bytes.

Note the following:

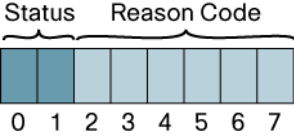
- Template IDs are not consistent across a router reboot. Template IDs should change only if the configuration of NetFlow on the export device changes.
- Templates periodically expire if they are not refreshed. Templates can be refreshed in two ways. A template can be resent every *N* number of export packets. A template can also be sent on a timer, so that it is refreshed every *N* number of minutes. Both options are user configurable.

Table 6. NetFlow Version 9 Field Type Definitions

Field Type	Value	Length (bytes)	Description
IN_BYTES	1	N (default is 4)	Incoming counter with length N x 8 bits for number of bytes associated with an IP Flow.
IN_PKTS	2	N (default is 4)	Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow
FLAWS	3	N	Number of flows that were aggregated; default for N is 4
PROTOCOL	4	1	IP protocol byte
SRC_TOS	5	1	Type of Service byte setting when entering incoming interface
TCP_FLAGS	6	1	Cumulative of all the TCP flags seen for this flow
L4_SRC_PORT	7	2	TCP/UDP source port number i.e.: FTP, Telnet, or equivalent
IPV4_SRC_ADDR	8	4	IPv4 source address
SRC_MASK	9	1	The number of contiguous bits in the source address subnet mask i.e.: the submask in slash notation
INPUT_SNMP	10	N	Input interface index; default for N is 2 but higher values could be used
L4_DST_PORT	11	2	TCP/UDP destination port number i.e.: FTP, Telnet, or equivalent
IPV4_DST_ADDR	12	4	IPv4 destination address
DST_MASK	13	1	The number of contiguous bits in the destination address subnet mask i.e.: the submask in slash notation
OUTPUT_SNMP	14	N	Output interface index; default for N is 2 but higher values could be used
IPV4_NEXT_HOP	15	4	IPv4 address of next-hop router
SRC_AS	16	N (default is 2)	Source BGP autonomous system number where N could be 2 or 4
DST_AS	17	N (default is 2)	Destination BGP autonomous system number where N could be 2 or 4
BGP_IPV4_NEXT_HOP	18	4	Next-hop router's IP in the BGP domain
MUL_DST_PKTS	19	N (default is 4)	IP multicast outgoing packet counter with length N x 8 bits for packets associated with the IP Flow

Field Type	Value	Length (bytes)	Description
MUL_DST_BYTES	20	N (default is 4)	IP multicast outgoing byte counter with length N x 8 bits for bytes associated with the IP Flow
LAST_SWITCHED	21	4	System uptime at which the last packet of this flow was switched
FIRST_SWITCHED	22	4	System uptime at which the first packet of this flow was switched
OUT_BYTES	23	N (default is 4)	Outgoing counter with length N x 8 bits for the number of bytes associated with an IP Flow
OUT_PKTS	24	N (default is 4)	Outgoing counter with length N x 8 bits for the number of packets associated with an IP Flow.
MIN_PKT_LNGTH	25	2	Minimum IP packet length on incoming packets of the flow
MAX_PKT_LNGTH	26	2	Maximum IP packet length on incoming packets of the flow
IPV6_SRC_ADDR	27	16	IPv6 Source Address
IPV6_DST_ADDR	28	16	IPv6 Destination Address
IPV6_SRC_MASK	29	1	Length of the IPv6 source mask in contiguous bits
IPV6_DST_MASK	30	1	Length of the IPv6 destination mask in contiguous bits
IPV6_FLOW_LABEL	31	3	IPv6 flow label as per RFC 2460 definition
ICMP_TYPE	32	2	Internet Control Message Protocol (ICMP) packet type; reported as ((ICMP Type*256) + ICMP code)
MUL_IGMP_TYPE	33	1	Internet Group Management Protocol (IGMP) packet type
SAMPLING_INTERVAL	34	4	When using sampled NetFlow, the rate at which packets are sampled i.e.: a value of 100 indicates that one of every 100 packets is sampled
SAMPLING_ALGORITHM	35	1	The type of algorithm used for sampled NetFlow: 0x01 Deterministic Sampling ,0x02 Random Sampling
FLOW_ACTIVE_TIMEOUT	36	2	Timeout value (in seconds) for active flow entries in the NetFlow cache
FLOW_INACTIVE_TIMEOUT	37	2	Timeout value (in seconds) for inactive flow entries in the NetFlow cache
ENGINE_TYPE	38	1	Type of flow switching engine: RP = 0, VIP/Linecard = 1
ENGINE_ID	39	1	ID number of the flow switching engine
TOTAL_BYTES_EXP	40	N (default is 4)	Counter with length N x 8 bits for bytes for the number of bytes exported by the Observation Domain
TOTAL_PKTS_EXP	41	N (default is 4)	Counter with length N x 8 bits for bytes for the number of packets exported by the Observation Domain
TOTAL_FLOWS_EXP	42	N (default is 4)	Counter with length N x 8 bits for bytes for the number of flows exported by the Observation Domain
Vendor Proprietary	43		
IPV4_SRC_PREFIX	44	4	IPv4 source address prefix (specific for Catalyst architecture)
IPV4_DST_PREFIX	45	4	IPv4 destination address prefix (specific for Catalyst architecture)
MPLS_TOP_LABEL_TYPE	46	1	MPLS Top Label Type: 0x00 UNKNOWN 0x01 TE-MIDPT 0x02 ATOM 0x03 VPN 0x04 BGP 0x05 LDP
MPLS_TOP_LABEL_IP_ADDR	47	4	Forwarding Equivalent Class corresponding to the MPLS Top Label
FLOW_SAMPLER_ID	48	1	Identifier shown in "show flow-sampler"
FLOW_SAMPLER_MODE	49	1	The type of algorithm used for sampling data: 0x02 random sampling. Use in connection with FLOW_SAMPLER_MODE
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	Packet interval at which to sample. Use in connection with FLOW_SAMPLER_MODE
Vendor Proprietary	51		

Field Type	Value	Length (bytes)	Description
MIN_TTL	52	1	Minimum TTL on incoming packets of the flow
MAX_TTL	53	1	Maximum TTL on incoming packets of the flow
IPV4_IDENT	54	2	The IP v4 identification field
DST_TOS	55	1	Type of Service byte setting when exiting outgoing interface
IN_SRC_MAC	56	6	Incoming source MAC address
OUT_DST_MAC	57	6	Outgoing destination MAC address
SRC_VLAN	58	2	Virtual LAN identifier associated with ingress interface
DST_VLAN	59	2	Virtual LAN identifier associated with egress interface
IP_PROTOCOL_VERSION	60	1	Internet Protocol Version Set to 4 for IPv4, set to 6 for IPv6. If not present in the template, then version 4 is assumed.
DIRECTION	61	1	Flow direction: 0 - ingress flow, 1 - egress flow
IPV6_NEXT_HOP	62	16	IPv6 address of the next-hop router
BGP_IPV6_NEXT_HOP	63	16	Next-hop router in the BGP domain
IPV6_OPTION_HEADERS	64	4	Bit-encoded field identifying IPv6 option headers found in the flow
Vendor Proprietary	65		
Vendor Proprietary	66		
Vendor Proprietary	67		
Vendor Proprietary	68		
Vendor Proprietary	69		
MPLS_LABEL_1	70	3	MPLS label at position 1 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_2	71	3	MPLS label at position 2 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_3	72	3	MPLS label at position 3 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_4	73	3	MPLS label at position 4 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_5	74	3	MPLS label at position 5 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_6	75	3	MPLS label at position 6 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_7	76	3	MPLS label at position 7 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_8	77	3	MPLS label at position 8 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_9	78	3	MPLS label at position 9 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
MPLS_LABEL_10	79	3	MPLS label at position 10 in the stack. This comprises 20 bits of MPLS label, 3 EXP (experimental) bits and 1 S (end-of-stack) bit.
IN_DST_MAC	80	6	Incoming destination MAC address
OUT_SRC_MAC	81	6	Outgoing source MAC address

Field Type	Value	Length (bytes)	Description
IF_NAME	82	N (default specified in template)	Shortened interface name i.e.: "FE1/0"
IF_DESC	83	N (default specified in template)	Full interface name i.e.: "FastEthernet 1/0"
SAMPLER_NAME	84	N (default specified in template)	Name of the flow sampler
IN_PERMANENT_BYTES	85	N (default is 4)	Running byte counter for a permanent flow
IN_PERMANENT_PKTS	86	N (default is 4)	Running packet counter for a permanent flow
* Vendor Proprietary*	87		
FRAGMENT_OFFSET	88	2	The fragment-offset value from fragmented IP packets
FORWARDING STATUS	89	1	<p>Forwarding status is encoded on 1 byte with the 2 left bits giving the status and the 6 remaining bits giving the reason code.</p>  <p>Status is either unknown (00), Forwarded (10), Dropped (10) or Consumed (11).</p> <p>Below is the list of forwarding status values with their means.</p> <p>Unknown</p> <ul style="list-style-type: none"> • 0 <p>Forwarded</p> <ul style="list-style-type: none"> • Unknown 64 • Forwarded Fragmented 65 • Forwarded not Fragmented 66 <p>Dropped</p> <ul style="list-style-type: none"> • Unknown 128, • Drop ACL Deny 129, • Drop ACL drop 130, • Drop Unroutable 131, • Drop Adjacency 132, • Drop Fragmentation & DF set 133, • Drop Bad header checksum 134, • Drop Bad total Length 135, • Drop Bad Header Length 136, • Drop bad TTL 137, • Drop Policer 138, • Drop WRED 139, • Drop RPF 140, • Drop For us 141, • Drop Bad output interface 142, • Drop Hardware 143, <p>Consumed</p> <ul style="list-style-type: none"> • Unknown 192, • Terminate Punt Adjacency 193, • Terminate Incomplete Adjacency 194, • Terminate For us 195
MPLS PAL RD	90	8 (array)	MPLS PAL Route Distinguisher.

Field Type	Value	Length (bytes)	Description
MPLS PREFIX LEN	91	1	Number of consecutive bits in the MPLS prefix length.
SRC TRAFFIC INDEX	92	4	BGP Policy Accounting Source Traffic Index
DST TRAFFIC INDEX	93	4	BGP Policy Accounting Destination Traffic Index
APPLICATION DESCRIPTION	94	N	Application description.
APPLICATION TAG	95	1+n	8 bits of engine ID, followed by n bits of classification.
APPLICATION NAME	96	N	Name associated with a classification.
postipDiffServCodePoint	98	1	The value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services Field, after modification.
replication factor	99	4	Multicast replication factor.
DEPRECATED	100	N	DEPRECATED
layer2packetSectionOffset	102		Layer 2 packet section offset. Potentially a generic offset.
layer2packetSectionSize	103		Layer 2 packet section size. Potentially a generic size.
layer2packetSectionData	104		Layer 2 packet section data.
	105 to 127		**Reserved for future use by cisco**

For the information on the field types with the numbers between 128 and 32768, please refer to the IANA registry of IPFIX information elements at <http://www.iana.org/assignments/ipfix>

When extensibility is required, the new field types will be added to the list. The new field types have to be updated on the Exporter and Collector but the NetFlow export format would remain unchanged.

In some cases the size of a field type is fixed by definition, for example PROTOCOL, or IPV4_SRC_ADDR. However in other cases they are defined as a variant type. This improves the memory efficiency in the collector and reduces the network bandwidth requirement between the Exporter and the Collector. As an example, in the case IN_BYTES, on an access router it might be sufficient to use a 32 bit counter (N = 4), on a core router a 64 bit counter (N = 8) would be required.

All counters and counter-like objects are unsigned integers of size N * 8 bits.

NetFlow Version 9 Data FlowSet Format

The format of the data FlowSet is described in Table 7, and the field descriptions are given in Table 8.

Table 7. NetFlow Version 9 Data FlowSet Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = Template ID															
Length															
Record 1 - Field 1 value															
Record 1 - Field 2 value															
Record 1 - Field 3 value															
Record 1 - Field 4 value															
.															
.															
.															
Record 1 - Field N value															
Record 2 - Field 1 value															

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Record 2 - Field 2 value															
Record 2 - Field 3 value															
.															
.															
.															
Record 2 - Field N value															
.															
.															
.															
Padding															

Table 8. NetFlow Version 9 Data FlowSet Field Descriptions

Field Name	Value
FlowSet ID = Template ID	A FlowSet ID precedes each group of records within a NetFlow Version 9 data FlowSet. The FlowSet ID maps to a (previously received) template ID. The collector and display applications should use the FlowSet ID to map the appropriate type and length to any field values that follow.
Length	This field gives the length of the data FlowSet. Length is expressed in TLV format, meaning that the value includes the bytes used for the FlowSet ID and the length bytes themselves, as well as the combined lengths of any included data records.
Record N – Field N	The remainder of the Version 9 data FlowSet is a collection of field values. The type and length of the fields have been previously defined in the template record referenced by the FlowSet ID/template ID.
Padding	Padding should be inserted to align the end of the FlowSet on a 32 bit boundary. Pay attention that the Length field will include those padding bits.

When interpreting the NetFlow Version 9 data FlowSet format, note that the fields cannot be parsed without a corresponding template ID. If a data FlowSet that does not have an appropriate template ID is received, the record should be discarded.

NetFlow Version 9 Options Template Format

One additional record type is very important within the NetFlow Version 9 specification: an options template (and its corresponding options data record). Rather than supplying information about IP flows, options are used to supply “meta-data” about the NetFlow process itself. The format of the options template is detailed in Table 9, and field descriptions are given in Table 10.

Table 9. NetFlow Version 9 Options Template

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = 1															
Length															
Template ID															
Option Scope Length															
Option Length															
Scope Field 1 Type															
Scope Field 1 Length															
.															

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.															
Scope Field N Length															
Option Field 1 Type															
Option Field 1 Length															
.															
.															
Option Field N Length															
Padding															

Table 10. NetFlow Version 9 Options Template Field Definitions

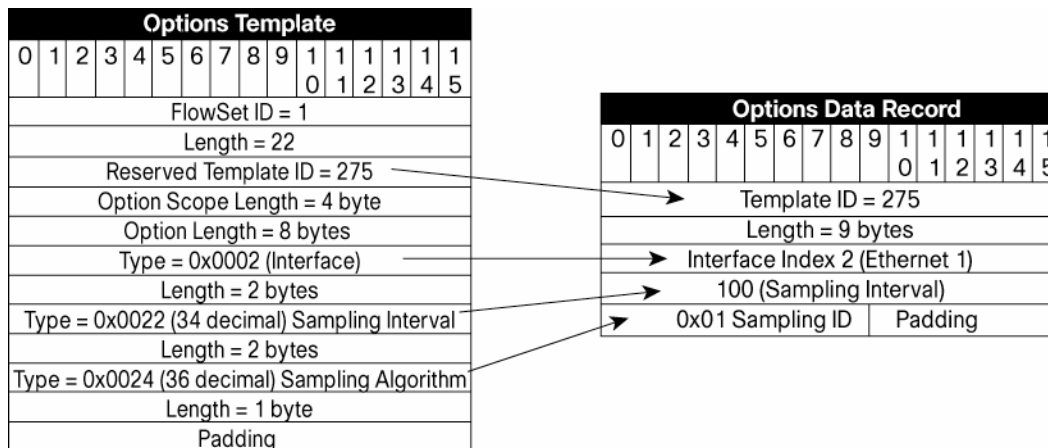
Field Name	Value
FlowSet ID = 1	The FlowSet ID is used to distinguish template records from data records. A template record always has a FlowSet ID of 1. A data record always has a nonzero FlowSet ID which is greater than 255.
Length	This field gives the total length of this FlowSet. Because an individual template FlowSet may contain multiple template IDs, the length value should be used to determine the position of the next FlowSet record, which could be either a template or a data FlowSet. Length is expressed in TLV format, meaning that the value includes the bytes used for the FlowSet ID and the length bytes themselves, as well as the combined lengths of all template records included in this FlowSet.
Template ID	As a router generates different template FlowSets to match the type of NetFlow data it will be exporting, each template is given a unique ID. This uniqueness is local to the router that generated the template ID. The Template ID is greater than 255. Template IDs inferior to 255 are reserved.
Option Scope Length	This field gives the length in bytes of any scope fields contained in this options template (the use of scope is described below).
Options Length	This field gives the length (in bytes) of any Options field definitions contained in this options template.
Scope Field 1 Type	This field gives the relevant portion of the NetFlow process to which the options record refers. Currently defined values follow: <ul style="list-style-type: none"> • 0x0001 System • 0x0002 Interface • 0x0003 Line Card • 0x0004 NetFlow Cache • 0x0005 Template For example, sampled NetFlow can be implemented on a per-interface basis, so if the options record was reporting on how sampling is configured, the scope for the report would be 0x0002 (interface).
Scope Field 1 Length	This field gives the length (in bytes) of the Scope field, as it would appear in an options record.
Option Field 1 Type	This numeric value represents the type of the field that appears in the options record. Possible values are detailed in Table 6 above.
Option Field 1 Length	This number is the length (in bytes) of the field, as it would appear in an options record.
Padding	Padding should be inserted to align the end of the FlowSet on a 32 bit boundary. Pay attention that the Length field will include those padding bits.

Examples

Example 1

Figure 1 shows an example of the options template.

Figure 1. Options Template Example



Example 2

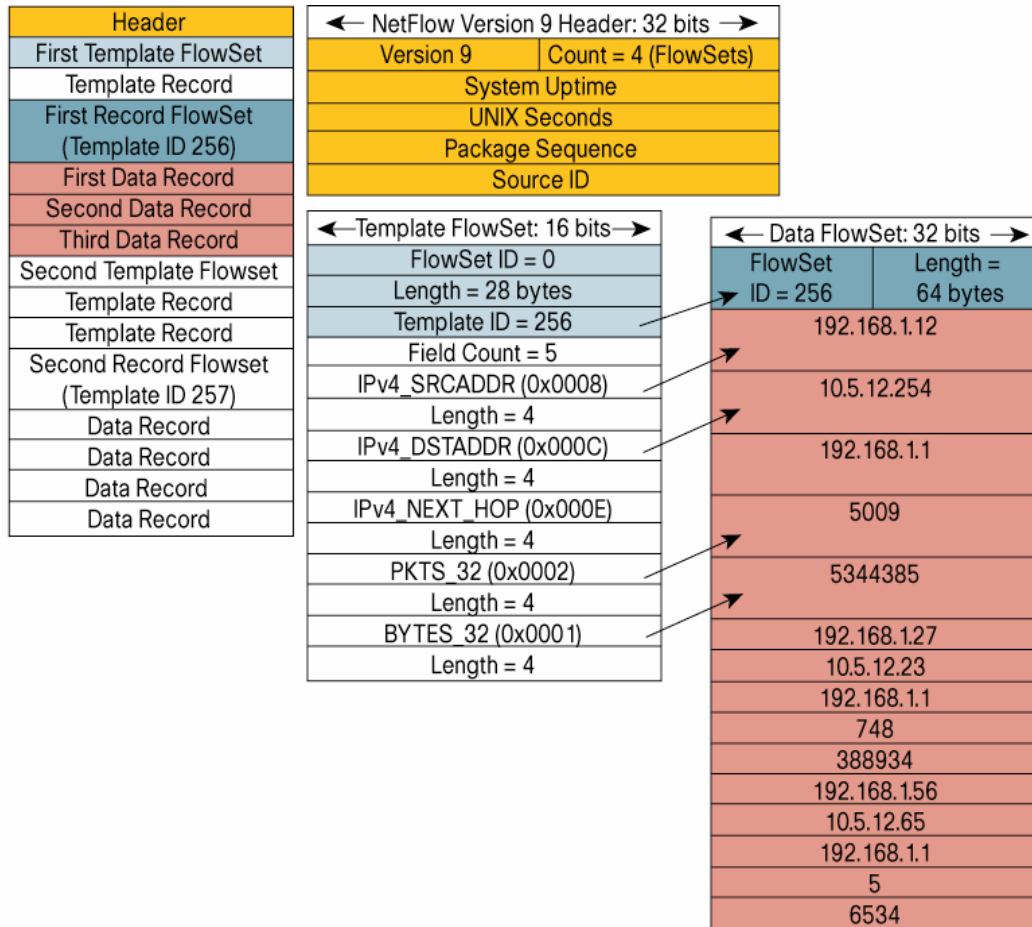
In this example, we are reporting the following 3 Flow records:

Src IP addr.	Dst IP addr.	Next Hop addr.	Packet Number	Bytes
198.168.1.12	10.5.12.254	192.168.1.1	5009	5344385
192.168.1.27	10.5.12.23	192.168.1.1	748	388934
192.168.1.56	10.5.12.65	192.168.1.1	5	6534

Figure 2 diagrams the NetFlow Version 9 export packet. Note the following:

- Export packets can be composed of both template and data FlowSets
- Template and data FlowSets can be interleaved
- The template ID in the template record maps to the FlowSet ID in a corresponding data FlowSet
- The layout of the data in the data record maps to the fields formats defined in the template record
- Although in this example the template FlowSet that defines template ID 256 happens to be followed by data FlowSets that reference template ID 256, this setup is for illustration purposes only. Data records are not necessarily preceded by their corresponding template within an export packet.

Figure 2. NetFlow Version 9 Export Packet Example



The Collector or Mediation Device

The Collector will receive template definitions from the Exporter, normally before receiving Flow Records. The Flow Records can then be decoded and stored locally on the devices. In case the template definitions have not been received at the time a Flow Record is received, the Collector should keep the Flow Record for later decode once the template definitions are received. A Collector device must not assume that the Data FlowSet and the associated Template IDs are exported in the same Export Packet.

The Collector must not assume that one and only one Template FlowSet is present in an Export Packet; in rare circumstances, the Export Packet may contain several Template FlowSets.

Templates live only for a certain timeframe. The lifetime of a Template should be deducted on the Collector based upon the time where the last Template FlowSet was received from the Exporter. The collector must not attempt to decode the Flow Records with an expired Template. The Collector should maintain a similar list:

<Exporter, Export Interface, Template ID, Template ID, Template Def, Last Received>

If a new Template definition is received (for example in case of an Exporter restart) it should immediately override the existing definition.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA

C11-395693-01 06/11