SOLARWINDS WHITEPAPER

NetFlow v9 Datagram

Brad Hale

Table of Contents

NetFlow Overview

Network traffic monitoring is a critical component of an overall network management framework and one of the most common ways to monitor network traffic is through the analysis of flow data. By analyzing flow data, a picture of network traffic flow and volume can be built. In other words, where the traffic is coming from, where it is going to, and how much is being generated.

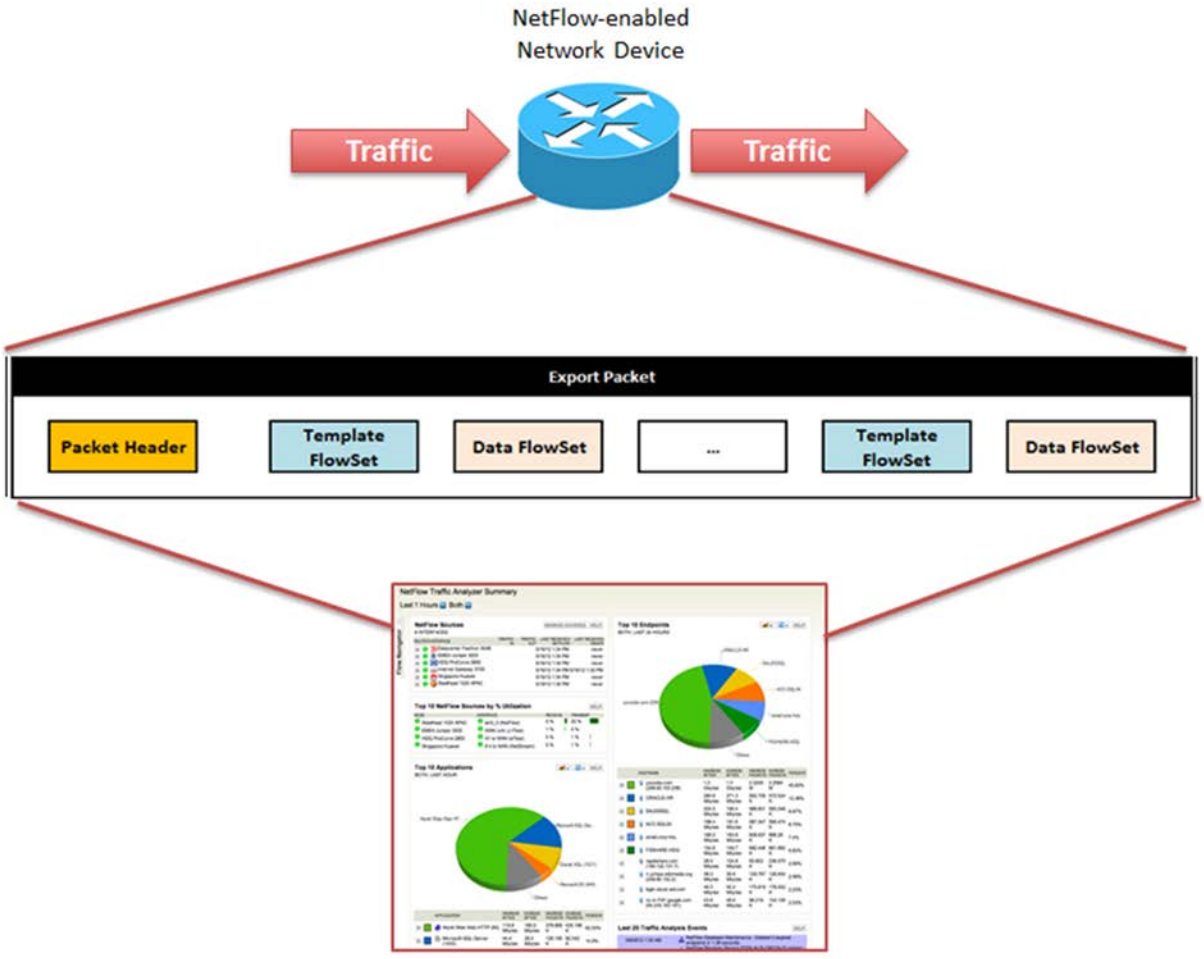
The intent of this paper is to provide the IT professional a basic understanding of how flow technology works, specifically Cisco's NetFlow v9, what metrics are being captured, and how they are interpreted.

Let's take a quick tour on the basics of NetFlow technology in this first part of the Knowledge Series.

What is NetFlow?

NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information and monitoring network traffic. While the term NetFlow has become a de-facto industry standard many other manufacturers support alternative flow technologies including; Juniper (Jflow); 3Com/HP, Dell and Netgear (s-flow); Huawei (NetStream); Alcatel-Lucent (Cflow); and Ericsson (Rflow).

Routers and switches that support NetFlow collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as NetFlow records, toward at least one NetFlow collector – typically a server that does the actual traffic analysis. The NetFlow collector then processes the data to perform the traffic analysis and presentation in a user-friendly format. NetFlow collectors can take the form of hardware based collectors or probes, or software based collectors. ***SolarWinds NetFlow Traffic Analyzer*** (NTA) is an example of a software based NetFlow collector that collects traffic data, correlates it into a useable format, and then presents it to the user in a web based interface.



SolarWinds NetFlow Traffic Analyzer

History of NetFlow

NetFlow v1 was originally introduced in 1990 and has since evolved to NetFlow version 9. Today, the most common versions are v5 and v9.

Version	Comment
v1	First implementation, now obsolete, and restricted to IPv4 (without IP mask and AS Numbers).
v2	Cisco internal version, never released.
v3	Cisco internal version, never released.
v4	Cisco internal version, never released.
v5	Most common version, available (as of 2009) on many routers from different brands, but restricted to IPv4 flows.
v6	No longer supported by Cisco. Encapsulation information.
v7	Like version 5 with a source router field. Used on Cisco Catalyst switches.
v8	Several aggregation form, but only for information that is already present in version 5 records
v9	Template Based, available (as of 2009) on some recent routers. Mostly used to report flows like IPv6, MPLS, or even plain IPv4 with BGP nexthop.
v10	aka IPFIX, IETF Standardized NetFlow 9 with several extensions like Enterprise-defined fields types, and variable length fields.

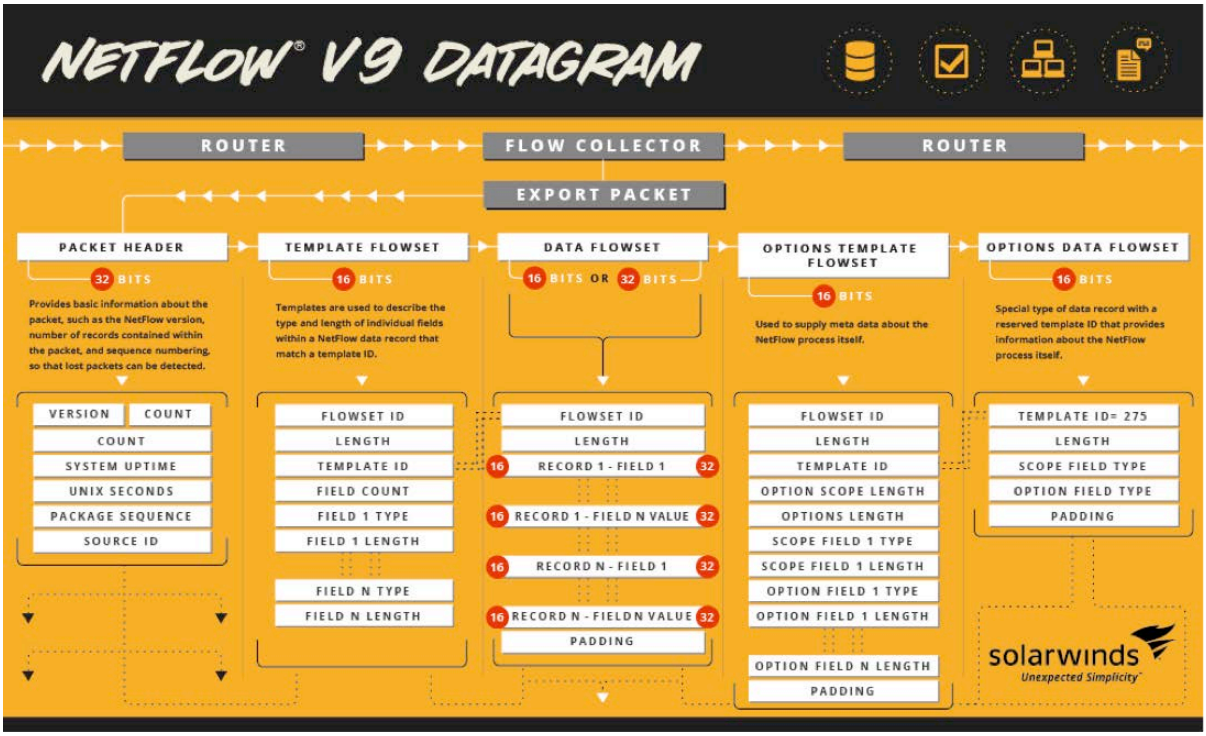
Benefits of Using NetFlow Technology for Monitoring Network Traffic

Monitoring and analyzing NetFlow will help obtain valuable information about network users and applications, peak usage times, and traffic routing. In contrast with traditional SNMP-dependent systems, NetFlow-based traffic monitoring has the ability to characterize traffic from applications and users, understand the traffic patterns, provide a holistic view into bandwidth utilization and WAN traffic, support CBQoS validation and performance monitoring, be used for network traffic forensics, and aid in compliance reporting.

Understanding the Datagram

The NetFlow Export datagram consists of a header and a sequence of flow records. The header contains information such as sequence number, record count, and sysuptime. The flow record contains flow information such as IP addresses, ports, and routing information.

Below is a simple datagram for NetFlow v9 that we will use throughout this paper to provide a detailed breakdown of the details of the NetFlow Export Packet format.

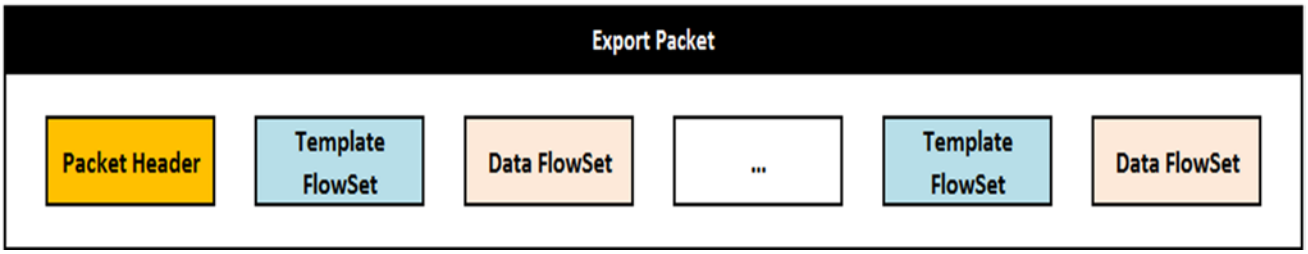


NetFlow v9 Packet Header

The NetFlow Packet Header provides basic information about the packet such as the NetFlow version, number of records contained within the packet, and sequence numbering, so that lost packets can be detected. All NetFlow packets begin with version-dependent header that contains at least these fields:

- Version number (v5, v8, v9, v10)
- Sequence number to detect loss and duplication
- Timestamps at the moment of export, as system uptime or absolute time.
- Number of records (v5 or v8) or list of templates and records (v9)

The NetFlow Version 9 record format consists of a packet header followed by at least one or more template or data FlowSets. The combination of packet header, and one or more template and data FlowSets is called an 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)



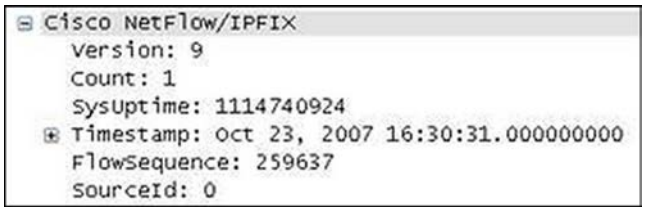
NetFlow v9 Packet Header Format

Packet Header																															
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 (2 bytes)																Count (2 bytes)															
System Uptime (4 bytes)																															
Unix Seconds (4 bytes)																															
Package Sequence (4 bytes)																															
Source ID (4 bytes)																															

Nomenclature	
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.

Sample Packet Header Data



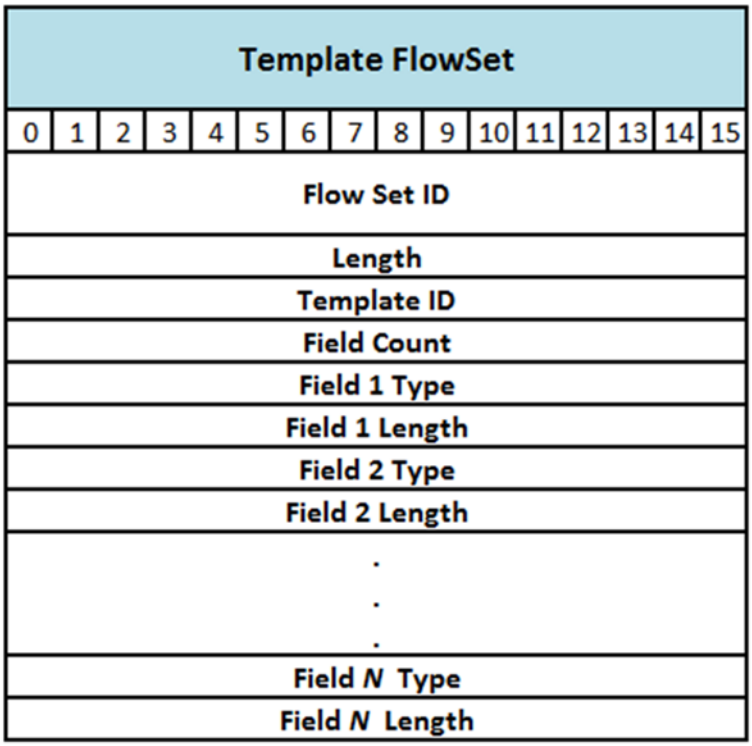
NetFlow v9 Template Flowset

Following the packet header, the FlowSet is an export packet containing 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** is a collection of one or more template records that have been grouped together in an export packet. 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.
- **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** 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.

NetFlow v9 Template FlowSet Format



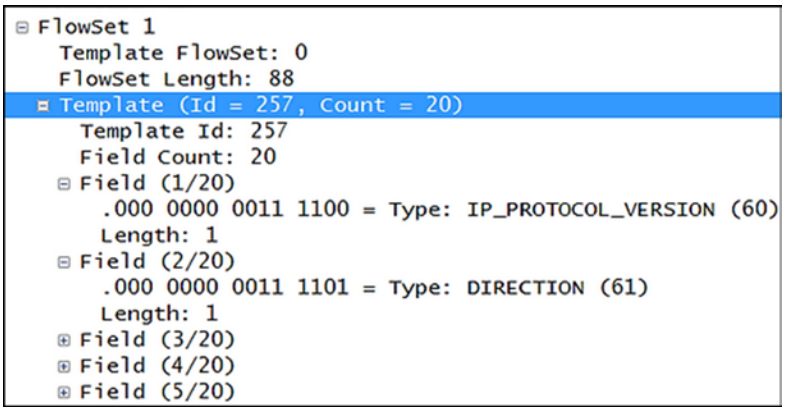
Nomenclature	
FlowSet ID	The FlowSet ID is used to distinguish template records from data records. A template record always has a FlowSet ID in the range of 0-255. Currently, the template record that describes flow fields has a FlowSet ID of zero and the template record that describes option fields (described 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 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:

- 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.

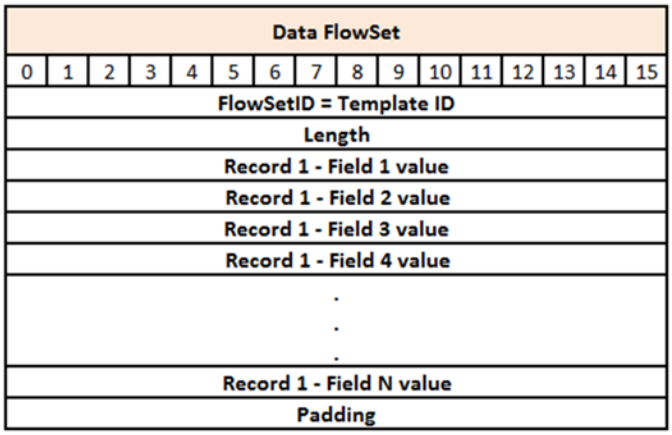
Sample Template FlowSet Data



NetFlow v9 Data FlowSet

The **Data FlowSet** is a collection of one or more data records that have been grouped together in an export packet. 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.

NetFlow v9 Data FlowSet Format



Data FlowSet															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSetID = 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															
Padding															

Nomenclature	
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.

Note: 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.

Sample Data FlowSet:

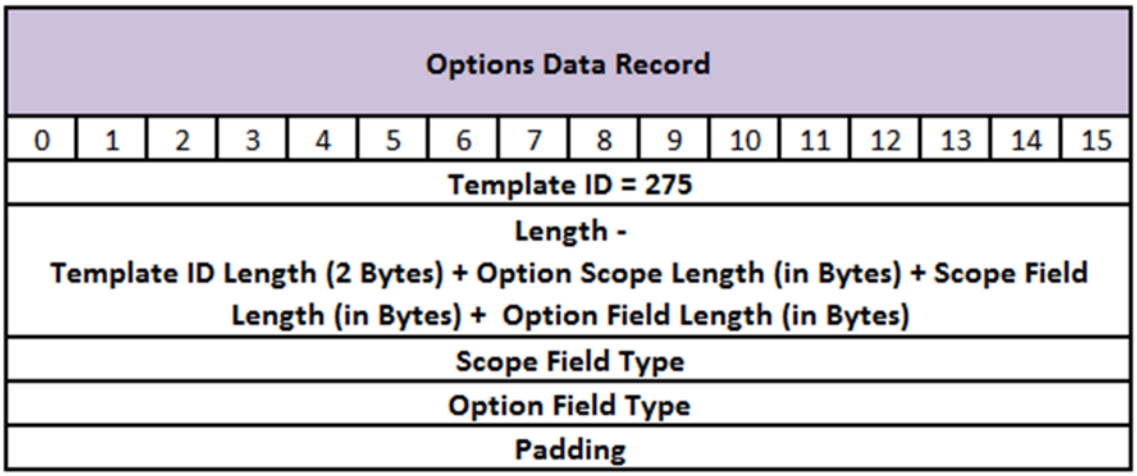
Data Flow Set: 32 bits	
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Flow Set ID = 256	Length = 64 Bytes
Record 1 Field 1 = 192.168.1.12	
Record 1 Field 2 = 10.5.12.254	
Record 1 Field 3 = 192.168.1.1	
Record 1 Field 4 = 5009	
Record 1 Field 5 = 5344385	
Record 2 Field 1 = 192.168.1.27	
Record 2 Field 2 = 10.5.12.23	
Record 2 Field 3 = 192.168.1.1	
Record 2 Field 4 = 748	
Record 2 Field 5 = 388934	
Record 3 Field 1 = 192.168.1.56	
Record 3 Field 2 = 10.5.12.65	
Record 3 Field 3 = 192.168.1.1	
Record 3 Field 4 = 5	
Record 3 Field 5 = 6534	

NetFlow v9 Options Template

The Options Template is a special type of template record used to communicate the format of data related to the NetFlow process.

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

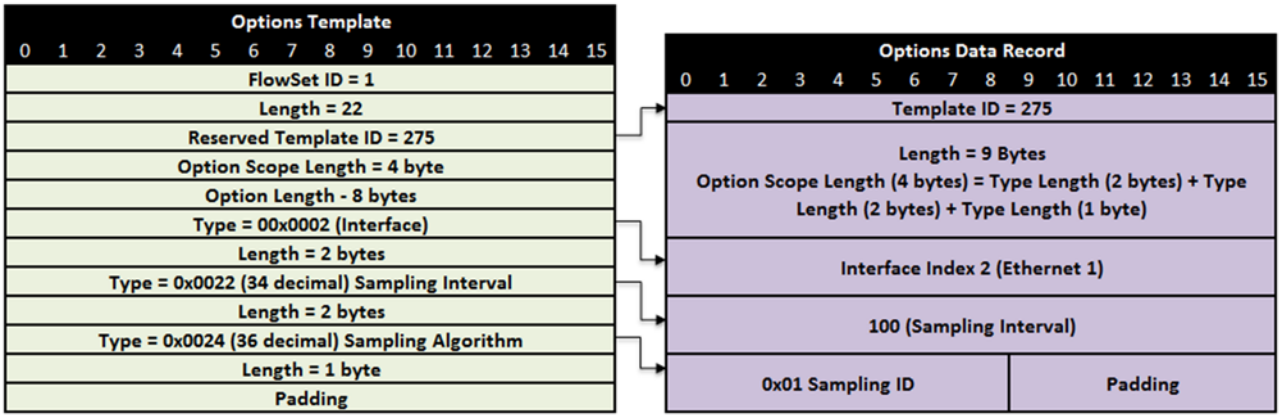
The **Options Data Record** is a special type of data record (based on an options template) with a reserved template ID that, rather than supplying information about IP flows, is used to supply "meta-data" about the NetFlow process itself



Nomenclature	
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: • 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.

Sample Options Template Data:



SolarWinds NetFlow Traffic Analyzer

SolarWinds NetFlow Analyzer (NTA) monitors network traffic by capturing flow data from network devices, including Cisco® NetFlow v5 or v9, Juniper® J-Flow, IPFIX, sFlow®, and Huawei NetStream™, and identifies which users, applications, and protocols are consuming the most bandwidth and highlights the IP addresses of the top talkers.

SolarWinds NTA helps you capture Cisco NetFlow (v5 or v9) data from continuous streams of network traffic passing through NetFlow-enabled network devices and convert the raw metrics of the Export Packet into easy-to-interpret charts and tables that quantify exactly how, by whom, and for what purpose the corporate network is being used.

Intelligent and Intuitive Dashboards

You can view key metrics in 'summary' or in 'detail' in the following categories:

- Applications
- Conversations
- Countries
- Endpoints
- IP Address Groups
- Protocols
- Receivers
- Types of Service
- Transmitters
- Border Gateway Protocol (BGP)

You can also access the data most critical to your network instantly by setting up Cisco NetFlow (v5 or v9) network traffic views.

Alerting and Reporting in SolarWinds NTA

- Set pre-defined thresholds and customize how you want to receive alerts, when and by what condition or threshold
- You can automate scheduling reports and leverage the reports available out of the box for instant use. SolarWinds NTA includes out-of-the-box reports for:
    - Top 100 Applications
    - Top 100 Conversations
    - Top 100 Conversations including applications
    - Top 20 Traffic Destinations By Domain
    - Top 20 Traffic Sources By Domain
    - Top 5 Protocols
    - Top 5 Traffic Destinations By IP Address Group
    - Top 5 Traffic Sources By IP Address Group
    - Top 50 Endpoints
    - Top 50 Endpoints by Unique Partners
    - Top 50 Receivers
    - Top 50 Receivers by Unique Partners
    - Top 50 Transmitters
    - Top 50 Transmitters by Unique Partners

More Information from *Cisco* on NetFlow v9

Learn more about how *SolarWinds NetFlow Analyzer* can help you with network traffic analysis and monitoring

Check out SolarWinds NetFlow Traffic Analyzer *live online demo*

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds online user community, *http://thwack.com*, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company's products. Learn more today at *http://solarwinds.com*.