



Cisco IOS Flexible NetFlow Overview

First Published: June 19, 2006
Last Updated: October 10, 2008

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow makes it easier to create more complex configurations for traffic analysis and data export through the use of reusable configuration components.

This module provides an overview of Flexible NetFlow and the advanced Flexible NetFlow features and services.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About Flexible NetFlow, page 1](#)
- [Where to Go Next, page 13](#)
- [Additional References, page 14](#)

Information About Flexible NetFlow

The following sections contain information about Flexible NetFlow.

- [Typical Uses for NetFlow, page 2](#)
- [Flows, page 3](#)
- [Original NetFlow and Flexible NetFlow, page 3](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- [Flexible NetFlow Components, page 5](#)
- [Security Detection with Flexible NetFlow, page 11](#)
- [Feature Comparison of Original NetFlow and Flexible NetFlow, page 11](#)

Typical Uses for NetFlow

NetFlow is typically used for several key customer applications, including the following:

- **Network monitoring.** NetFlow data enables extensive near-real-time network monitoring capabilities. Flow-based analysis techniques are used to visualize traffic patterns associated with individual routers and switches and network-wide traffic patterns (providing aggregate traffic or application-based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution.
- **Application monitoring and profiling.** NetFlow data enables network managers to gain a detailed time-based view of application usage over the network. This information is used to plan, understand new services, and allocate network and application resources (for example, web server sizing and voice over IP (VoIP) deployment) to meet customer demands responsively.
- **User monitoring and profiling.** NetFlow data enables network engineers to gain detailed understanding of customer and user use of network and application resources. This information may then be used to efficiently plan and allocate access, backbone, and application resources and to detect and resolve potential security and policy violations.
- **Network planning.** NetFlow can be used to capture data over a long period of time, affording the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, and higher-bandwidth interfaces. NetFlow services data optimizes network planning for peering, backbone upgrades, and routing policy. NetFlow helps to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and quality of service (QoS), and allows the analysis of new network applications. NetFlow will give you valuable information to reduce the cost of operating your network.
- **Security analysis.** NetFlow identifies and classifies distributed denial of service (DDoS) attacks, viruses, and worms in real time. Changes in network behavior indicate anomalies that are clearly demonstrated in Flexible NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents.
- **Billing and accounting.** NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS) and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization.
- **NetFlow data warehousing and data mining.** NetFlow data (or derived information) can be warehoused for later retrieval and analysis in support of proactive marketing and customer service programs (for example, figuring out which applications and services are being used by internal and

external users and targeting them for improved service, advertising, and so on). In addition, Flexible NetFlow data gives market researchers access to the “who,” “what,” “where,” and “how long” information relevant to enterprises and service providers.

Flows

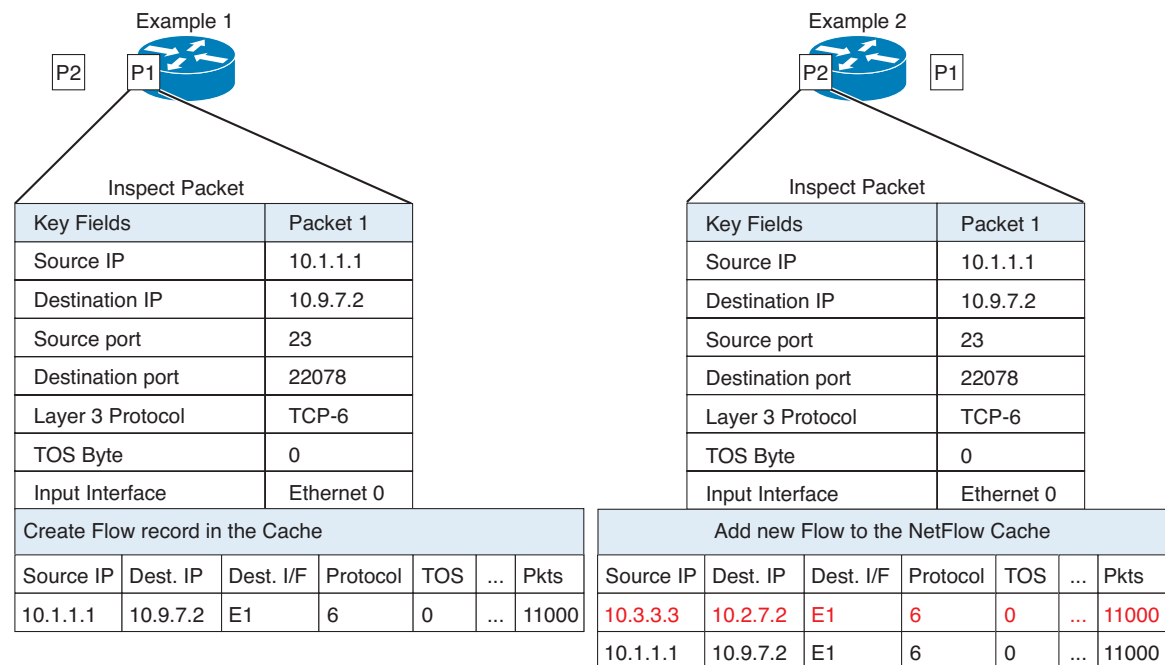
Original NetFlow and Flexible NetFlow both use the concept of flows. A *flow* is defined as a stream of packets between a given source and a given destination.

Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. When the value of the data in the key field of a datagram is unique with respect to the flows that already exist, a new flow is created.

Original NetFlow and Flexible NetFlow both use non-key fields as the criteria for identifying fields from which data is captured from the flows. The flows are populated with data that is captured from the values in the non-key fields.

Figure 1 is an example of the process for inspecting packets and creating flow records in the cache. In this example, two unique flows are created in the cache because there are different values in the source and destination IP address key fields.

Figure 1 Packet Inspection



Original NetFlow and Flexible NetFlow

Original NetFlow uses a fixed seven tuple of IP information to identify a flow. The new flexible concept allows the flow to be user defined. The benefits of Flexible NetFlow include:

Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform traffic analysis and data export. The user-defined flow records and the component structure of Flexible NetFlow make it easy for you to create various configurations for traffic analysis and data export on a networking device with a minimum number of configuration commands. Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The same flow monitor can be used in conjunction with different flow samplers to sample the same type of network traffic at different rates on different interfaces. The following sections provide more information on Flexible NetFlow components:

- [Records, page 5](#)
- [Flow Monitors, page 7](#)
- [Flow Exporters, page 9](#)
- [Flow Samplers, page 11](#)

Records

In Flexible NetFlow a combination of key and non-key fields is called a *record*. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data. Flexible NetFlow includes several predefined records that can help you get started using Flexible NetFlow. To use Flexible NetFlow to its fullest potential, you need to create your own customized records.

- [NetFlow Predefined Records, page 5](#)
- [User-Defined Records, page 6](#)

NetFlow Predefined Records

Flexible NetFlow includes several predefined records that you can use right away to start monitoring traffic in your network. The predefined records are available to help you quickly deploy Flexible NetFlow and are easier to use than user-defined flow records. You can choose from a list of already defined records that may meet the needs for network monitoring. As Flexible NetFlow evolves, popular user-defined flow records will be made available as predefined records to make them easier to implement.

The predefined records ensure backward compatibility with your existing NetFlow collector configurations for the data that is exported. Each of the predefined records has a unique combination of key and non-keys fields that offer you the built-in ability to monitor various types of traffic in your network without customizing Flexible Netflow on your router.

Two of the predefined records (NetFlow original¹ and NetFlow IPv4/IPv6 original output) emulate original (ingress) NetFlow and the Egress NetFlow Accounting feature in original NetFlow, respectively. Some of the other Flexible NetFlow predefined records are based on the aggregation cache schemes available in original NetFlow. The Flexible NetFlow predefined records that are based on the aggregation cache schemes available in original NetFlow do not perform aggregation. Instead each flow is tracked separately by the predefined records.

1. The “Netflow Original” and “NetFlow IPv4/IPv6 original-input” predefined records are functionally equivalent.

If you want to learn more about the Flexible NetFlow predefined records, refer to the [“Getting Started with Configuring Cisco IOS Flexible NetFlow”](#) module or the [“Configuring Cisco IOS Flexible NetFlow with Predefined Records”](#) module.

User-Defined Records

Flexible NetFlow enables you to define your own records for a Flexible NetFlow flow monitor cache by specifying the key and non-key fields to customize the data collection to your specific requirements. When you define your own records for a Flexible NetFlow flow monitor cache, they are referred to as *user-defined records*. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow. Flexible NetFlow enables you to capture counter values such as the number of bytes and packets in a flow as non-key fields.

You can create user-defined records for applications such as QoS and bandwidth monitoring, application and end user traffic profiling, and security monitoring for denial of service (DoS) attacks. Flexible NetFlow also includes several predefined records that emulate original NetFlow.

Flexible NetFlow user-defined records provide the capability to monitor a contiguous section of a packet of a user-configurable size, and use it in a flow record as a key or a non-key field along with other fields and attributes of the packet. The section may potentially include any Layer 3 data from the packet.

The packet section fields allow the user to monitor any packet fields that are not covered by the Flexible NetFlow predefined keys. The ability to analyze packet fields that are not collected with the predefined keys enables more detailed traffic monitoring, facilitates the investigation of distributed denial of service (DDoS) attacks, and enables implementation of other security applications such as URL monitoring.

Flexible NetFlow provides predefined types of packet sections of a user-configurable size. The following Flexible NetFlow commands (used in flow record configuration mode) can be used to configure the predefined types of packet sections:

- **collect ipv4 section header size** *header-size*—Starts capturing the number of bytes specified by the *header-size* argument from the beginning of the IPv4 header of each packet.
- **collect ipv4 section payload size** *payload-size*—Starts capturing bytes immediately after the IPv4 header from each packet. The number of bytes captured is specified by the *payload-size* argument.
- **collect ipv6 section header size** *header-size*—Starts capturing the number of bytes specified by the *header-size* argument from the beginning of the IPv6 header of each packet.
- **collect ipv6 section payload size** *payload-size*—Starts capturing bytes immediately after the IPv6 header from each packet. The number of bytes captured is specified by the *payload-size* argument.

The *header-size* and *payload-size* values are the sizes in bytes of these fields in the flow record. If the corresponding fragment of the packet is smaller than the requested section size, Flexible NetFlow will fill the rest of the section field in the flow record with zeros. If the packet type does not match the requested section type, Flexible NetFlow will fill the entire section field in the flow record with zeros.

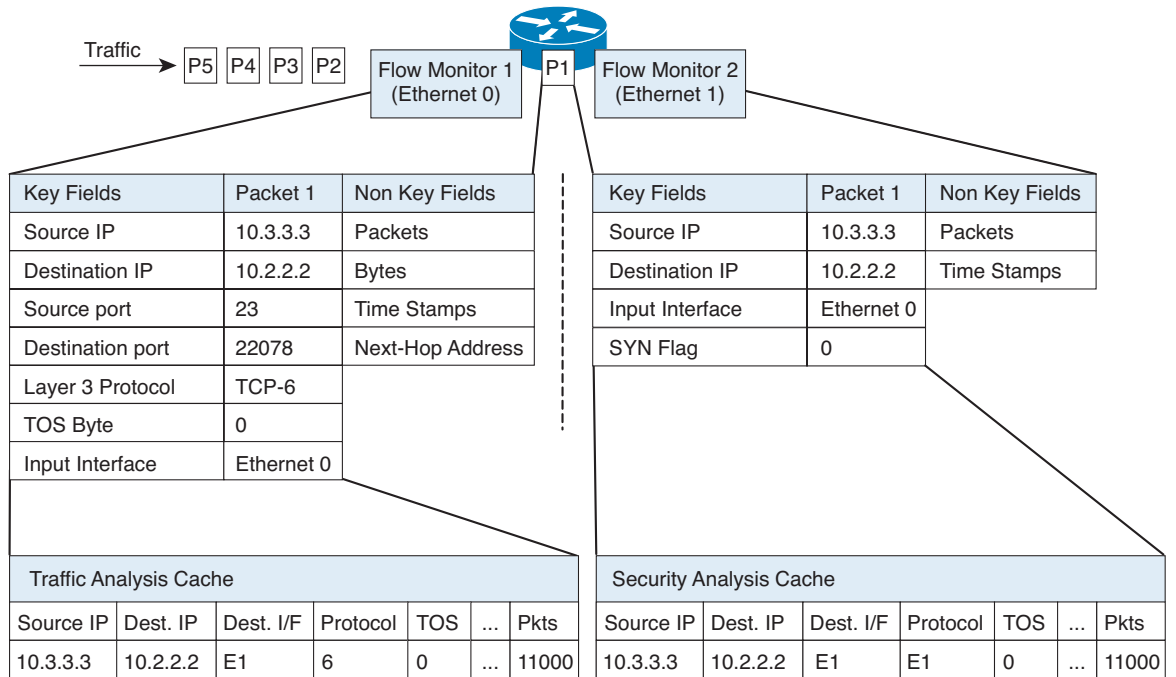
Flexible NetFlow adds a new Version 9 export format field type for the header and packet section types. Flexible NetFlow will communicate to the NetFlow collector the configured section sizes in the corresponding Version 9 export template fields. The payload sections will have a corresponding length field that can be used to collect the actual size of the collected section.

Flow Monitors

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a user-defined or predefined record, an optional flow exporter, and a cache that is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and non-key fields in the flow record.

Flexible NetFlow can be used to perform different types of analysis on the same traffic. In [Figure 3](#), packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

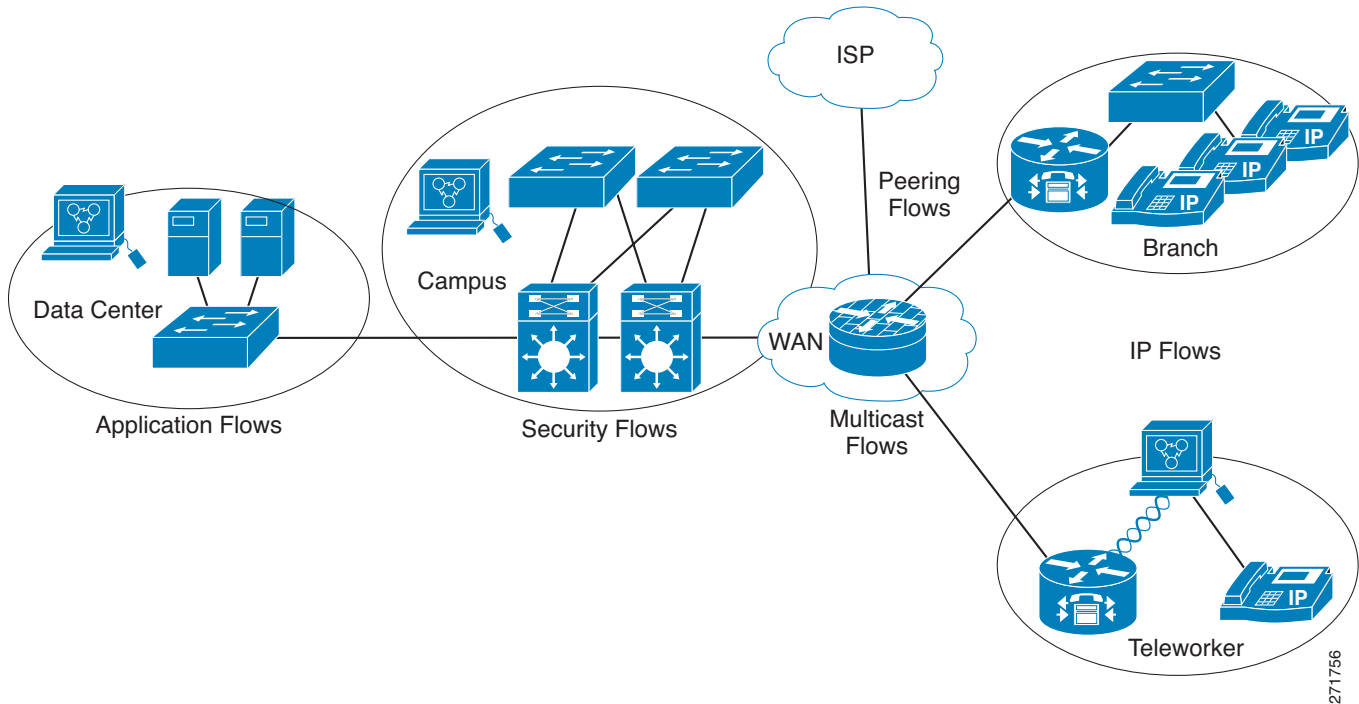
Figure 3 Example of Using Two Flow Monitors to Analyze the Same Traffic



271755

Figure 4 shows a more complex example of how you can apply different types of flow monitors with custom records.

Figure 4 Complex Example of Using Multiple Types of Flow Monitors with Custom Records



There are three types of flow monitor caches. You change the type of cache used by the flow monitor after you create the flow monitor. The three types of flow monitor caches are as follows:

- [Normal](#), page 8
- [Immediate](#), page 8
- [Permanent](#), page 9

Normal

The default cache type is “normal.” In this mode, the entries in the cache are aged out according to the timeout active and timeout inactive settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured.

Immediate

A cache of type “immediate” ages out every record as soon as it is created. As a result, every flow contains just one packet. The commands that display the cache contents will provide a history of the packets seen.

This mode is desirable when you expect only very small flows and you want a minimum amount of latency between seeing a packet and exporting a report.



Caution

This command may result in a large amount of export data that can overload low-speed links and overwhelm any systems that you are exporting to. We recommended that you configure sampling to reduce the number of packets that are processed.

**Note**

The cache timeout settings have no effect in this mode.

Permanent

A cache of type “permanent” never ages out any flows. A permanent cache is useful when the number of flows you expect to see is low and there is a need to keep long-term statistics on the router. For example, if the only key field in the flow record is the 8-bit IP ToS field, only 256 flows can be monitored. To monitor the long-term usage of the IP ToS field in the network traffic, a permanent cache can be used. Permanent caches are useful for billing applications and for an edge-to-edge traffic matrix for a fixed set of flows that are being tracked. Update messages will be sent periodically to any flow exporters configured according to the “timeout update” setting.

**Note**

When a cache becomes full in permanent mode, new flows will not be monitored. If this occurs, a “Flows not added” message will appear in the cache statistics.

**Note**

A permanent cache uses update counters rather than delta counters. This means that when a flow is exported, the counters represent the totals seen for the full lifetime of the flow and not the additional packets and bytes seen since the last export was sent.

Flow Exporters

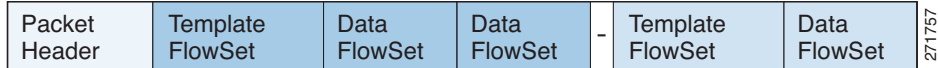
Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

NetFlow Data Export Format Version 9

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 export format is known as Version 9. The distinguishing feature of the NetFlow Version 9 export 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 do not have to recompile their applications each time a new NetFlow feature is added. Instead, they should be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow 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.

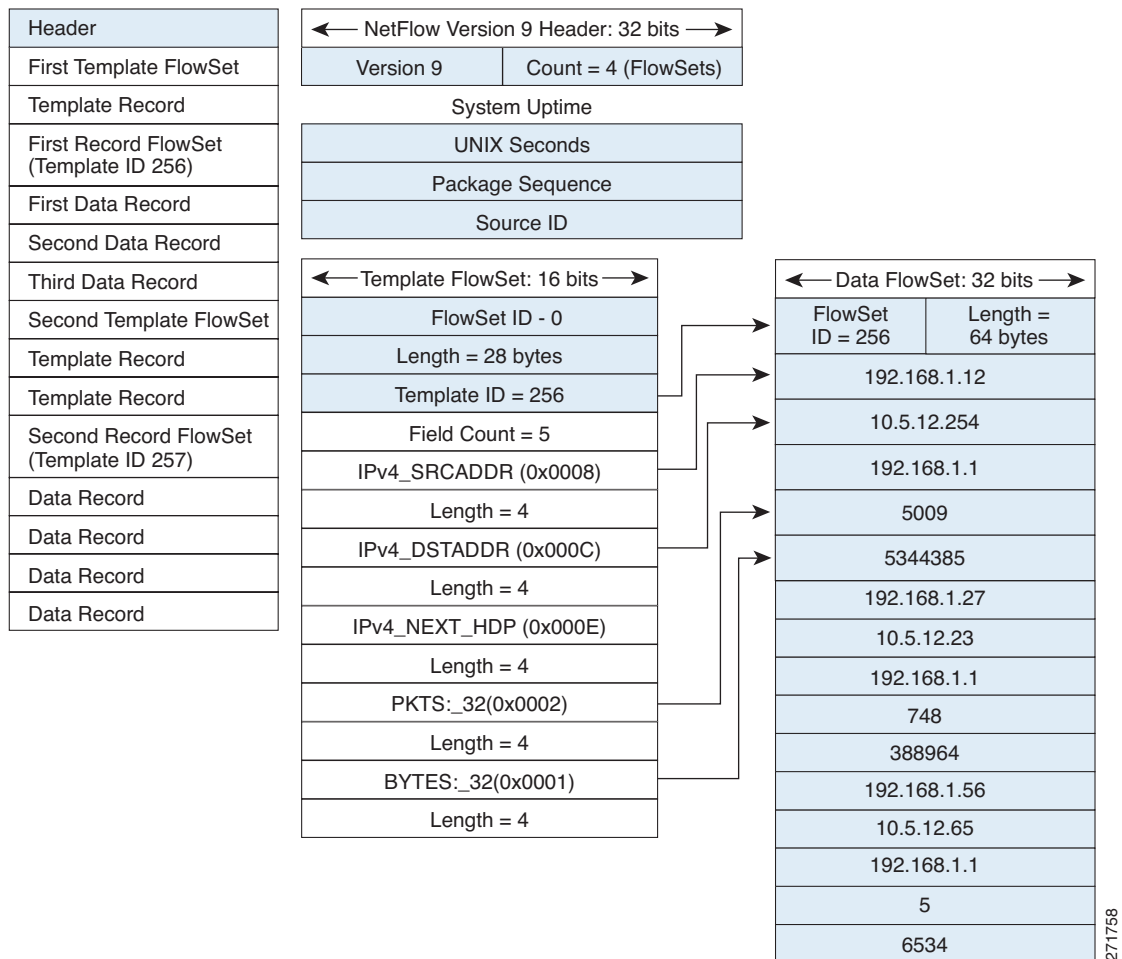
The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent export packets. Template flow and data flow sets can be intermingled within a single export packet, as illustrated in [Figure 5](#).

Figure 5 Version 9 Export Packet

NetFlow Version 9 will periodically export the template data so the NetFlow collector will understand what data is to be sent and also export the data flow set for the template. The key advantage to Flexible NetFlow is that the user configures a flow record, which is effectively converted to a Version 9 template and then forwarded to the collector. Figure 6 is a detailed example of the NetFlow Version 9 export format, including the header, template flow and data flow sets.

**Note**

The NetFlow Version 5 export format is a fixed export format that would provide limited information for Flexible NetFlow data. This is why Flexible Netflow uses the Version 9 export format.

Figure 6 Detailed Example of the NetFlow Version 9 Export Format

For more information on the Version 9 export format, refer to the white paper entitled *Cisco IOS NetFlow Version 9 Flow-Record Format*, available at this url:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml.

Flow Samplers

Flow samplers are used to reduce the load that Flexible NetFlow places on the networking device to monitor traffic by limiting the number of packets that are analyzed. You can configure a rate of sampling that is 1 out of a range of 2 to 32768 packets. For example, a sampling rate of 1 out of 2 results in the analysis of 50 percent of the packets processed by the networking device.

Flow samplers are applied to interfaces in conjunction with a flow monitor to implement Flexible NetFlow flow sampling. Packets are analyzed at the rate specified by the sampler and compared with the flow record associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

Security Detection with Flexible NetFlow

Flexible NetFlow can be used as a network attack detection tool with capabilities to track all parts of the IP header and even packet sections and characterize this information into flows. Security detection systems can listen to Flexible NetFlow data, and upon finding an issue in the network, create a virtual bucket or virtual cache that will be configured to track specific information and identify details about the attack pattern or worm propagation. The capability to create caches dynamically with specific information combined with input filtering (for example, filtering all flows to a specific destination) makes Flexible NetFlow a powerful security detection tool.

One common type of attack occurs when TCP flags are used to flood open TCP requests to a destination server (for example, a SYN flood attack). The attacking device sends a stream of TCP SYNs to a given destination address but never send the ACK in response to the servers SYN-ACK as part of the TCP three-way handshake. The flow information needed for security detection server requires the tracking of three key fields: destination address or subnet, TCP flags, and packet count. The security detection server may be monitoring general Flexible NetFlow information, and this data may trigger a detailed view of this particular attack by dynamically creating a new flow monitor in the router's configuration. The new flow monitor might include input filtering to limit what traffic is visible in the Flexible NetFlow cache along with the tracking of the specific information to diagnose the TCP-based attack. In this case the user may want to filter all flow information to the server destination address or subnet to limit the amount of information the security detection server needs to evaluate. If the security detection server decided it understood this attack, it might then program another flow monitor to collect and export payload information or sections of packets to take a deeper look at a signature within the packet. This example is just one of many possible ways that Flexible NetFlow can be used to detect security incidents.

Feature Comparison of Original NetFlow and Flexible NetFlow

Table 1 provides a feature-by-feature comparison of original NetFlow and Flexible NetFlow.

Table 1 Feature-by-Feature Comparison of Original NetFlow and Flexible NetFlow

Feature	Original NetFlow	Flexible NetFlow	Comments
NetFlow Data Capture	Supported	Supported	Data capture is available with the predefined ¹ and user-defined records in Flexible NetFlow.
NetFlow Data Export	Supported	Supported	Flow exporters export data from the Flexible NetFlow flow monitor caches to remote systems.

Table 1 Feature-by-Feature Comparison of Original NetFlow and Flexible NetFlow (continued)

Feature	Original NetFlow	Flexible NetFlow	Comments
NetFlow for IPv6	Supported	Supported	IPv6 support was removed from original NetFlow in Cisco IOS Release 12.4(20)T. The Flexible NetFlow - IPv6 Unicast Flows feature implemented IPv6 support for Flexible NetFlow in Cisco IOS Release 12.4(20)T.
MPLS-Aware NetFlow	Supported	Not supported	—
MPLS Egress NetFlow	Supported	Supported	The Flexible Netflow - MPLS Egress NetFlow feature implemented MPLS NetFlow egress support for Flexible NetFlow in Cisco IOS Release 12.4(22)T.
NetFlow BGP Next Hop Support	Supported	Supported	Available in the predefined and user-defined keys in Flexible NetFlow records.
Random Packet Sampled NetFlow	Supported	Supported	Available with Flexible NetFlow sampling.
NetFlow v9 Export Format	Supported	Supported	Available with Flexible NetFlow exporters.
NetFlow Subinterface Support	Supported	Supported	Flexible NetFlow monitors can be assigned to subinterfaces.
NetFlow Multiple Export Destinations	Supported	Supported	Available with Flexible NetFlow exporters.
NetFlow ToS-Based Router Aggregation	Supported	Supported	Available in the predefined and user-defined records in Flexible NetFlow records.
NetFlow Minimum Prefix Mask for Router-Based Aggregation	Supported	Supported	Available in the predefined and user-defined records.
NetFlow Input Filters	Supported	Not supported	—
NetFlow MIB	Supported	Not supported	—
NetFlow MIB and Top Talkers	Supported	Not supported	—

Table 1 Feature-by-Feature Comparison of Original NetFlow and Flexible NetFlow (continued)

Feature	Original NetFlow	Flexible NetFlow	Comments
NetFlow Multicast Support	Supported	Supported	In Cisco IOS release 12.4(9)T through 12.4(20)T Flexible NetFlow collects statistics for multicast flows. However, specific additional fields such as replication counts for bytes and packets are not supported. The Flexible Netflow - IPv4 Multicast Statistics Support feature implemented support for capturing multicast replication counts for bytes and packets in Cisco IOS Release 12.4(22)T.
NetFlow Layer 2 and Security Monitoring Exports	Supported	Partially supported	The Flexible Netflow - Layer 2 Fields feature implemented support for capturing MAC addresses and virtual LAN (VLAN) IDs in Cisco IOS Release 12.4(22)T.
Egress NetFlow Accounting	Supported	Supported	Flexible NetFlow monitors can be used to monitor egress traffic on interfaces and subinterfaces.
NetFlow Reliable Export with SCTP	Supported	Not supported	—
NetFlow Dynamic Top Talkers CLI	Supported	Supported	The Flexible Netflow - Top N Talkers Support feature implemented in Cisco IOS Release 12.4(22)T provides the same functionality.

1. Flexible NetFlow has several predefined keys that emulate the traffic analysis capabilities of original NetFlow.

Where to Go Next

To implement a basic Flexible NetFlow configuration that emulates original NetFlow traffic analysis and data export, refer to the [“Getting Started with Configuring Cisco IOS Flexible NetFlow”](#) module. To implement other Flexible NetFlow configurations, refer to the [“Related Documents”](#) section on page 14.

Additional References

The following sections provide references related to Flexible NetFlow.

Related Documents

Related Topic	Document Title
Flexible NetFlow Feature Roadmap	“Cisco IOS Flexible NetFlow Features Roadmap”
Emulating original NetFlow with Flexible NetFlow	“Getting Started with Configuring Cisco IOS Flexible NetFlow”
Configuring flow exporters to export Flexible NetFlow data	“Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters”
Customizing Flexible NetFlow for your network	“Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors”
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	“Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic”
Configuring Flexible NetFlow using predefined records	“Configuring Cisco IOS Flexible NetFlow with Predefined Records”
Using Flexible Netflow Top N Talkers to Analyze Network Traffic	“Using Cisco IOS Flexible Netflow Top N Talkers to Analyze Network Traffic”
Configuring IPv4 Multicast Statistics Support for Flexible NetFlow	“Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow”
Configuration commands for Flexible NetFlow	Cisco IOS Flexible NetFlow Command Reference

RFCs

RFC	Title
RFC #3954	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

