Cisco IOS NetFlow Overview

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology. This module provides an overview of the NetFlow application and advanced NetFlow features and services.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Cisco IOS NetFlow

The NetFlow Application

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol, either between routers or to any other networking device or end station. NetFlow does not require any change externally--either to the packets themselves or to any networking device. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

NetFlow is supported on IP and IP encapsulated traffic over most interface types and encapsulations. However, NetFlow does not support ATM LAN emulation (LANE) and does not support an Inter-Switch Link (ISL)/virtual LAN (VLAN), ATM, or Frame Relay interfaces when more than one input access control list (ACL) is used on the interface. Cisco 12000 IP Service Engine ATM line cards do not have this restriction when more than one input ACL is used on the interface.

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution data, IP flow switching cache information, and flow information. See the NetFlow Flows, on page 3.

NetFlow Benefits Monitoring Analysis and Planning Security and Accounting and Billing

NetFlow captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service (ToS) information that can be used for a wide variety of purposes such as network application and user monitoring, network analysis and planning, security analysis, accounting and billing, traffic engineering, and NetFlow data warehousing and data mining.

Network Application and User Monitoring

NetFlow data enables you to view detailed, time- and application-based usage of a network. This information allows you to plan and allocate network and application resources, and provides for extensive near real-time network monitoring capabilities. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection and efficient troubleshooting, and it facilitates rapid problem resolution. You can use NetFlow information to efficiently allocate network resources and to detect and resolve potential security and policy violations.

Network Planning

NetFlow can capture data over a long period of time, which enables you to track and anticipate network growth and plan upgrades. NetFlow service data can be used to optimize network planning, which includes peering, backbone upgrade planning, and routing policy planning. It also enables you 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) usage, and enables the analysis of new network applications. NetFlow offers valuable information that you can use to reduce the cost of operating the network.

Denial of Service and Security Analysis

You can use NetFlow data to identify and classify denial of service (DoS) attacks, viruses, and worms in real-time. Changes in network behavior indicate anomalies that are clearly reflected in NetFlow data. The data is also a valuable forensic tool that you can use to understand and replay the history of security incidents.

>Accounting and Billing

NetFlow data provides fine-grained metering for highly flexible and detailed resource utilization accounting. For example, flow data includes details such as IP addresses, packet and byte counts, timestamps,

type-of-service, and application ports. Service providers might utilize the information for billing based on time-of-day, bandwidth usage, application usage, or quality of service. Enterprise customers might utilize the information for departmental chargeback or cost allocation for resource utilization.

Traffic Engineering

NetFlow provides autonomous system (AS) traffic engineering details. You can use NetFlow-captured traffic data to understand source-to-destination traffic trends. This data can be used for load-balancing traffic across alternate paths or for forwarding traffic to a preferred route. NetFlow can measure the amount of traffic crossing peering or transit points to help you determine if a peering arrangement with other service providers is fair and equitable.

>NetFlow Data Storage and Data Mining

NetFlow data (or derived information) can be stored for later retrieval and analysis in support of marketing and customer service programs. For example, the data can be used to find out which applications and services are being used by internal and external users and to target those users for improved service and advertising. In addition, NetFlow data gives market researchers access to the who, what, where, and how long information relevant to enterprises and service providers.

NetFlow Cisco IOS Packaging Information

Cisco 7200/7500/7400/MGX/AS5800

Although NetFlow functionality is included in all software images for these platforms, you must purchase a separate NetFlow feature license. NetFlow licenses are sold on a per-node basis.

>Other Routers

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

NetFlow Flows

A NetFlow network flow is defined as a unidirectional stream of packets between a given source and destination. The source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is defined by the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might also contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format), depending on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Main Cache Operation

The key components of NetFlow are the NetFlow cache that stores IP flow information, and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers data for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers data for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers data for all egress MPLS-to-IP packets.

NetFlow Export Formats

NetFlow exports data in UDP datagrams in one of five formats: Version 9, Version 8, Version 7, Version 5, or Version 1. Version 9 export format, the latest version, is the most flexible and extensive format. Version 1 was the initial NetFlow export format; Version 7 is supported only on certain platforms, and Version 8 only supports export from aggregation cache. (Versions 2 through 4 and Version 6 were either not released or are not supported.)

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. The distinguishing feature of the NetFlow Version 9 format is that it is template based. Templates provide a means of extending the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Internet Protocol Information Export (IPFIX) was based on the Version 9 export format.

- Version 8--A format added to support data export from aggregation caches. Version 8 allows export datagrams to contain a subset of the usual Version 5 export data, if that data is valid for a particular aggregation cache scheme.
- Version 7--A version supported on Catalyst 6000 series switches with a Multilayer Switch Feature Card (MSFC) on CatOS Release 5.5(7) and later.

On Catalyst 6000 series switches with an MSFC, you can export using either the Version 7 or Version 8 format.

Information about and instructions for configuring NetFlow on Catalyst 6000 series switches is available in the Catalyst 6500 Series Switches documentation.

- Version 5--A version that adds BGP autonomous system (AS) information and flow sequence numbers.
- Version 1, the initially released export format, is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format for data export from the main cache.

For more information on a specific NetFlow data export format, see the "Configuring NetFlow and NetFlow Data Export" module.

NetFlow Operation Processing Order of NetFlow Features

The NetFlow application supports features that you can set up to further analyze network traffic data. NetFlow divides these features and services into the following three categories for processing:

- Preprocessing features that allow you to collect subsets of your network traffic data for analysis.
- Advanced features and services based on the flexible NetFlow Version 9 export format that allow you to collect data on types of traffic in addition to IP traffic.
- Postprocessing features that allow you to define fields that control how traffic data is exported.

You need to decide if you want to further analyze your network traffic. If you do want to do further analysis, you need to make choices in two areas:

- Do you want to customize or fine-tune the way that you collect NetFlow data? For example, you might want to configure packet sampling, or packet filtering, or an aggregation scheme.
- Do you want to collect and analyze data about the use of other Cisco IOS applications? For example, you might want to configure NetFlow support for BGP next hop, multicast, MPLS, or IPv6.

Before you configure or enable an additional NetFlow feature or service, you need to understand the prerequisites, restrictions, and key concepts that apply to each feature or service. Refer to the following sections for information about and links to the NetFlow features and services:

NetFlow Preprocessing Features Filtering and Sampling

The table below briefly describes preprocessing features and indicates where you can find concept and task information about each. You set up these features to select the subset of traffic of interest to you before NetFlow processing begins.

Table 1: NetFlow Preprocessing Features

Preprocessing Feature	Brief Description	Source for Concept and Task Information
Packet sampling	Sets up statistical sampling of network traffic for traffic engineering or capacity planning	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.
Filtering	Sets up a specific subset of network traffic for class-based traffic analysis and monitoring on-network or off-network traffic	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.

NetFlow Advanced Features and Services BGP Next Hop Multicast MPLS NetFlow Layer 2

The table below briefly describes advanced features and services supported by NetFlow and indicates where you can find concept and task information about each. Configure these features and services to collect and analyze NetFlow traffic statistics about them (features such as BGP Next Hop, multicast, and MPLS).

Table 2: NetFlow Advanced Features and Services

Feature or Service	Brief Description	Source for Concept and Task Information
BGP next hop support	Sets up the export of BGP next hop information for the purpose of measuring network traffic on a per BGP next hop basis	See the "Configuring NetFlow BGP Next Hop Support for Accounting and Analysis" module.
Multicast support	Sets up the capture of multicast-specific data that allows you to get a complete multicast traffic billing solution	See the "Configuring NetFlow Multicast Accounting" module.
MPLS support	Sets up the capture of MPLS traffic containing both IP and non-IP packets for use in MPLS network management, network planning, and enterprise accounting	See the "Configuring MPLS-aware NetFlow" module.
NetFlow Layer 2 and Security Monitoring Exports	Sets up the capture of Layer 2 and Layer 3 fields for use in security monitoring, network management, network planning, and enterprise accounting	See the "NetFlow Layer 2 and Security Monitoring Exports" module.

NetFlow Postprocessing Features Aggregation Schemes and Export to Multiple Destinations

The table below briefly describes postprocessing features and indicates where you can find concept and task information about each. You configure these features to set up the export of NetFlow data.

Table 3: NetFlow Postprocessing Features

Postprocessing Features	Brief Description	Source for Concept and Task Information
Aggregation schemes	Sets up extra aggregation caches with different combinations of fields that determine which traditional flows are grouped together and collected when a flow expires from the main cache	"Configuring NetFlow Aggregation Caches"
Export to multiple destinations	Sets up identical streams of NetFlow data to be sent to multiple hosts	"Configuring NetFlow and NetFlow Data Export"

NetFlow MIBs

The NetFlow MIB and the NetFlow MIB and Top Talkers features provide real time access to NetFlow cache information. These feature do not require a collector to obtain NetFlow data. This allows smaller enterprises to collect NetFlow data.

With the NetFlow MIB feature, you can access in real time the system information that is stored in the NetFlow cache by utilizing a MIB implementation based on the Simple Network Management Protocol (SNMP). This information is accessed by **get** and **set** commands entered on the network management system (NMS) workstation for which SNMP has been implemented. The NetFlow MIB feature provides MIB objects that allow you to monitor cache flow information, the current NetFlow configuration, and statistics. For details about the NetFlow MIB, see the "Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data" module.

The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. You can use this feature for security monitoring or accounting purposes for top talkers, and matching and identifying addresses for key users of the network. You configure the criteria by which flows from the NetFlow cache are sorted and placed in a special cache. The flows that are displayed by this feature are known as "top talkers." For details about the NetFlow MIB and Top Talkers, see the "Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands" module.

How to Configure Cisco IOS NetFlow

There are no tasks for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Configuration Examples for Cisco IOS NetFlow

There are no configuration examples for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Where to Go Next

To configure basic NetFlow, refer to the "Configuring NetFlow and NetFlow Data Export" module. See the "Additional References" section for links to configuration information about additional NetFlow features and services.

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	"Cisco IOS NetFlow Overview"
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	"Getting Started with Configuring NetFlow and NetFlow Data Export"
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	"Configuring NetFlow Aggregation Caches"
Tasks for configuring NetFlow BGP next hop support	"Configuring NetFlow BGP Next Hop Support for Accounting and Analysis"

Related Topic	Document Title
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	"NetFlow Layer 2 and Security Monitoring Exports"
Tasks for configuring the SNMP NetFlow MIB	"Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data"
Tasks for configuring the NetFlow MIB and Top Talkers feature	"Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
• RFC 2460	Internet Protocol, Version 6 (IPv6) Specification

RFCs	Title
• RFC 3954	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided into areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

IPv6 --IP Version 6. Replacement for the current version of IP (Version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL --Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

multicast --When single packets are copied by the network and sent to a specific subset of network addresses, they are said to be multicast. These addresses are specified in the Destination Address field.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router

or switch that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow V9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

QoS --quality of service. A measure of performance for a transmission system that reflects the system's transmission quality and service availability.

traffic engineering --Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

VLAN --virtual LAN. Group of devices on one or more LANs that are configured (by management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.