Cisco IOS Flexible NetFlow Technology

Last Updated: December 2008

The Challenge: The ability to characterize IP traffic and understand the origin, the traffic destination, the time of day, the application utilization is critical for network availability, performance and troubleshooting. By analyzing NetFlow data, a network engineer can identify the cause of congestion; determine the class of service (CoS) for each user and application; and identify the source and destination network for your traffic. Monitoring IP traffic flows facilitates more accurate capacity planning and ensures that resources are used appropriately in support of organizational goals. This presents business opportunities that help justify and optimize the vast investment involved in building a network, ranging from traffic engineering (to optimize traffic flow through the network) and understanding network detailed behavior. Understanding behavior allows customers to implement new IP Services and applications with confidence. The challenge, however, is finding a scalable, manageable, and reliable solution to provide the necessary data to support these opportunities.

The Solution

Cisco IOS® Flexible NetFlow is the next-generation in flow technology allowing optimization of the network infrastructure, reducing operation costs, improving capacity planning and security incident detection with increased flexibility and scalability. Flexible NetFlow has many benefits above the Cisco traditional NetFlow functionality available for years in Cisco hardware and software.

Key Advantages to using Flexible NetFlow:

- Flexibility, scalability of flow data beyond traditional NetFlow
- The ability to monitor a wider range of packet information producing new information about network behavior not available today
- Enhanced network anomaly and security detection
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
- Convergence of multiple accounting technologies into one accounting mechanism

Flexible NetFlow is integral part of Cisco IOS Software that collects and measures data allowing all routers or switches in the network to become a source of telemetry and a monitoring device. Flexible NetFlow allows extremely granular and accurate traffic measurements and high-level aggregated traffic collection. Because it is part of Cisco IOS Software, Flexible NetFlow enables Cisco product-based networks to perform traffic flow analysis without purchasing external probes--making traffic analysis economical on large IP networks.

Opportunities and Uses of Flexible NetFlow include:

- Application and network usage

- Network productivity and utilization of network resources
- The impact of changes to the network
- Network anomaly and security vulnerabilities
- Long term compliance, business process and audit trail
- Understand who, what, when, where, and how network traffic is flowing

Applications for NetFlow data are constantly being invented but the key usages include:

- Real-time Network monitoring
- Application and user Profiling
- Network planning and capacity planning
- Security incident detection and classification
- Accounting and billing
- Network data warehousing, forensics and data mining
- Troubleshooting

Network Application and User monitoring

Flexible NetFlow data enables users to view detailed, time-based and application-based usage of a network. This information allows planning and allocation of network and application resources including extensive near real-time network monitoring capabilities and can be used to display traffic patterns application-based views. Flexible NetFlow services data optimizes network planning including device ingress and egress information and is useful for monitoring to and between datacenters. Flexible NetFlow provides proactive problem detection, efficient troubleshooting, and rapid problem resolution and the information is used to efficiently allocate network resources as well as to detect and resolve potential security and policy violations. Flexible NetFlow adds the benefit of customized flow analysis allowing the customization of network information in the diagnosis of the issue and focusing on the details of the problem at hand.

Network Planning

Flexible NetFlow can be used to capture data over a long period of time producing the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher- bandwidth interfaces. Flexible 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.. Flexible NetFlow allows the tracking of information within a NetFlow database or Flow Monitor. Multiple flow monitors may be implemented that include specific information useful for network planning. Flexible NetFlow will give you valuable information to reduce the cost of operating your network.

Security Analysis

Flexible NetFlow data identifies and classifies DDOS attacks, viruses and worms in real-time. Changes in network behavior indicate anomalies that are clearly demonstrated in NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents. Flexible NetFlow adds capability such as packet section export for deep packet inspection of security incidents. Security analysis may include detailed customized Flow Monitors to create

virtual or on demand views of network data enhancing detection capabilities already available in traditional NetFlow.

IP Accounting and Usage-Based Billing

Flexible NetFlow also enables customers to implement usage-based billing, providing them with the ability to implement competitive pricing schemes and premium services. Flexible NetFlow has the concept of permanent monitoring in which metering or accounting information is continuously and periodically completed (i.e similar to SNMP counters). Customers can, therefore, use NetFlow to track IP traffic flowing into or out of their datacenters for capacity planning or to implement usage-based billing.

Traffic Engineering

NetFlow can measure the amount of traffic crossing peering or transit points to determine if a peering arrangement with other service providers is fair and equitable. For instance Flexible NetFlow includes the use of information such as BGP policy accounting traffic index, detailed peering analysis with BGP NextHop and BGP AS information for peering analysis.

How Does NetFlow produce information for your network?

NetFlow includes two key components that perform the following capabilities:

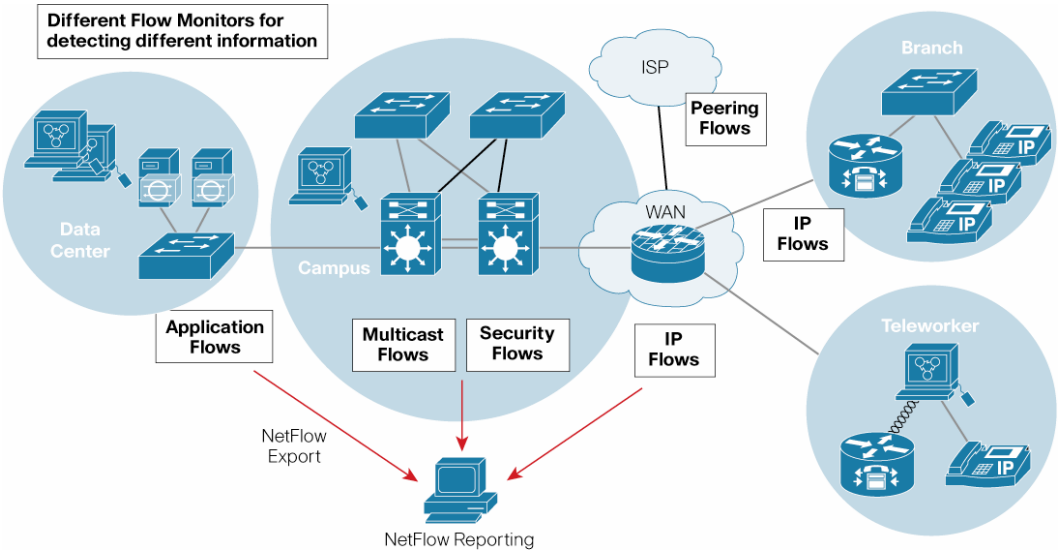
- **Flow caching** analyzes and collects IP data flows within a router or switch and prepares data for export. Flexible NetFlow has the ability to implement multiple flow caches or flow monitors for tracking different NetFlow applications simultaneously. For instance, the user can track security and traffic analysis simultaneously in separate NetFlow caches. This gives the ability to focus, pinpoint and monitor specific information for the application. Flexible flow data is now available using the latest NetFlow v.9 export data format.
- **NetFlow reporting collection** utilizes exported data from multiple routers and filters and aggregates the data according to customer policies, and then stores this summarized or aggregated data. NetFlow collection systems allow users to complete real-time visualization or trending analysis of recorded and aggregated flow data. Users can specify the router and aggregation scheme and time interval desired. Collection systems can be commercial or third party freeware products and optimized for specific NetFlow applications such as traffic or security analysis. For more information on NetFlow reporting solutions see the following links:

Commercial Solutions:
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/index.shtml

Freeware Solutions:
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/index.shtml

Cisco Solutions:
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/applications/index.shtml

Figure 1. Cisco IOS Flexible NetFlow Flow Monitors and collection of the export data



Flexible NetFlow can track a wide range of packet information for Layer2, IPv4, IPv6 Flows.

- Source and destination Mac Addresses
- Source and destination IPv4 or IPv6 addresses
- Source and destination TCP/User Datagram Protocol (UDP) ports
- Type of service (ToS)
- DSCP
- Packet and byte counts
- Flow timestamps
- Input and output interface numbers
- TCP flags and encapsulated protocol (TCP/UDP) and individual TCP Flags
- Sections of packet for deep packet inspection
- All fields in IPv4 Header including IP-ID, TTL and others
- All fields in IPv6 Header including Flow Label, Option Header and others
- Routing information (next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask, BGP Next Hop, BGP Policy Accounting traffic index)

For More Information

For more information about Cisco IOS Flexible NetFlow, please visit: http://www.cisco.com/go/fnf, or contact your Cisco account manager or global service manager.

To understand how Cisco IT uses NetFlow see the following link:
http://www.cisco.com/warp/public/732/Tech/nmp/docs/cisco_it_case_study_netflow.pdf

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.

Printed in USA C78-513098-00 12/08