



DATA SHEET

CISCO IOS NETFLOW

THE CHALLENGE

As IP traffic continues its explosive growth across today's networks, enterprise and service providers must be able to characterize this traffic and account for how and where it flows. 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® NetFlow technology is an integral part of Cisco IOS Software that collects and measures data as it enters specific routers or switch interfaces. 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 traffic. NetFlow allows extremely granular and accurate traffic measurements and high-level aggregated traffic collection. Because it is part of Cisco IOS Software, NetFlow enables Cisco product-based networks to perform IP traffic flow analysis without purchasing external probes--making traffic analysis economical on large IP networks.

OPPORTUNITIES

- **Network Application and User monitoring**

NetFlow data enables users to view detailed, time- 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. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection, efficient troubleshooting, and rapid problem resolution. This information is used to efficiently allocate network 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, which enables users to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher- bandwidth interfaces. NetFlow services data optimizes network planning, which includes peering, backbone upgrade planning, and routing policy planning. It minimizes 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 enables the analysis of new network applications. NetFlow will offer valuable information to reduce the cost of operating the network.

- **Security Analysis**

NetFlow data identifies and classifies Denial of Service (DoS) 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.

- **IP Accounting and Usage-Based Billing**

NetFlow technology also enables customers to implement usage-based billing, providing them with the ability to implement competitive pricing schemes and premium services.

In addition to measurement and billing, NetFlow also performs strategic analysis on their point-of-presence (POP) traffic for network planning, acceptable usage policy enforcement, or service-level management (SLM). Customers can, therefore, use NetFlow to track IP traffic flowing into or out of their server farms 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.

To understand how Cisco IT uses NetFlow see the following

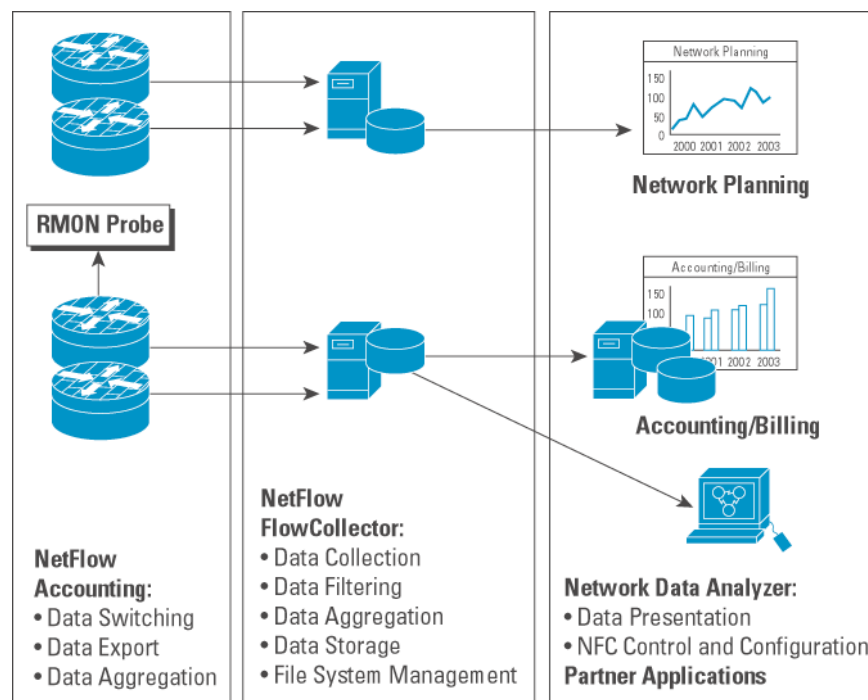
http://www.cisco.com/warp/public/732/Tech/nmp/docs/cisco_it_case_study_netflow.pdf

FROM COLLECTION TO ANALYSIS

NetFlow includes three key components that perform the following capabilities:

- *Flow caching* analyzes and collects IP data flows entering router or switch interfaces and prepares data for export. It enables the accumulation of data on flows with unique characteristics, such as IP addresses, application, and CoS. Flexible flow data is now available using the latest NetFlow v.9 export data format. NetFlow supports key technologies, including IPv4, IPv6, Multicast, and Multiprotocol Label Switching (MPLS).
- *FlowCollector and Data Analysis* captures exported data from multiple routers and filters and aggregates the data according to customer policies, and then stores this summarized or aggregated data. Users can leverage Cisco NetFlow collector as a flow collector, or they can opt for a variety of third-party partner products. A Graphical user interface displays and analyzes NetFlow data collected from FlowCollector files. This allows users to complete near-real-time visualization or trending analysis of recorded and aggregated flow data. Users can specify the router and aggregation scheme and desired time interval.

Figure 1



Cisco IOS NetFlow Infrastructure

Typical flow analysis information found in a NetFlow data record includes:

- Source and destination IP address

- Source and destination TCP/User Datagram Protocol (UDP) ports
- Type of service (ToS)
- Packet and byte counts
- Start and end timestamps
- Input and output interface numbers
- TCP flags and encapsulated protocol (TCP/UDP)
- Routing information (next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)

CISCO NETFLOW ECOSYSTEM

Cisco has developed a robust ecosystem of NetFlow partners who have developed value-add functionality and reporting specialties, including accounting, traffic analysis, security, billing, network planning, and network monitoring.

FOR MORE INFORMATION

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



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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 Web site 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. (0402R)
204044_ETMG_SH_09.04

