How Cisco IT Uses NetFlow to Capture Network Behavior, Security, and Capacity Data

Network management solution increases network security and simplifies network capacity planning.

BUSINESS BENEFITS
• Easier calculation of TCO and cost savings
• Accurate capacity planning
• Better utilization of network resources
• Enhanced virus and intrusion detection
• Lower networking costs
• Improved management

"Capacity planning will be a good deal easier as we continue to collect NetFlow historical data."

– Keith Brambaugh, network engineer, Cisco IT

The stakes for network availability and performance at Cisco are huge. For example, 93 percent of Cisco revenue—more than US$33,000 in sales per minute—is booked online using Cisco Internet connections and internal networks. More than 80 percent of Cisco products are manufactured by partners that rely on Cisco extranet connections to Cisco data centers. And more than 55,000 employees and partners worldwide rely on the global WAN that connects more than 250 sites worldwide, as well as remote access VPNs.

Not surprisingly, the ability to characterize IP traffic and account for how and where it flows is critical. Monitoring IP traffic flow facilitates more accurate capacity planning. It ensures that resources are used appropriately. It helps IT determine where to apply quality of service (QoS) so that vital traffic receives priority. And it plays a vital role in network security.

As recently as 2000, Cisco relied almost exclusively on Simple Network Protocol (SNMP) to monitor Internet bandwidth. But while SNMP facilitates capacity planning, it does little to characterize traffic, and essential capability for ensuring business continuity.

Gradually, Cisco has deployed Cisco IOS NetFlow technology, which is built into most Cisco switches and routers. NetFlow answers the who, what, when, where, and how of network traffic, and it has become the primary network accounting technology and anomaly-detection technology in the industry.

The results have been significant. NetFlow ensures that applications are deployed cost-effectively and that services remain available at all times for all employees, customers, and partners worldwide. Cisco IT also uses NetFlow data to protect the network from viruses and attacks, and to understand the impact of current and planned applications on the network.

All responsible organizations need a handle on network utilization to ensure resource alignment, capacity planning, and security. As converged networks and IP telephony become more prevalent, the ability to characterize traffic on the network will become even more critical.

Cisco has enabled Netflow on over 1900 WAN router interfaces.

Case Study: http://www.cisco.com/web/about/ciscoitatwork/case_studies/network_management_dl3.html

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.