Case Study

NetFlow gives network managers a detailed view of application flows on the network

Cisco® IT Case Study / Cisco Network Management / NetFlow: This case study describes Cisco IT's internal use of Cisco IOS® NetFlow technology within the Cisco global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"As converged networks and IP telephony become more prevalent, the ability to characterize traffic on the network—both for capacity planning and anomaly detection—will become even more critical." –Roland Dobbins, Cisco IT Network Engineer

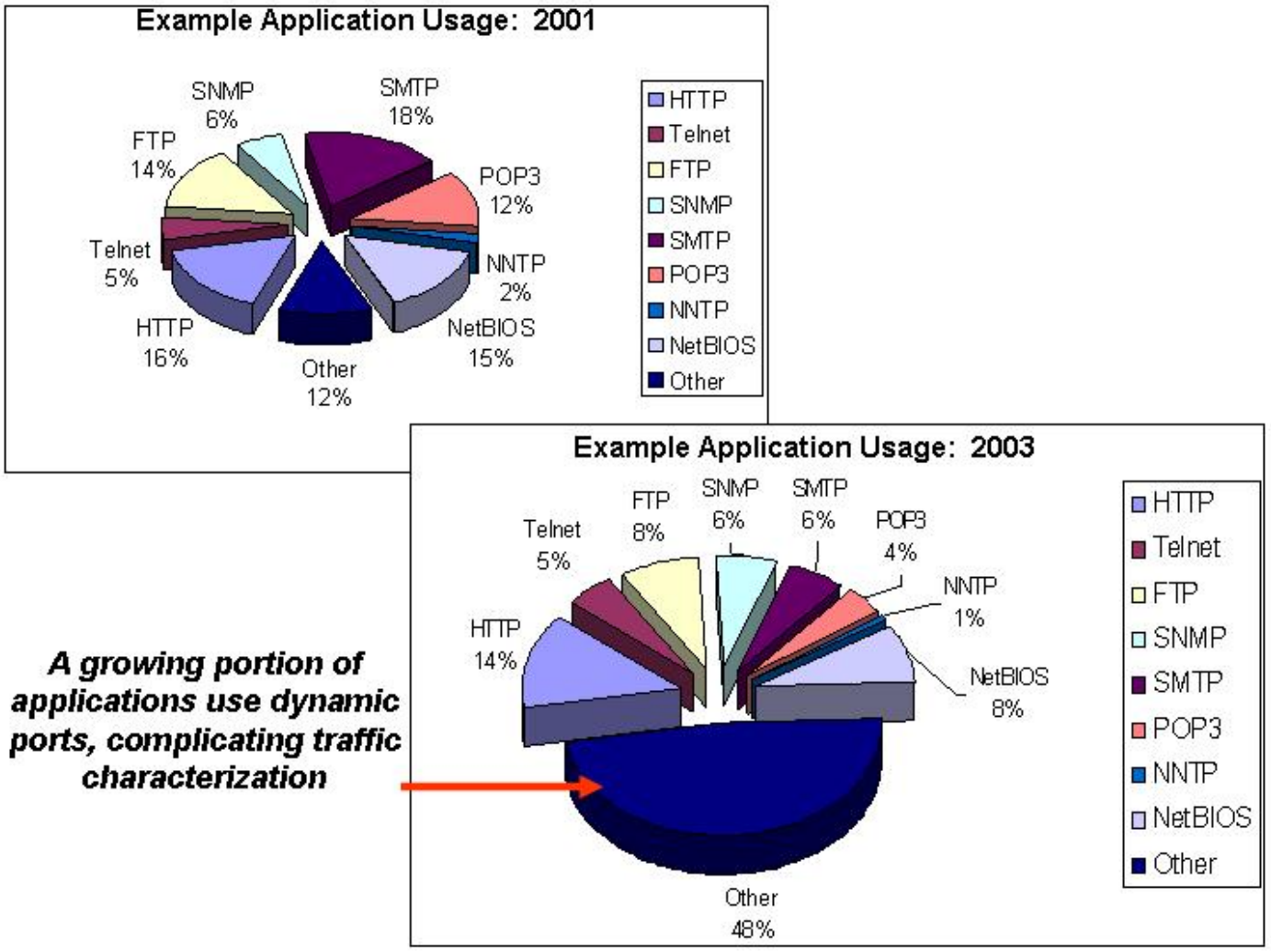
Challenge

At Cisco Systems®, the ability to characterize IP traffic and account for how and where it flows is critical for network availability and performance. Monitoring IP traffic flow facilitates more accurate capacity planning. It enables resource alignment—that is, ensuring that resources are used appropriately in support of organizational goals. 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 Cisco continuously monitors traffic to detect denial-of-service (DoS) attacks, network-propagated worms, and other undesirable network events.

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. Cisco customers open approximately 80 percent of Cisco Technical Assistance Center (TAC) cases online, and TAC engineers often resolve the problems by troubleshooting remotely across the network. 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. Vital Cisco voice traffic travels over Cisco AVVID (Architecture for Voice, Video and Integrated Data), as does corporate videoconferencing traffic and closed circuit IP video traffic from security cameras. And Cisco customers expect the network to be available 24 hours as they download Cisco IOS® Software and Cisco ® Catalyst ® Operating System (CatOS) Software upgrades and access documentation.

As recently as 2000, Cisco relied almost exclusively on Simple Network Management Protocol (SNMP) to monitor Internet bandwidth. But while SNMP facilitates capacity planning, it does little to characterize traffic, an essential capability for ensuring business continuity, determining if increases in utilization warrant adding capacity, determining if QoS parameters are adequate for target service levels, and more. "We needed a more granular understanding of how Cisco bandwidth is used," says Roland Dobbins, network engineer with the Cisco IT Internet Services group. Complicating the challenge of traffic characterization was the reality that many newer applications do not use the same ports each time, but rather dynamically select new ports for each use (see Figure 1).

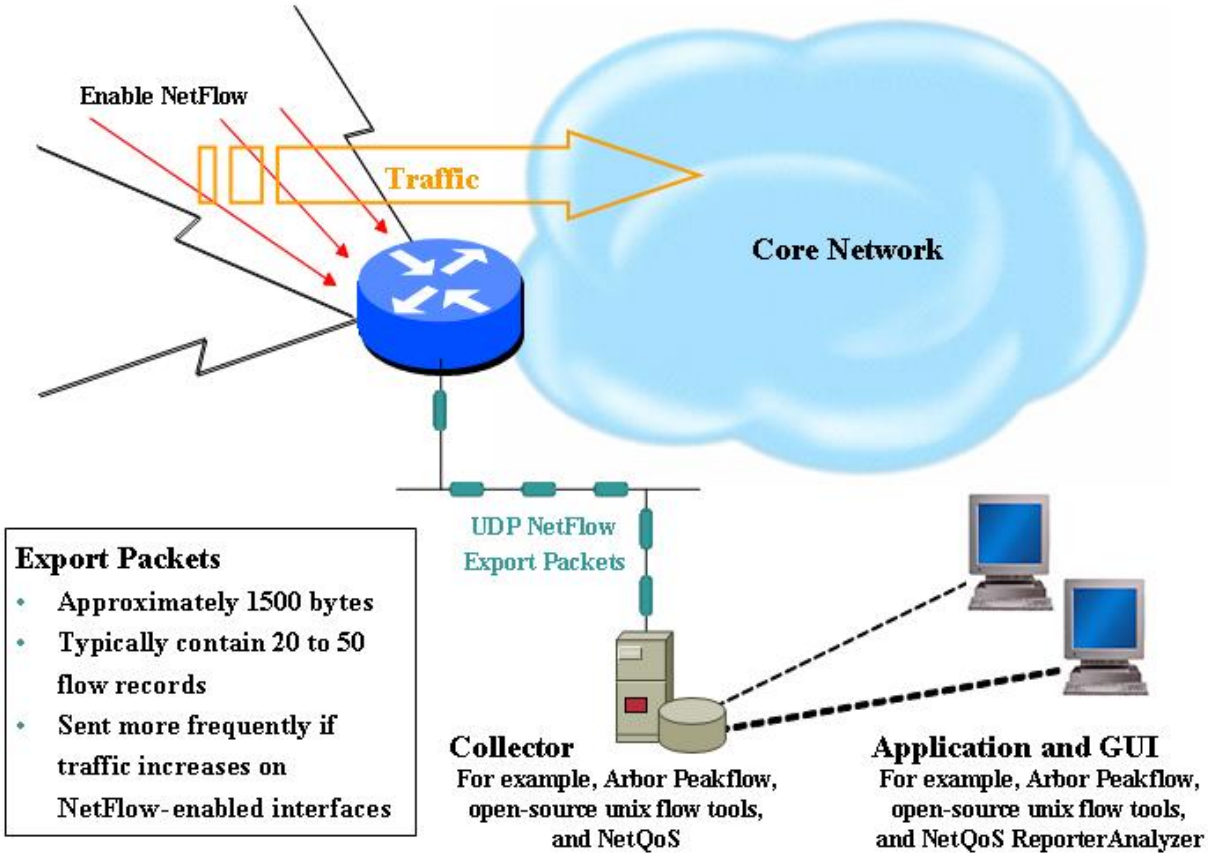
Figure 1 Shift in Types of Applications Used at Cisco Systems



Solution

Cisco gained the ability to characterize and analyze network traffic flows with Cisco NetFlow technology, which is built into most Cisco switches and routers using a specialized application-specific integrated circuit (ASIC) and some specialized features of Cisco IOS Software and Cisco Catalyst Operating System Software. Developed at Cisco in 1996, 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. In 2003, Cisco NetFlow Version 9 was chosen for a proposed IETF standard called IP Flow Information Export (IPFIX). IPFIX defines the format by which IP flow information can be transferred from an exporter, such as a Cisco router, to a collector application that analyzes the data (see Figure 2). To export data, routers represent each network traffic flow based on the source and destination IP address, source and destination port, Layer 3 protocol type, type of service, and input logical interface. “You can think of NetFlow as a form of telemetry pushed from routers and Layer 3 switches, each one acting as a sensor,” says John Cornell, a member of the Cisco IT technical staff.

Figure 2 Creating Export Packets



Whereas intrusion detection system (IDS) and packet sniffing software are micro-analytical tools that examine packet contents, Cisco NetFlow is a macroanalytical tool that characterizes large volumes of traffic in real time. In fact, one way that Cisco uses NetFlow is to identify instances in which IDS and packet capture could provide useful information. To explain the difference between Cisco NetFlow and packet capture, Dobbins uses a phone bill analogy. “NetFlow shows who talks to whom, for how long, at what intervals, using which protocols and ports, and how much data they exchange,” he explains. “Because it describes conversations without actually listening in on the conversation itself, NetFlow can scale for very large networks. Packet capture applications, in contrast, are more like wiretaps, useful for uncovering detailed information about specific conversations.”

Solution Components

Cisco IT has enabled Cisco NetFlow Version 5 on hundreds of its own network routers, switches, and monitors—from Cisco 3700 Series multiservice access routers through Cisco 6000 Series IP DSL switches and Cisco 12000 Series routers. NetFlow provides information on each individual IP flow traversing that switch or router (see Figure 3). When a router or Layer 3 switch receives an individual IP flow, NetFlow exports the stream in NetFlow Data Export format and sends it to a server running analysis software, such as Peakflow software from Arbor

Networks, NetQoS ReporterAnalyzer, or open source tools such as OSU flow-tools from splintered.net. Figure 4 shows a sample report based on Cisco NetFlow data.

Figure 3 NetFlow Version 5 Flow Information

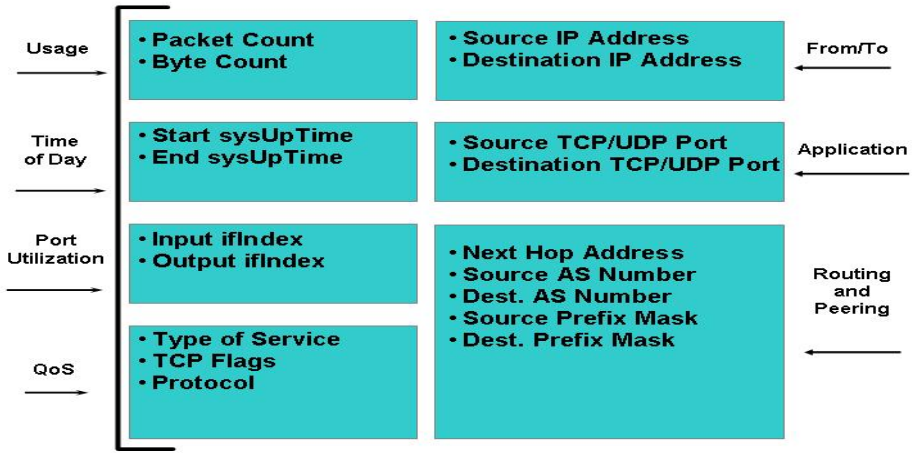
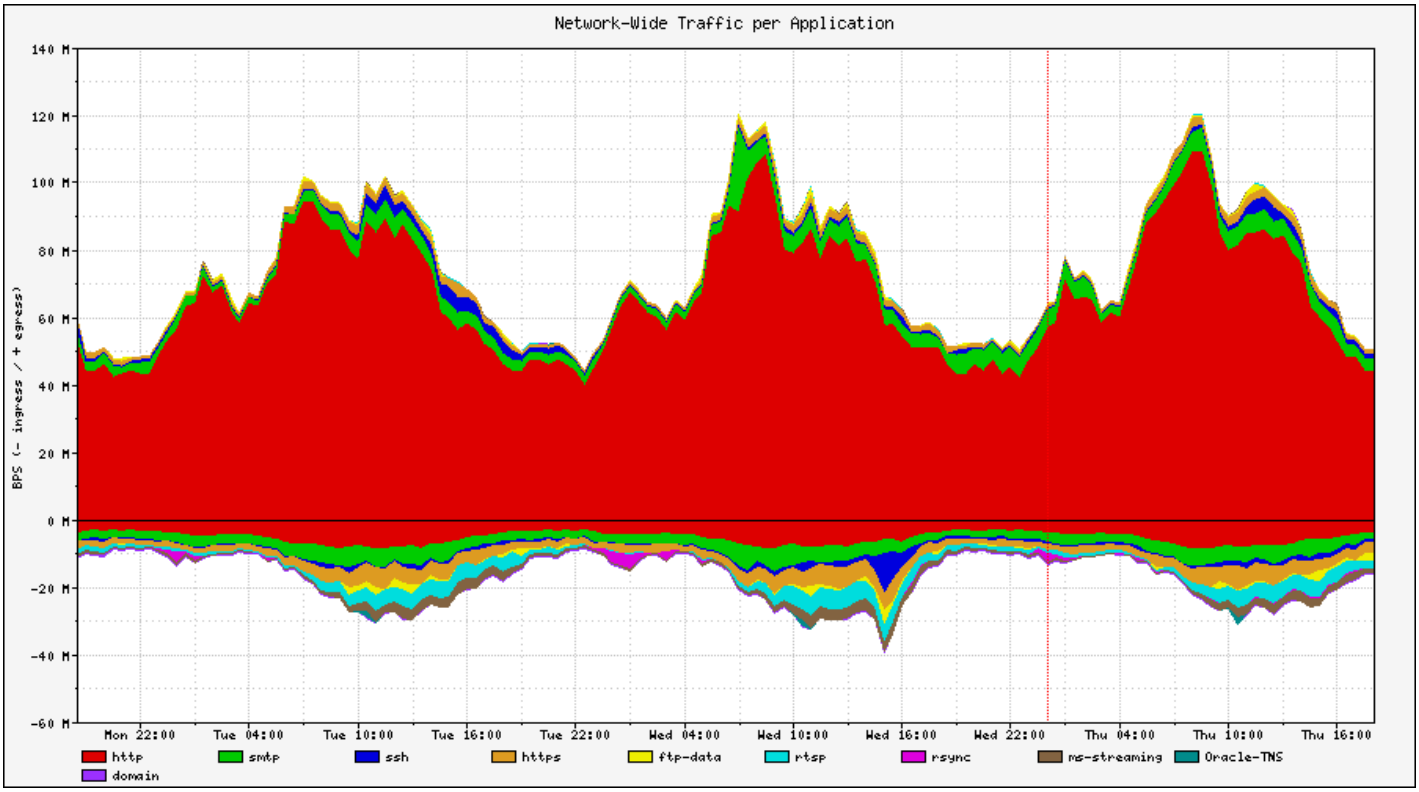


Figure 4 A graph of Cisco NetFlow Data by Arbor Networks Peakflow Traffic, to Characterize Traffic by Application



Cisco NetFlow is more cost effective in gathering network traffic information than Remote Monitoring (RMON) probes. Although the same information can be obtained from RMON probes, separate hardware must be installed at each site and on each link that needs to be investigated. This is a drawback, because many sites are difficult to get to; and if multiple links on a router need investigating, it requires a probe on every link. Because NetFlow is a feature of Cisco IOS Software, which is already running on every Cisco router, installation is easy and no hardware costs are involved. (Note: this is only partly true for Cisco network access modules (NAMs)—NAM blades that can be installed on Cisco Catalyst 6500s and Cisco Series 7600 routers, which allows engineers to look at all ports on a machine from one blade—but it does require hardware cost and installation. Also, Cisco Series 7200, 7500, and 7600 routers require a NetFlow software license fee.)

Deployment Description

Cisco enabled the NetFlow feature of Cisco IOS Software in several places on the Cisco network that process incoming and outgoing traffic, for a total of more than 1900 WAN interfaces. “Monitoring this many interfaces with RMON probes would have been cost-prohibitive, as a separate probe is required for each link,” notes Michael Chang, Cisco IT project manager. The information from each location is useful on its own, as well as in combination with other network-related business intelligence. For example, the combination of Cisco NetFlow and Border Gateway Protocol (BGP) routing information provides visibility into the origin and destination of Cisco network traffic, which helps to ensure optimal peering with Internet service providers (ISPs). More examples appear in the Results section.

Table 1 shows where the Cisco NetFlow traffic is collected and the types of analysis for which it is used.

Table 1 Analysis Software Used by Cisco IT: Network Location and Purpose of Data Collection

Network Location	Analysis Software	Purpose
Internet gateway routers that connect to ISP links	Arbor Networks Peakflow Traffic Arbor Networks Peakflow DoS	Network traffic analysis by application Correlation of network traffic with BGP routing information Anomaly detection
Routers at inner edge of public-facing network	Arbor Networks Peakflow DoS	Anomaly detection
WAN core (aggregation layer)	NetQoS ReporterAnalyzer	Network traffic analysis by application, for capacity planning
WAN edge	NetQoS ReporterAnalyzer	Network traffic analysis by application, for capacity planning
Core routers on public-facing network	OSU flow-tools from splintered.net	Collection of historical data, useful for forensics and diagnostics
Network Address Translation (NAT) gateway	OSU flow-tools from splintered.net	Collection of historical data, useful for forensics and diagnostics Auditing of addresses that have undergone NAT (“NATed” addresses)

Internet and Security Application Examples

Total Avoidance of SQL Slammer Worm

On January 24, 2003, the SQL Slammer worm, also called Sapphire, propagated worldwide in just eight minutes. It felled networks worldwide, including entire networks of automated teller machines and leading enterprises. “Many organizations thought they blocked Slammer at their Internet borders on Friday night, only to return Monday to discover their networks were compromised from laptops, VPN connections, other indirect vectors,” says Dobbins.

Cisco, however, experienced no loss of business continuity from SQL Slammer, a victory the IT team attributes to teamwork, an established communications plan, a robust network architecture, and the effective use of Cisco NetFlow technology. “Cisco NetFlow gave us visibility into the event so that we could understand the severity of the threat and react appropriately,” says Dobbins. NetFlow played a vital role in a six-phase approach that Cisco borrowed from the ISP world. “Increasingly, enterprises are the ISPs for their employees,” says Dobbins. “They deliver content and services across Internet connections as well as internally. Therefore, many of the concepts and technologies developed for service providers apply to the enterprise, as well.” Cisco NetFlow was a critical part of the Cisco six phase approach to security, highlighted here in the response to SQL Slammer:

- *Phase 1: Preparation*—An extremely important factor in detecting Slammer and reacting appropriately was implementing Cisco NetFlow and the analytical software prior to the event. Because Cisco had a baseline to understand normal network traffic behavior, the company was in a position to recognize potentially hostile deviations from that behavior.
- *Phase 2: Identification*—Arbor Peakflow DoS alerted Cisco IT to the presence of a large volume of anomalous traffic on UDP port 1434. Cisco immediately confirmed that the traffic was unexpected and suspicious by using Arbor Peakflow Traffic to look through the Cisco NetFlow data for historical precedents based on traffic, bits per second, duration, sources, and destinations.
- *Phase 3: Classification*—Cisco classified and scoped the threat using the input from Cisco NetFlow and Arbor Peakflow. Not all anomalous traffic poses the same threat to availability, and the Arbor Peakflow solution allowed Cisco IT to rapidly classify Slammer as a high-level threat.
- *Phase 4: Trace-back*—Cisco identified all potential Slammer sources or vectors. “Traceback was essential to our ability to avoid damage from Slammer,” says Dobbins. “Many other organizations failed to account for indirect vectors, such as VPNs and laptops, and paid the price on Monday.”
- *Phase 5: Reaction*—Having identified potential vectors, Cisco closed network access to this traffic by placing both inbound and outbound access control lists (ACLs) at all Internet points of presence worldwide. “Because of the severity of the threat, we pushed ACLs to the desktop distribution level in every Cisco facility worldwide and also in strategic places in our WAN backbone,” says Dobbins. “Network professionals would regard these as draconian actions; yet we knew they were warranted because of the information we received from Cisco NetFlow and Arbor Peakflow.”
- *Phase 6: Post-mortem*—Cisco IT followed up daily for two weeks after the incident to be sure that the threat was eradicated.

The defense against Slammer was an unqualified success. “The Monday following the attack, Cisco customers had full use of the Cisco resources they needed to handle the effects of SQL Slammer,” says Cornell.

Detection and Prevention of DoS attacks and Other Undesirable Traffic

Like other organizations with high-profile online presences, Cisco from time to time receives traffic intended to produce a DoS attack. DoS attacks flood the network with packets, often of an unusual size, from an untrusted source to a single destination. Cisco detects and prevents DoS attacks by using Cisco NetFlow to collect the packet source, destination, protocol number, port number, and packet size, and then sends the information to Arbor Peakflow DoS for anomaly detection. Figure 5 shows a sample anomaly detection report. Cisco NetFlow steers the

company's use of microanalytical technology, including ACLs, QoS, Unicast Reverse Path Forwarding blackholing triggered by BGP, and Cisco NAM-2 for the Cisco Catalyst 6500 Series Switch.

Figure 5 Sample Peakflow DoS Report for Anomaly Detection

Audit of NAT'ed Traffic

An inherent limitation of NAT is the many-to-one relationship between non-Internet-routable addresses—used by mobile workers, for example—and publicly routable Internet addresses. Cisco NetFlow gives Cisco the ability to audit NAT traffic to help troubleshoot and resolve network and security issues, as well as periodically ensure that mobile workers adhere to corporate network access policy.

Intranet and Extranet Application Examples

Capacity Planning for Transition from Managed DSL service to Internet VPN

In 2001, when the cost of direct DSL and ISDN access increased markedly, Cisco transitioned tens of thousands of teleworkers and remote office workers worldwide to remote access VPNs. To determine if additional capacity was needed, Cisco used Cisco NetFlow in conjunction with various open-source tools to characterize existing traffic and then extrapolate expected traffic. With this business intelligence, Cisco successfully transitioned 22,000 users to VPN in only three months.

Detection of Unauthorized WAN Traffic

Usually when a WAN link experiences consistently high utilization levels, a company makes an investment to upgrade the link. Cisco has avoided costly upgrades in some cases by identifying the applications causing the congestion and, if appropriate, changing the usage policy. For

example, when one office experienced a rapid rise in utilization, Cisco IT used Cisco NetFlow and NetQoS ReporterAnalyzer to identify the application and hosts associated with the traffic and determined that the culprit was an unauthorized HTTP application. The problem disappeared on its own when Cisco reminded employees of corporate policies forbidding the transport of unauthorized files on the corporate network. In a similar application, Cisco IT uses Cisco NetFlow to confirm that extranets the company provides to its business partners are used for authorized applications only. Deployed on the Cisco intranet, Cisco NetFlow is also used by the company to detect possible corporate information theft—for instance, when unusually high volumes of information are downloaded from individual servers over short periods of time.

Reduction in Peak WAN Traffic

When WAN traffic over several links increased significantly from one month to the next, Cisco NetFlow and NetQoS ReporterAnalyzer quickly revealed the cause: 55 percent of the traffic in Europe, Middle East, and Africa, and a significant portion everywhere, originated from a new PC backup tool that had been deployed in sales offices. The initial backup sent large volumes of traffic over the WAN, and Cisco IT requested that employees perform their initial backups at night. In addition, IT built time-based QoS statements in the WAN routers that limited WAN link capacity to 10 percent by day but guaranteed 50 percent of link capacity at night. The statements allowed the routers to discard packets above those thresholds when link capacity was needed for other applications. The result: Cisco postponed costly WAN link upgrades, managed traffic while employees completed their initial large PC backups, and instigated a search for more efficient PC backup software. After migrating to the new backup solution, Cisco IT will use NetFlow statistics to measure WAN traffic improvement.

Validation of QoS Parameters

Cisco IT allocates a certain portion of WAN capacity to data, voice, and video. The allocation is based on theoretical models of the amount of traffic each site generates, as well as target QoS levels. In the past, the challenge was to verify that QoS goals had been achieved. “Cisco IT overcame these challenges by using Cisco NetFlow and NetQoS ReporterAnalyzer to confirm that appropriate bandwidth has been allocated to each class of service (CoS) and that no CoS is over- or under-subscribed,” says Chang. Cisco IT also uses Cisco NetFlow with NetQoS ReporterAnalyzer to confirm that WAN links are engineered to avoid dropping other data traffic, even when voice and video usage reach their peak levels. For example, the OC-3 link connecting Chicago to New York had allocated 10 percent of the bandwidth, or 15.5 Mbps, to voice over IP (VoIP) traffic. By turning on Cisco NetFlow in the routers, Cisco IT determined that VoIP traffic accounted for less traffic even during peak times of day, and the amount allocated was more than adequate to ensure QoS.

Analysis of VPN Traffic and Teleworker Behavior

Using Cisco NetFlow, Cisco IT easily can identify teleworker traffic because it all travels over generic routing encapsulation tunnels. This kind of traffic analysis facilitates capacity planning for Internet access. And by differentiating different types of teleworker traffic—voice, e-mail, Web browsing, other applications—Cisco can better understand employee behavior with the goal of providing optimum support, such as creating time of day QoS statements to support more business voice traffic during the day and more data backup at night.

To determine the relative amount of Cisco IP phones and Cisco IP SoftPhone software traffic among teleworkers—information that is useful for marketing as well as IT planning—Cisco IT uses Cisco NetFlow and NetQoS ReporterAnalyzer to monitor the type of service (ToS) and packet size bits. All voice traffic has a ToS bit value of five, and the IP flow is 80 kilobits per second (kbps) for the Cisco IP phone (based on the G.711 compression codec) compared to 24 kbps for SoftPhone streams (based on the G.729 compression codec).

Confirming Carrier Class of Service

In the United States, the Cisco WAN uses leased line circuits. It is relatively easy to determine how Cisco IT has supported different classes of service on their WAN, because IT engineers simply can look at the router configuration to verify the QoS statements. But when WAN circuits are supplied by the carrier on a shared Multiprotocol Label Switching (MPLS) network, as they are in the European Cisco WAN, this option is not available: Cisco IT cannot examine QoS configurations within a service provider’s network. Cisco IT wanted the ability to confirm the

carrier's delivery of different classes of service for two reasons. First, Cisco IT pays the MPLS VPN provider a higher rate to deliver certain types of traffic with a higher CoS, and therefore it needs assurance that the service level agreement is met. Second, if Cisco IT should ever underestimate the amount of voice or video traffic requiring premium CoS, it needs to know as soon as possible so that it can place an upgrade order. Cisco IT plans to use Cisco NetFlow to look for jitter and packet loss on the MPLS-based VPN in Europe. "Collecting QoS information not only will confirm that we're receiving the CoS in the contract, but also that we've allocated the right amount of bandwidth to each CoS to support the business applications," says Chang.

Calculating Total Cost of Ownership for Applications

Before releasing new applications to large numbers of users, Cisco Systems determines total cost of ownership (TCO). One significant factor in TCO can be the WAN impact (see "Reduction in Peak WAN Traffic"). To eliminate surprises regarding WAN impact, the Cisco application development groups attempt to first deploy new applications in a test environment, using Cisco NetFlow to measure how much WAN traffic the application is likely to generate when released to a larger population. This helps to calculate TCO more accurately. The testing requires no dedicated lab or test equipment, because the application designer can configure the application to run through a Cisco router in the lab with NetFlow enabled. Some of the ways that Cisco IT uses NetFlow to calculate application TCO include:

- *Upgrading the surveillance camera system to an IP-based closed circuit TV (CCTV) system.* The Cisco Safety and Security department (responsible for remotely monitoring over two thousand security cameras in over 270 Cisco locations) was planning to stream occasional on-demand video across the WAN, and was also planning to migrate their campus MAN video traffic from dedicated fiber onto the shared Gigabit Ethernet LAN. By collecting and analyzing Cisco NetFlow data in the lab, Safety and Security demonstrated that the resulting IP traffic would not cause significant spikes in metropolitan-area network and WAN traffic.
- *Deploying Cisco Unity™ voice mail across the WAN.* The Cisco NetFlow data provided assurance that traffic demands for the planned deployment of *Cisco Unity™ voice mail* would not exceed the WAN bandwidth allocated for voice traffic.
- *Calculating cost savings from 50,000 Cisco IP phones worldwide.* Cisco IT management wanted to quantify the cost savings of migrating from a traditional voice network to the IP WAN. Using Cisco NetFlow, Cisco IT presently is measuring the amount of voice traffic on the WAN between locations and using this data to estimate the cost of carrying identical traffic over the public switched telephone network.
- *Calculating cost savings from the Cisco Application and Content Networking System (ACNS) Software*. Cisco ACNS servers store cached and preselected content closer to the end user on the Cisco IT WAN, reducing WAN traffic and increasing access speeds. Cisco IT uses Cisco NetFlow to determine how much traffic is offloaded from the WAN so that they can estimate cost savings.
- *Planning for future services*: As Cisco IT continues to deploy future services (for example, Oracle 11.i and Cisco Unity are two large applications with potential WAN impact), they will continue to use NetFlow to capture lab and pilot network data to determine the total WAN impact, and WAN cost, associated with these new services.

Results

For Cisco, the benefits of Cisco NetFlow are to ensure that applications are deployed cost-effectively and that services remain available at all times for all employees, customers, and partners worldwide. Cisco IT uses NetFlow data to protect the network from viruses and attacks, and to understand the impact of current and planned applications on the network. "By providing visibility into network traffic, Cisco NetFlow helps us defend against DoS attacks and other forms of undesirable traffic, react appropriately to network-based threats, and gather valuable intelligence about application usage for capacity planning purposes," says Cornell.

Next Steps

The next steps for Cisco IT are to benefit from the increasing value of the network data being collected and to expand the use of NetFlow to other parts of the network.

"Capacity planning will be a good deal easier as we continue to collect more NetFlow historical data. After we have a sufficient amount of historical data to compare, we'll be able to see historical trending a lot more easily. Also, we'll have a much clearer picture of what normal

traffic on the corporate network can look like so that we can catch anomalous traffic a lot faster," says Keith Brumbaugh, a capacity planning network engineer in Cisco IT.

Cisco IT started its use of Cisco NetFlow information gathering gradually in small areas, starting with Internet gateways and then adding collection points at WAN and Extranet gateways. "We've mostly been collecting information on traffic going from the Internet to the intranet, and from the intranet to the Internet," says John Cornell. "We're going to be expanding our use of NetFlow within the intranet as well." Adds Roland Dobbins, "We're planning to extend our capacity planning reach into the campus LANs, especially the data center LANs, and the connection points between these data center LANs and the Internet."

Cisco continues to extend its use of Cisco NetFlow from public-facing networks to internal networks. "As network perimeters 'crumble,' a result of wireless and VPN tunnels, for example, internal network security is becoming the most pressing IT security dilemma," says Dobbins. "By characterizing traffic flow on the intranet and to the edges of the desktop network, we'll be able to detect hosts that are generating undesirable traffic or attempting to access resources inappropriately." Cisco also anticipates extending capacity planning methodologies used for Internet connectivity to internal networks on the Cisco WAN.

"Any responsible organization, whether a business or governmental agency needs a handle on network utilization to ensure resource alignment, capacity planning, and security," says Dobbins. "As converged networks and IP telephony become more prevalent, the ability to characterize traffic on the network—both for capacity planning and anomaly detection—will become even more critical. For Cisco, NetFlow provides that capability."

For additional Cisco IT Case Studies on a variety of business solutions,
go to Cisco IT @ Work

www.cisco.com/go/ciscoitatwork

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.

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • 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 • TurkeyUkraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA