



Get Application Aware with Your Cisco Network Devices

By: Ben Erwin, NetQoS, Inc.

An important part of shifting a network management strategy from up/down availability measurements to one based on performance is moving beyond a limited, “device-aware” approach to a focus on application delivery—an “application-aware” approach. This entails understanding the content flowing over the links and prioritizing traffic based on the value and importance of that content.

Some of the most advanced application-aware technologies already exist within Cisco routers and switches and don’t require the purchase of additional modules, cards, probes, or proprietary analytical engines. When deployed along with a Simple Network Management Protocol (SNMP) polling product, application-aware technologies such as Cisco IP Service Level Agreement (IP SLA), Cisco Class-Based Quality of Service (CBQoS), and Cisco Network-Based Application Recognition (NBAR) put the data you need right at your fingertips.

This white paper introduces a set of application-aware capabilities, explains how they can be leveraged within Cisco routers and switches, and outlines their critical role in an overall application delivery management strategy.

Application-Aware Network Management

Trends such as data center and server consolidation, increasing numbers of remote workers, the rise of voice and video traffic, and multi-tiered applications have led to an increase in the volume and complexity of network traffic. At the same time, device availability has stabilized, with hardware or software infrastructure failures occurring infrequently.

Recognizing the critical nature of the network and the data it carries for the productivity and health of the enterprise, many of the world's largest organizations have begun taking a *Performance First™* approach to network management. By focusing on application delivery across the network and identifying areas where improvement is needed, network managers at these organizations are now able to make more informed infrastructure investments and rapidly resolve problems before they affect the bottom line.

An important part of shifting a network management strategy from up/down availability measurements to one based on performance is moving from the limited perspective of “device-aware” network management to a focus on application delivery—an “application-aware” perspective that’s both more comprehensive and more cost-effective. Being application-aware means understanding the content flowing over the network. Once armed with that understanding, you can prioritize traffic flows and configure devices based on the value and priority of that all-important content.

Such a shift in strategy doesn’t necessarily require new tools. Some of the most advanced application-aware technologies already exist within your Cisco routers and switches. In many cases, no additional modules, cards, probes, or proprietary analytical engines are required. For example, application-aware technologies such as Cisco **IP Service Level Agreement (IP SLA)**, Cisco **Class Based Quality of Service (CBQoS)**, and Cisco **Network Based Application Recognition (NBAR)** are right at everyone’s fingertips.

Using a Simple Network Management Protocol (SNMP) polling product to access the necessary Cisco data is the key to leveraging these technologies. A common misperception of SNMP polling products is that they are limited to providing simple up/down status of network devices, device utilization, and some shallow insight into the status of device components such as CPU and memory utilization. However, some SNMP products are being leveraged in more advanced use cases, including capacity planning, trending, and even protocol analysis with Remote Network Monitoring (RMON) technology.

While all of these device-monitoring capabilities are necessary for managing application delivery, only a few SNMP products also allow you to benefit from the application-aware monitoring capabilities within existing devices—capabilities that are arguably more important tools for managing application delivery.

The purpose of this white paper is to introduce a set of application-aware network management capabilities that rely on a combination of superior tools and time-tested technologies. The Cisco technologies that underlie the application-aware approach outlined here have existed for a number of years, but are often underutilized. We’ll

explain how they can be leveraged within the Cisco routers and switches you already have and delineate their critical role in an overall application delivery management strategy.

Managing Application Response Times with Cisco IP SLA

Application response times are at the heart of application delivery management. The speed of the application's responses to the end user's requests will ultimately determine whether the user's experience using that application is excellent, adequate, or unacceptable. While measuring real application transactions is the most accurate method for measuring response times, sometimes that approach is not an option. For example, during the pre-deployment assessment phase of rolling out a new application, or when measuring a service provider SLA edge-to-edge, real transactions that would be applicable to the usage scenarios you need to test are not being performed. It's in such situations where synthetic transactions, generated and measured by the **Cisco IP SLA** functionality, can offer some assistance.

IP SLA is built into almost every model of Cisco router and switch, from the access-layer devices to the core, including the Catalyst 6500 and 7600 Series. Because it is included in the Cisco equipment, IP SLA does not require additional licenses or hardware to operate. The IP SLA capabilities can simply be activated through the device's command line interface (CLI) or through an SNMP polling product with the appropriate credentials. Once IP SLA is enabled, the configuration and reporting can begin immediately.

IP SLA operates by sending synthetic transactions between two network devices or between a network device and a server. One device acts as the "sender" of the test data, and the other acts as the "responder." The sender can be configured to send different types of synthetic transactions based on port, packet size, type of service, and even more advanced characteristics, as is the case with Voice over Internet Protocol (VoIP) tests. Table 1 below lists some of the different IP SLA test types.

Test Name	Measurement Capability	Example Use
UDP Jitter	Round-trip delay, one-way delay, one-way jitter, one-way packet loss. One-way delay requires time synchronization between the Cisco IOS IP SLAs source and target routers	Validating and monitoring delay for latency-sensitive UDP applications
UDP Echo	Round-trip delay	Validating and monitoring delay for specific UDP applications

Test Name	Measurement Capability	Example Use
UDP Jitter for VoIP	Round-trip delay, one-way delay, one-way jitter, one-way packet loss, VoIP codec simulation: G.711 ulaw, G.711 alaw, and G.729aMOS, and ICPIF voice quality scoring capability. One-way delay requires time synchronization between the Cisco IOS IP SLA source and target routers.	Validating and monitoring VoIP environments, especially prior to rolling out VoIP or investing in VoIP infrastructure
TCP Connect	Connection time	Validating and monitoring delay for connection establishment on TCP applications
Domain Name System (DNS)	DNS lookup time	Validating and monitoring DNS resolution times across the network
Dynamic Host Configuration Protocol (DHCP)	Round-trip time to get an IP address	Validating and monitoring DHCP lookup times across the network
FTP	Round-trip time to transfer a file	Validating and monitoring file transfer times using the FTP protocol across the network
HTTP	Round-trip time to get a Web page	Validating and monitoring Web transactions across the network
Internet Control Message Protocol (ICMP) Echo	Round-trip delay	Validating and monitoring delay for ping response times over the ICMP protocol
ICMP Path Echo	Round-trip delay for the full path	Validating and monitoring service provider latency SLAs at all levels of service
ICMP Path Jitter	Round-trip delay, jitter, and packet loss for the full path	Validating and monitoring service provider latency and delivery SLAs at all levels of service

Table I - Cisco IP SLA test types

Once the sender is configured with the desired IP SLA test parameters, packets are sent to the selected responder. Emulating a typical client-server interaction, the responder sends a response packet back to the sender. The sender then calculates the response-time metrics appropriate for the test type, and the process repeats multiple times, based on the test configuration.

Extracting the IP SLA response-time metrics directly from routers and switches can be difficult, but tools are available with monitoring capabilities that can greatly ease this situation. Instead of relying on the device CLI for copying metrics from a Telnet session to a spreadsheet for graphing purposes, you can deploy an SNMP polling product to collect data automatically, directly from the device. Given the proper credentials, this class of product can extract the response-time metrics recorded during IP SLA testing, store them in a database, and display the results in a graphical user interface. Some SNMP polling products can also provide analytical function beyond data collection, such as calculating baselines, displaying trends, and triggering threshold alerts based on collected IP SLA data.

NetQoS NetVoyant®, the device performance management module of the NetQoS® Performance Center, offers a user interface into IP SLA testing that includes analytical reports to help dissect the data that's collected. In addition, NetVoyant provides a wizard-style interface for configuring and deploying IP SLA tests directly to the sender(s), allowing even the most inexperienced users to leverage IP SLA without special training on network device CLIs. NetVoyant can eliminate the need to use the router or switch CLI with IP SLA altogether, not only saving time, but also simplifying the interpretation of test results.

Top IP SLA RTT Deviation From Norm 25 May 2007 CDT

VoIP Jitter

Name	Type	Src	Dst	Normal	Actual	Deviation (%)
New York to Raleigh Jitter	Jitter	New York	Raleigh:80	198.8 ms	685.0 ms	244.6
Los Angeles, California - 192.168.2.0/24 to Chicago, Illinois - 192.168.5.0/24 Jitter	Jitter	Los Angeles, California - 192.168.2.0/24	Vancouver:80	136.4 ms	75.3 ms	-44.8
Los Angeles, California - 192.168.2.0/24 to Raleigh Jitter	Jitter	Los Angeles, California - 192.168.2.0/24	Los Angeles:80	173.8 ms	206.6 ms	18.9
Chicago, Illinois - 192.168.5.0/24 to Los Angeles, California - 192.168.2.0/24 Jitter	Jitter	Chicago, Illinois - 192.168.5.0/24	Los Angeles:80	244.7 ms	269.9 ms	10.3
San Antonio, Texas - 192.168.3.0/24 to Los Angeles, California - 192.168.2.0/24 Jitter	Jitter	San Antonio, Texas - 192.168.3.0/24	Montreal:80	195.7 ms	187.0 ms	-4.5
Chicago, Illinois - 192.168.5.0/24 to San Antonio, Texas - 192.168.3.0/24 Jitter	Jitter	Chicago, Illinois - 192.168.5.0/24	Osaka:80	208.8 ms	217.1 ms	3.9

Show Top: 10

Figure 1 - NetVoyant displays VoIP Jitter tests deviating from baseline

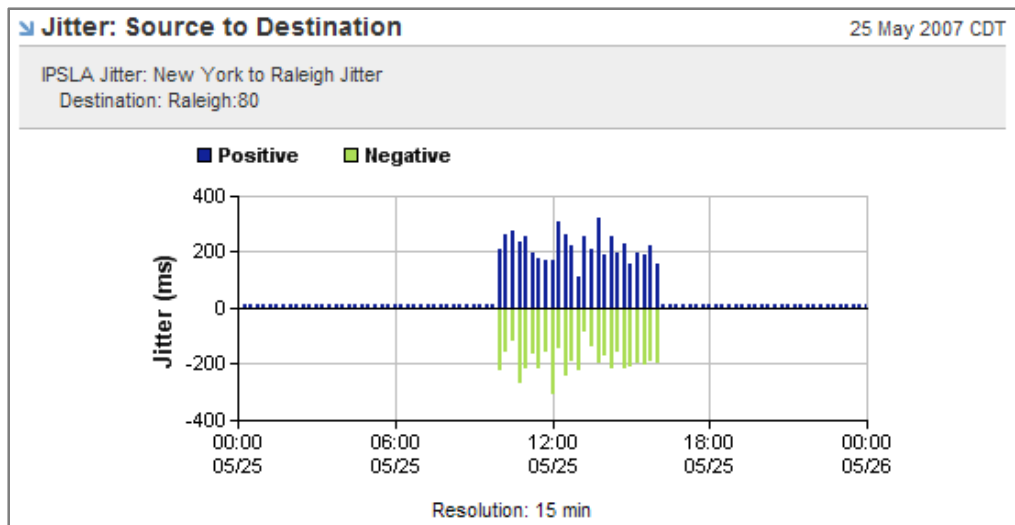


Figure 2 - NetVoyant displays jitter measurements from Cisco IP SLA running between the New York and Raleigh network sites

IP SLA Over-Threshold Scorecard									25 May 2007 CDT
Group ▲	Target	Oct	Nov	Dec	Jan	Feb	Mar	Apr	Average
All Routers	>= 10.00	✓ 19.253	✓ 18.446	✓ 18.587	✓ 18.224	✓ 18.794	✓ 18.864	✓ 18.357	✓ 18.646
Data Sources	>= 10.00	✓ 19.253	✓ 18.446	✓ 18.587	✓ 18.224	✓ 18.794	✓ 18.864	✓ 18.357	✓ 18.646
Tiger Industries	>= 10.00	✓ 19.062	✓ 17.096	✓ 18.502	✓ 17.810	✓ 17.831	✓ 18.336	✓ 17.414	✓ 18.007
VoIP Infrastructure	>= 10.00	✓ 19.253	✓ 18.446	✓ 18.587	✓ 18.224	✓ 18.794	✓ 18.864	✓ 18.357	✓ 18.646
WAAS Candidates	>= 10.00	✓ 20.886	✓ 19.949	✓ 20.051	✓ 19.612	✓ 20.319	✓ 20.480	✓ 19.616	✓ 20.130

1 of 1 Max Per Page: 10

Figure 3 - NetVoyant scorecards provide a management-level view into how IP SLA test responses are meeting target thresholds month over month

Cisco IP SLA should be part of every network manager's toolbox for managing application delivery. As a free component of Cisco routers and switches, it provides numerous benefits once you've enabled it and have begun running it as part of any new application pre-deployment program.

An SNMP polling product with application-aware monitoring capabilities is similarly essential to an application-aware approach to the network. While IP SLA is an extremely powerful data source, collecting metrics from a CLI can be time-consuming, and raw data has only limited usefulness for most IT staff.

Deploying Quality of Service with Cisco CBQoS

If application response times are the heart of managing of application delivery, Quality of Service (QoS) rules act like cholesterol medication to unclog arteries, keep blood flowing, and help the heart stay healthy. A QoS strategy is a mandatory component of an application delivery management program. Within any enterprise, the end-user experience with certain applications will always be more critical than it is with others. QoS is a blanket term for network policies and practices that help to manage different types of data traffic that share network links.

Effectively, QoS determines how different types of traffic, with different priorities, are handled whenever tradeoffs that are likely to impede performance must be made.

Many network managers deploy QoS in the hope that it's a magic bullet. They expect QoS to solve their performance issues by prioritizing the routing and switching of certain application traffic without any visibility into the QoS operation and its impact on the network. However, this "keep your fingers crossed" method for implementing QoS has a better alternative: Cisco Class-Based Quality of Service (CBQoS).

The CBQoS mechanism has two primary functions: congestion avoidance and congestion management. Both types of CBQoS policy ensure application delivery by deploying strategies for dropping traffic, adjusting application responses, and building packet queues. Given the changes CBQoS is implementing when it's deployed, it is necessary to take a closer look at how it is affecting application performance and traffic flow.

The CBQoS Management Information Base (MIB) contains a wealth of statistics relative to existing QoS policies. Because the QoS configuration lives on the router, CBQoS collects statistics about the traffic traversing the router and reports how the QoS configuration is being applied.

Similar to Cisco IP SLA, CBQoS is built into Cisco IOS, so no additional licenses or hardware are required to enable and leverage its capabilities. However, an SNMP polling product with application-aware capabilities is a necessity in this type of environment. SNMP products with CBQoS capabilities can poll the CBQoS MIB to retrieve some of the following metrics:

- » Input and output QoS class map utilization
- » QoS class map drop percentage
- » QoS class map packet counts
- » QoS pre- vs. post- utilization traffic volume, traffic rate, and packet count
- » QoS traffic-shaping packets
- » QoS packet queue size
- » QoS police showing traffic marked in conformance, in excess, and in violation of defined policies

Instead of forcing network managers to wear a blindfold once QoS has been implemented, these metrics complement any QoS deployment strategy for maintaining control over application delivery. Visibility into the utilization, health, and scope of QoS policies is a necessity for properly troubleshooting applications that are part of the QoS policy tree.

NetVoyant's application-aware capabilities offer full visibility into CBQoS metrics for any Cisco device supporting the MIB. NetVoyant can be configured to perform SNMP polling for CBQoS metrics at the user's discretion, with no requirement to build custom reports. NetVoyant CBQoS reporting provides a wealth of insight into the effects of QoS deployment to help you judge and tune its effectiveness.

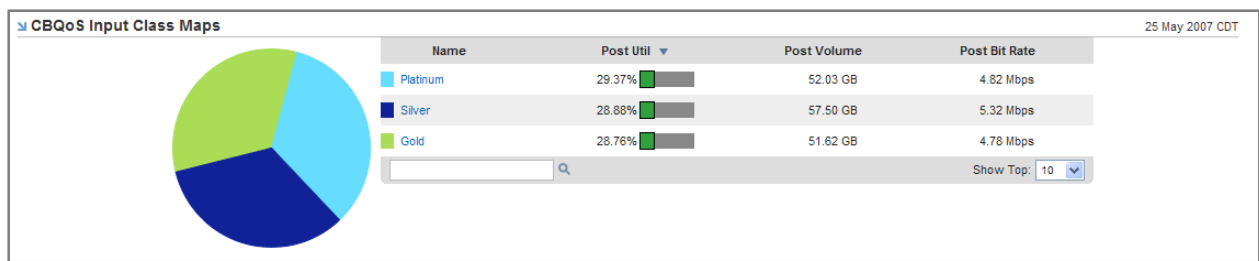


Figure 4 - NetVoiant displays overall utilization by class in a graphical user interface

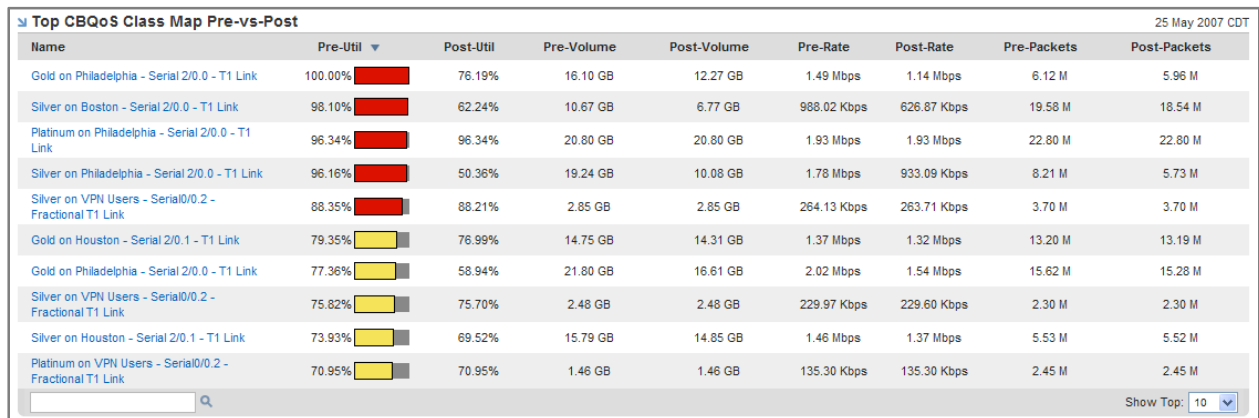


Figure 5 - NetVoiant provides analytical views into pre- and post- class statistics on any QoS enabled network circuit

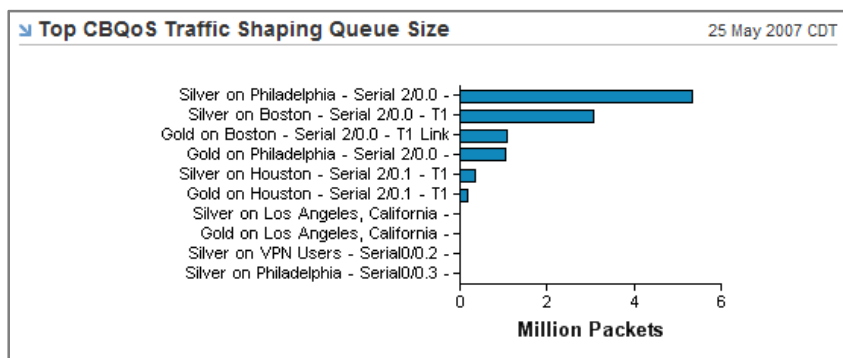


Figure 6 - NetVoiant reports queue size on any QoS class, network circuit combination

Alongside response time metrics for QoS-enabled applications and protocol-based traffic analysis intelligence per QoS class, CBQoS provides the network device's point of view of device utilization, health, and operation before and after QoS deployment. Without CBQoS, network managers are flying blind. They're at the mercy of their QoS configurations, hoping, based on little or no evidence, that their strategy is not adversely affecting the applications running on the network.

Gaining a New Level of Visibility with Cisco NBAR

Given the complex behavior and architecture of many popular applications, the discovery and identification of application traffic flowing over network links can be challenging. To continue the analogy to the human circulatory system, where doctors use expensive microscopes to analyze blood cells, network managers have to acquire their own costly tools to analyze and identify applications. However, application discovery is essential for managing application delivery because, after all, you need to know what needs to be managed. Instead of littering the network with probes and devices to analyze network traffic for application inspection, Cisco has developed a better solution: Cisco Network-Based Application Recognition (NBAR).

Similar to IP SLA and CBQoS, NBAR is built into Cisco IOS. From within the network device operating system, NBAR can inspect packets traversing the device and identify the corresponding applications. This means traffic such as TCP packets running over port 80 could be more accurately labeled as `http://www.google.com`, SAP, Microsoft SharePoint, or `http://www.salesforce.com`. This level of identification at the router is especially beneficial in virtualized environments, where associating server port ranges with IP addresses to identify applications can be challenging. Service providers can also benefit from NBAR capabilities by properly identifying applications prior to VPN encryption, allowing them to provide differentiated services across their WAN. Table 2 below is a sample list of protocols NBAR is able to properly tie to their layer 7 applications.

Sample List of Protocols		
Protocol	Type	Description
BitTorrent	TCP	File-sharing application
Gnutella	TCP	File-sharing application
Kazaa2	TCP	File-sharing application
eDonkey	TCP	File-sharing application
Fasttrack	TCP	File-sharing application
Napster	TCP	File-sharing application
SCCP	TCP	Skinny Call Control Protocol
SIP	TCP and UDP	Session Initiation Protocol
MGCP	TCP and UDP	Media Gateway Control Protocol
H.323	TCP and UDP	An ITU-T standard for digital videoconferencing over TCP/IP networks
SKYPE	TCP and UDP	Application allowing telephone conversation over the Internet
FTP	TCP	File Transfer Protocol
Exchange	TCP	MS-RPC for Exchange
HTTP	TCP	HTTP with URL, host, or MIME classification
Citrix	TCP	Citrix published application
Netshow	TCP/UDP	Microsoft Netshow
RealAudio	TCP/UDP	RealAudio Streaming Protocol
r-commands	TCP	rsh, rlogin, rexec
StreamWorks	UDP	Xing Technology Stream Works audio/video
SQL*NET	TCP/UDP	SQL*NET for Oracle
SunRPC	TCP/UDP	Sun Remote Procedure Call
TFTP	UDP	Trivial File Transfer Protocol
VDOLive	TCP/UDP	VDOLive streaming video

Table 2 – Cisco NBAR supported applications and protocols

While Cisco IOS NetFlow has become the de facto standard for identifying protocol traffic mixes on network circuits, it does not provide application-layer visibility. Instead, it requires the user to make the connection between protocol port and a specific application. NBAR closes this gap for programs requiring specific application classification, such as QoS. While NetFlow continues to rise in popularity due to its widespread availability and straightforward implementation, NBAR complements NetFlow when application layer identification is needed.

Once again, an SNMP polling product can make data collection from Cisco tools significantly less time-consuming compared to manually copying metrics from a CLI or developing custom scripts. Unlike network management tools that rely solely on NetFlow for traffic identification, NetVoyant forms part of a comprehensive approach to application-aware network management by adding NBAR data to the NetQoS Performance Center. Similar to CBQoS, NetVoyant polls network devices via SNMP to collect metrics specific to the NBAR configuration. When deployed alongside the NetFlow collection and analytical capabilities of NetQoS ReporterAnalyzer, NetVoyant provides unparalleled insight into the dynamics of network traffic composition.

NetVoyant NBAR data views provide utilization, volume, and rate metrics on a per-application basis relative to the network circuit carrying the traffic.

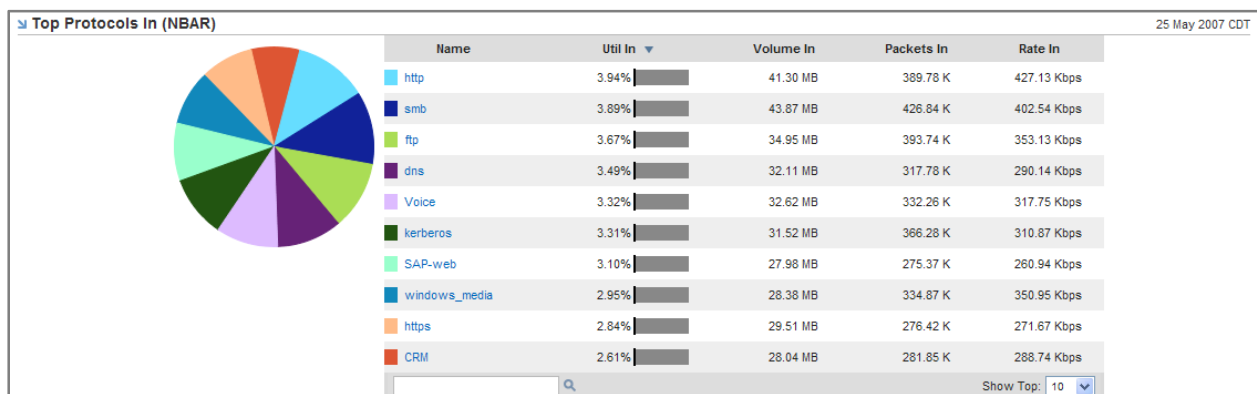


Figure 7 - NetVoyant shows the NBAR protocol/application mix, utilization, packets and rate for specific network devices and circuits

Application discovery and identification are necessary components of managing application delivery, and Cisco NBAR is an accessible technology for accomplishing the task. As a free component within Cisco devices, NBAR is a much more cost-effective solution than application discovery hardware when deployed across the wide area network. With all of these benefits, NBAR collection should be a requirement for any SNMP polling product that is part of an application delivery management portfolio.

Conclusion

Leveraging application-aware capabilities as part of a revamped approach to network management does not have to be difficult, expensive, or time-consuming. First, all of the capabilities discussed in this white paper are free of charge because they already exist in most of Cisco’s router and switch product lines. Second, relying on a SNMP

polling product such as NetVoyant for data collection in all cases can save time and greatly increase the value of your Cisco device and configuration data. There are better ways to use a network engineer's time than copying values out of a CLI or supporting a series of scripts.

Perhaps the most useful strategy within the application-aware approach is leveraging the analytical capabilities of a top-flight SNMP polling product. NetVoyant provides deep and broad reporting based on SNMP polling for Cisco device data, along with baselines, thresholds, and alerts to help makes sense of the data and enable management by exception.

We've tried to emphasize the importance and value of making application-aware data from network devices part of the application delivery strategy in your environment. No other data source can provide this level of understanding of traffic composition and knowledge of application performance while also offering low cost, ease of deployment, and convenience.

About the NetQoS Performance Center

The NetQoS Performance Center unlocks the intelligence needed to quantify network and application performance across an entire organization with end-to-end application response time monitoring, network traffic analysis, device performance management, long-term packet capture and analysis, and VoIP performance monitoring. Via a single Web-based management console, the NetQoS Performance Center integrates the data in customized views to help organizations optimize application delivery, solve problems faster, mitigate the risks from change, and make the most efficient use of resources. With role-specific views for different groups in an IT organization, such as network engineering, operations, IT service managers, and IP telephony management, the NetQoS Performance Center enables staff at all levels to:

- » Measure end-user application response times
- » Provide consistent application service delivery
- » Understand how infrastructure changes affect network and application performance
- » Isolate performance problems to the application, server, or network
- » Identify the applications and users consuming bandwidth, and when
- » Avoid unnecessary WAN costs
- » Correlate network performance to VoIP call quality of experience
- » Manage the convergence of voice, video and data
- » Identify virus or denial of service attacks and unauthorized application usage

About NetQoS

NetQoS is the fastest growing network performance management products and services provider. NetQoS has enabled hundreds of the world's largest organizations to take a Performance First approach to network management—the new vanguard in ensuring optimal application delivery across the WAN. By focusing on the performance of key applications running over the network and identifying where there is opportunity for improvement, IT organizations can make more informed infrastructure investments and resolve problems that impact the business. Today, NetQoS is the only vendor that can provide global visibility for the world's largest enterprises into all key metrics necessary to take a Performance First management approach. More information is available at www.netqos.com.

NetQoS Global Headquarters

5001 Plaza On The Lake

Austin, TX, 78746 United States

Phone: 512.407.9443

Toll-Free: 877.835.9575

Fax: 512.407.8629

NetQoS EMEA

1650 Arlington Business Park

Theale Reading, RG7 4SA United Kingdom

Phone: + 44 (0) 118 929 8032

Fax: + 44 (0) 118 929 8033

NetQoS APAC

NetQoS Singapore Representative Office

Level 21, Centennial Tower

3 Temasek Ave., Singapore 039190

Phone: + 65 6549 7476

Website: www.netqos.com

E-mail: sales@netqos.com

© 2001-2008 NetQoS, Inc. All rights reserved. NetQoS, the NetQoS logo, SuperAgent, and NetVoyant are registered trademarks of NetQoS, Inc. ReporterAnalyzer and Allocate are trademarks of NetQoS, Inc. Other brands, product names and trademarks are property of their respective owners.
20080930