Multi-Protocol Label Switching and the *nGenius*® Solution

Networked Application Visibility Where and When You Need It

Executive Summary

Multi-Protocol Label Switching (MPLS) is becoming mainstream as enterprises and government agencies look for new ways to lower costs, extend scalability, improve reliability, and secure their networked data. In some cases, however, MPLS comes with a lack of visibility because the very thing that helps optimize packet routing may also obscure the details most network professionals require for troubleshooting and traffic engineering their networks.

This paper outlines the best practices for collecting network and application performance information over MPLS-enabled wide area networks (WANs) by using the *nGenius*® Solution's Site Monitoring feature to monitor traffic flows destined for remote sites. Site Monitoring overcomes the complexity involved in MPLS network configurations by letting IT staff deploy *nGenius* Probes on the LAN side of the network while still monitoring traffic from the remote-site WAN perspective.

MPLS

MPLS enables organizations to deliver IP traffic over the shared, public network with the reliability and security of a dedicated point-to-point network connection. The use of MPLS is increasing because it is expressly built to transport multimedia voice, video, and data traffic in a manner that maintains high quality and low latency delivery.

Challenges to Monitoring MPLS Deployments

The choice to implement MPLS is often coupled with a few other elements: VoIP, QoS, and/or VPNs. VoIP implementations are growing past test phases to general enterprise-wide use, thus making efficient transport over WAN connectivity a further initiative. QoS technology is often deployed in conjunction with MPLS services to ensure that latency-intolerant, converged applications such as voice and video are provided a higher level of service. This adds to the complexity of monitoring and analyzing the applications and their QoS classes. These applications and their associated QoS levels are the foundation for proper traffic classification and delivery to their respective remote locations, therefore it is crucial that IT staff have the necessary insight into them in order to effectively troubleshoot and traffic engineer their MPLS networks. Finally, securing data traffic and confidential information often makes it necessary to implement encryption and security measures to protect transport over a public WAN.

As IT departments migrate from traditional Frame Relay and ATM networks to MPLS, they need to maintain visibility into how their applications are performing across the WAN. The packet labeling and/or security services, characteristic of MPLS networks (e.g., encryption and VPNs), can obscure views into application flows and activity in MPLS trunks. Where these links and their associated remote locations are critical to the organization's communication strategy, IT staff must have visibility into them so they can optimize network and application performance.

Leveraging CDM™ Technology to Monitor Applications in MPLS Environments

WAN MPLS networks are often deployed over T3/E3 or OC-3/OC-12 circuits in central sites and over T1/E1 or T3/E3 physical connections at remote offices. Packet labeling and/or security services often mask the application-layer details of the traffic over the segments. Site Monitoring, a feature of NetScout's *nGenius* Performance Management System, enables *nGenius* Probes to monitor traffic flows destined for remote sites. It overcomes the complexity involved in monitoring MPLS network configurations by letting IT staff deploy *nGenius* Probes at the WAN edge of the network in their central sites yet still monitor traffic from the remote site perspective.

Where to Instrument Your WAN MPLS Network

The best vantage point in an enterprise network where *nGenius* Probes or *nGenius* AFMons can be deployed to gain visibility around the MPLS network is on the LAN side of the edge router. Regardless of whether the first MPLS label is applied at the router in the carrier's cloud, or on your CPE router (serving as the Label Edge Router), the LAN side of that WAN-edge router provides the best monitoring location for overall investment protection.

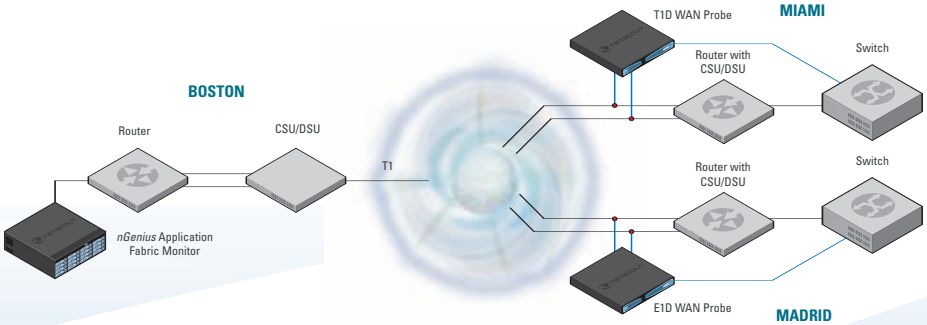

Figure 1 (left):

The network diagram shows an MPLS WAN deployment where the *nGenius* Probe is deployed on the LAN side of the customer premise router for the monitoring application flow traffic regardless of whether the customer's router or the first router in the carrier network serves as the Label Edge Router.

Deploying an *nGenius*® Fast Ethernet or Gigabit Ethernet Probe or *nGenius* AFMons on the LAN side of the WAN router of either headquarters and/or data center locations will provide visibility into all the traffic between a headquarters, data centers, and/or remote locations. Site Monitoring makes it possible for the *nGenius* Solution to monitor and analyze application traffic on the segment from the individual remote sites' perspective.

How Site Monitoring Works for MPLS Visibility

Site Monitoring, enabled by NetScout's innovative CDM™ technology, gives visibility through multiple WAN cloud technologies. For monitoring remote offices, a variety of Site Monitoring configuration choices is available and includes:

- Identifying each remote site with the associated subnet addresses for that office, such as 108.60.0.0/32.
- Naming each remote site, such as Chicago or Beijing Office.
- Assigning the interface speed of the probe that is tapping the LAN side of the router to match the actual speed of the WAN trunk. For T3 it would be 45Mbps or for E3, 34Mbps in each direction.
- Setting the virtual interface speed for each site to match the bandwidth for each channel, such as 1.544Mbps.

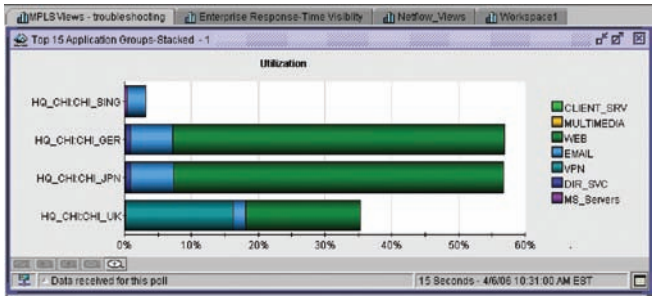

Figure 2: When configured with the Site Monitoring feature, *nGenius* Performance Manager provides real-time views of application activity between headquarters and remote sites. In this case, the graph displays application activity between the headquarter location and remote locations in Singapore, Germany, Japan, and the United Kingdom

The *nGenius* Probe or *nGenius* AFMon monitors every configured remote site with the same level of detail and granularity as if it were a Frame Relay DLCI or ATM PVC. Real-time views of protocols, applications, hosts and conversations for each remote site can be displayed in Workspace Views in *nGenius* Performance Manager.

Users can create *nGenius* Performance Manager Newspapers so that the Capacity Planning section reports on Most Utilized sites with drill downs to articles on Site Application Breakdown, Most Active Applications, and top Application Hosts and Conversations. Site Monitoring provides all the rich real-time analysis and historical reporting necessary for optimizing the network and application performance at remote locations. Designed with high-definition granularity reports can provide details at one-minute intervals.

QoS Monitoring Over MPLS Networks

As they prepare to migrate to MPLS services, enterprise corporations often also initiate a QoS policy for the first time and may internally assign the following QoS delivery groups:

- Highest precedence delivery: latency-intolerant voice and video applications
- Secondary precedence delivery: revenue-generating business applications
- Best effort delivery: non-critical, email and web-surfing traffic.

Service providers have responded by developing and offering comparable multi-tiered MPLS service offerings to provide the required security and priority delivery choices for sensitive or critical enterprise business traffic. For instance, Gold, Silver and Bronze classes of service may be offered.

Once the IT staff configures the priority levels in corporate infrastructure routers, typically by setting a standard Differentiated Services Code Point (DSCP), that same designation is used to inform the MPLS Router which delivery class of service to set for the packet. It is imperative that the QoS class assignments in the enterprise are configured correctly so that the carrier can deliver them appropriately. For instance, if voice is mistakenly configured to the lowest QoS priority level in the enterprise network, users may experience latency in their VoIP phone calls. IT staff needs visibility to see precisely which applications reside in each QoS class for every remote site in the network so that they can be prioritized as they intended.

nGenius Performance Manager provides real-time views of QoS levels in network segments as identified by DSCP classifications as well as the applications assigned to each QoS category. This functionality makes it possible for IT staff to monitor and trend patterns of application behavior for network segments, remote sites and associated QoS categories simultaneously. Further, they can maximize the performance of QoS implementations by pinpointing application and configuration issues through in-depth, on-going monitoring and analysis. As enterprises and service providers work together to ensure the optimal delivery of business applications, it is essential to have this level of granularity for application-layer visibility.

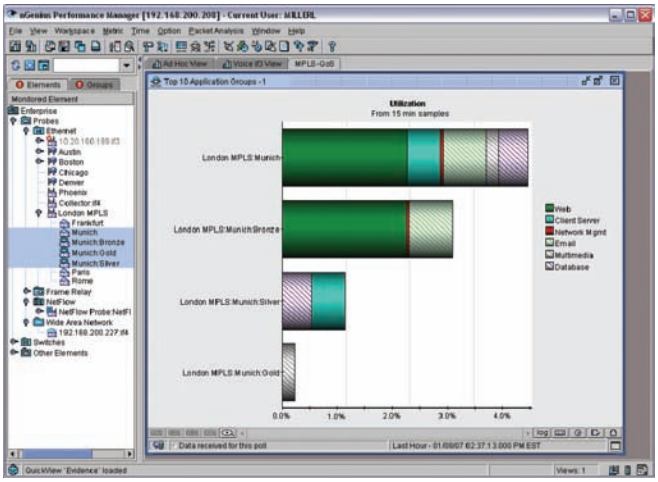

Figure 3: When QoS is used in conjuction with an MPLS network, the Site Monitoring feature in the *nGenius* Performance Management System enables display of real-time views of application activity within each QoS class for the associated remote location. In this case, the graph shows application activity for the Munich remote site along with its three assigned QoS classes.

Cases In Point

A Global Airline Gains Maintains Visibility During MPLS Rollout

A global airline based in Europe needed to optimize performance of the applications that supported ticket purchases, credit card authorization requests, passenger check-ins, seat assignments, and checked baggage information during a global MPLS rollout. Using the *nGenius* Performance Manager Site Monitoring feature, the airline had valuable visibility to over 350 sites as they migrated from Frame Relay and ATM to MPLS services.

The *nGenius* Solution provides visibility to identify and track the applications traversing their network, regardless of WAN access topology in use. With specific application identification, bandwidth consumption, and key user information, the airline IT staff can effectively troubleshoot network and application problems and plan for capacity changes based on the business use of the network. Further, the IT group publishes daily, weekly, and monthly *nGenius* NewsPaper reports to executives and IT staff that are grouped by geographic regions. These newspapers can roll up site information for all remote locations, regardless of whether they use MPLS, Frame Relay or ATM for their connectivity.

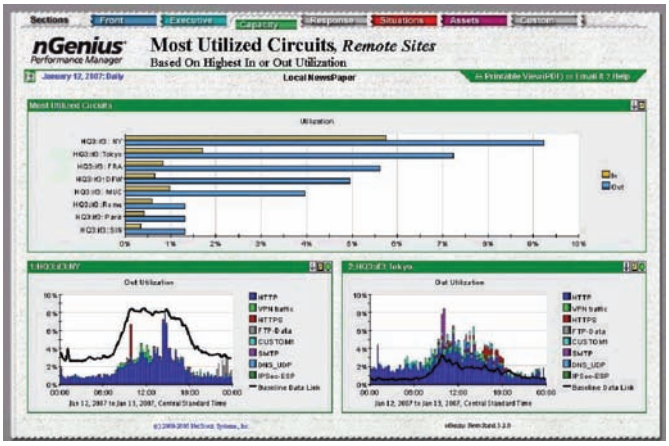

Figure 4: nGenius Performance Manager's NewsPapers, such as the one illustrated, for daily, weekly, and monthly reporting enabled the airline to see most utilized circuits to remote locations around the world for their busiest sales offices and airport locations.

Home Improvement Retailer uses nGenius Solution to "Measure Twice, Cut Once"

A large home improvement retailer with hundreds of stores in North America implemented the *nGenius* Solution with site monitoring prior to starting their MPLS rollout. Knowing they were soon to migrate, they selected *nGenius* LAN Probes and installed them on the LAN side of the WAN routers that connected to Frame Relay links. During pre-deployment, network engineers had visibility into the types and volumes of traffic that was typical for each site, prior to converting them to MPLS.

When the time came to contract with their WAN carrier for each site's new MPLS service, the network engineers were able to order the bandwidth necessary to support each location's business use of the network based on the evidence collected for that site. Once the cutover was complete, the network engineers used the exact same *nGenius* LAN Probes on the LAN side of the WAN routers to continue to monitor the application flows for troubleshooting and capacity planning activities with *nGenius* Performance Manager. This is cost-effective from both the management tool perspective – same tool without any additional purchase - as well as from the bandwidth management perspective – cost avoidance that might have occurred with change orders and over capacity costs.

nGENIUS

The *nGenius* Performance Management System
The *nGenius* Solution addresses the complex requirements of network and application performance management in today's converged, virtualized environment and is comprised of:

- ***nGenius* Performance Manager:** Software that analyzes the information collected by *nGenius* Probes, Collectors, Application Fabric Monitors, and other intelligent network devices and delivers integrated network and application monitoring, troubleshooting, capacity planning, and reporting in a single product.
- ***nGenius* Probes:** Dedicated hardware monitoring devices that passively identify, collect, and analyze application-level traffic data across the enterprise.
- ***nGenius* Collectors:** Dedicated hardware devices that collect application conversation data via NetFlow records and IP SLA tests.
- ***nGenius* Application Fabric Monitors:** Appliances that combine real-time and historical monitoring and analysis with storage for large packet trace captures for high performance, high reliability, high capacity recording and infrastructure monitoring.
- ***nGenius* Analytics:** Software that delivers automated, proactive early detection and aids in diagnosis of network and application performance anomalies.

NETSCOUT

Corporate Headquarters
NetScout Systems, Inc
310 Littleton Road
Westford, MA USA
Ph: 978.614.4000
Fax: 978.614.4004
www.netscout.com

European Headquarters
100 Pall Mall
London SW1Y 5HP
United Kingdom
Ph: +44 20 7321 5660
Fax: +44 20 7321 5663

Asia/Pacific Headquarters
Room 105, 17F/B,
No. 167
Tun Hwa N. Road
Taipei, Taiwan
Ph: +886 2 2717 1999
Fax: +886 2 2547 010

North American Offices
New York City, NY
Washington DC
Chicago, IL
San Jose, CA
Toronto, Ontario,
Montreal, Quebec

European Offices
Frankfurt, Germany
Paris, France
Oslo, Norway

Asian Offices
Beijing, China
Guangzhou, China
Hong Kong, China
Tokyo, Japan
Singapore
Pune, India

MPLS20070412
2007-04-17