Executive Summary

Multi-Protocol Label Switching (MPLS) has gained attention recently as increasing numbers of enterprises and government agencies look for new ways to lower cost, 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.
**What is MPLS**

Multi-Protocol Label Switching (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 making it an increasingly popular networking alternative. As companies today grapple with the demands of converging their voice, video, and data networks into one while maintaining the high quality and low latency delivery that their users have come to expect, MPLS is one approach that makes this possible.

MPLS supports Layer 2 services such as Ethernet, Frame Relay and ATM with high reliability and performance while simultaneously offering the scalability necessary to deliver Layer 3 services such as IP VPNs. MPLS is a fast-path routing technology, where the router makes a forwarding decision on a packet based on a label included in the packet. A Forward Equivalence Class (FEC) is assigned to each packet defining the priority and routing with which it will be handled. The first router to apply an MPLS Label to a packet is known as the Label Edge Router (LER). The packet traverses a Label Switch Path (LSP) hopping between Label Switch Routers (LSR) with the forwarding decisions based on the Labels they see.

**Challenges to Monitoring MPLS Deployments**

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.

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, adding 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 to troubleshoot and traffic engineer their MPLS networks.

**Leveraging CDM™ Technology to Monitor Applications in MPLS Environments**

NetScout’s CDM™ architecture provides the flexibility and underlying structure for tracking and optimizing networked applications regardless of the topology involved. In the case of MPLS, the nGenius Solution provides the necessary application level visibility with slightly different approaches for each of the major encapsulation methods listed in the MPLS Standards call out box. Regardless of the encapsulation method being deployed, PPP, Frame Relay, or ATM, the nGenius Solution provides the information needed to optimize application performance over the enterprise-wide network.
**PPP Networks**

Point to Point (PPP) networks are used in Ethernet, POS, and in some T1/E1 and T3/E3 dedicated circuits. NetScout’s *nGenius* Fast Ethernet and Gigabit Ethernet Probes, the OC-3 and OC-12 POS Probes, as well as T1/E1 and T3/E3 WAN Probes all support RFC 3032 that defines PPP over MPLS networks.

![PPP Network Diagram](image)

*nGenius* Probes deployed in PPP environments, such as Fast Ethernet or Gigabit Ethernet segments or switches, recognize the MPLS label on packets traversing the monitored traffic. They can bypass the 32-bit MPLS header to view the critical Layer 3 through 7 network and application level information and collect details from the packets for all the applications, hosts and conversations traversing the network. These details can be used for real-time viewing in *nGenius* Performance Manager, or for logging into the database and generating daily, weekly and monthly *nGenius* NewsPaper Reports.

**Frame Relay and ATM Networks**

Frame Relay and ATM encapsulations are typically found in WAN MPLS networks and are often deployed over T3/E3 or OC-3/OC-12 circuits in central sites and in T1/E1 or T3/E3 physical connections at remote offices. When Frame Relay and ATM are running over MPLS per the RFC 3034 and 3035 standards, the packet labeling and/or security services, such as encryption and VPNs, characteristic of MPLS networks, may 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 Frame Relay and ATM over MPLS network configurations by letting IT staff deploy *nGenius* Probes at the WAN edge of the network in their central sites while still monitoring traffic from the remote site perspective.

**Where to Instrument Your WAN MPLS Network**

There are two points in an Enterprise network where you can deploy *nGenius* Probes to gain visibility around the MPLS network – either on the LAN side of the edge router or on the WAN side, depending on how your MPLS service is delivered. Telecommunications providers can offer MPLS service that starts either at the customer premise or at the carrier WAN cloud. If the first MPLS label is applied at the router in the carrier’s cloud, then the packets leaving the corporation’s premise router is considered to be native traffic and NetScout can monitor and analyze it with a standard WAN probe, for instance a T3 or E3 probe.
If the Enterprise Customer’s WAN router serves as the MPLS Label Edge Router, that is, it applies the first label for directing the pathing and priority of the packets, then the trunk connected to that router at the point of demarcation will be masked, making WAN-side traffic visibility challenging. NetScout’s Site Monitoring feature overcomes the complexity created by MPLS network configurations and enables IT organizations to deploy nGenius Probes on the LAN side of the WAN router and monitor traffic destined for remote sites.

In MPLS WAN scenarios, an nGenius Fast Ethernet or Gigabit Ethernet Probe is deployed on the LAN side of the WAN router. Many companies deploy a hub and spoke architecture for communicating between headquarters and remote locations. When the nGenius LAN Probe at the headquarters has the Site Monitoring feature enabled, then the nGenius Solution can monitor and analyze application traffic on the segment from the individual remote sites’ perspective.

Figure 3: The network diagram illustrates an MPLS WAN deployment where the Label Edge Router is located in the WAN cloud. This means that the first label to instruct delivery and priority handling of the packet is applied by the router in the telecommunications provider’s network.

Figure 4: The network diagram shows an MPLS WAN deployment where the Label Edge Router is located on the customer premise. This means that the first label to instruct delivery and priority handling of the packet is applied by the router at the edge of the customer’s enterprise network. The first router the packet encounters in the WAN cloud is a Label Switch Router, which will switch the packet based on the label it sees on the arriving packet.

Figure 5: nGenius Fast Ethernet or Gigabit Ethernet Probes are deployed on the LAN side of the edge router of a MPLS segment. With site monitoring configured, IT staff obtains the necessary visibility to application traffic to and from their remote offices.
How Site Monitoring Works for MPLS Visibility

Site Monitoring, enabled by NetScout’s innovative CDM™ technology, provides visibility through multiple WAN cloud technologies. For monitoring remote offices, a variety of Site Monitoring configuration choices are available and include:

- 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 Miami or Madrid 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.
- Setting the virtual interface speed for each site to match the bandwidth for each channel, such as 1.544Mbps.

The nGenius Probe monitors every configured remote site 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.

nGenius Performance Manager Newspapers can be created 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.

QoS Monitoring Over MPLS Networks

Companies who have initiated a QoS policy with their MPLS service may assign the following QoS delivery groups:

- Highest: latency intolerant Voice and Video applications
- Mid-level: revenue generating business applications
- Lowest: non-critical e-mail and web surfing traffic.

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, it is not the carrier’s issue if users 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 granularity of application layer visibility.

Case Study

The ticket offices, airport locations, and travel agents of a global airline need to communicate ticket purchases, credit card authorization requests, passenger check-ins and seat assignments, as well as checked baggage information with their European headquarters over the Wide Area Network (WAN). In the summer of 2003, the airline began converting their airline locations and largest sales offices from Frame Relay and ATM services to MPLS services. While achieving their budgetary and cost savings goals, they lost visibility into the application-layer details that they had previously had seen.

Using the nGenius Performance Manager Site Monitoring feature, the airline was able to restore valuable visibility to the nearly 100 sites now using MPLS services. Site Monitoring was implemented as follows:

- At the European data center, the WAN routers provided by the telecommunications carrier serve as the label edge router, applying the first MPLS label to designate pathing and priority information.
- On the LAN side of the router, the IT staff installed nGenius Fast Ethernet Probes and set the interface speeds to match the WAN connection for monitoring and utilization analysis.
- Each remote office had a unique subnet address or group of subnet and IP addresses which the network managers then used to configure the individual sites in the nGenius Probe, identifying each site with its location name, such as Hong Kong, Rome and New York.
- When this had been completed, the IT staff began monitoring application traffic between the European central data centers and each remote airport or sales office location.

The valuable information derived from application visibility to their daily operations is the most significant benefit the airline's IT department has gained from their nGenius deployment. With the MPLS locations essentially devoid of specific application identification, bandwidth consumption, and specific user information, the airline IT staff was having difficulty troubleshooting network and application problems. Once application visibility was restored, they could identify and track 95% of the applications traversing their network. Now when they see an increase over the 5% "unknown" traffic on their network, it is easy for them to execute a packet capture and apply sophisticated decodes from NetScout's more than 1300 discrete decodes. They can pinpoint whether the traffic is from the addition of a new business application or whether it is something more malicious, such as a new network virus.
The airline has realized other concrete benefits from their NetScout installation. They can:

- Publish daily, weekly, and monthly NewsPaper Reports to Executives and IT staff that are grouped by geographic regions for Europe, Asia, and North America. These newspapers can roll up site information for all remote locations, regardless of whether they use MPLS, Frame Relay or ATM for their connectivity.

- Analyze application responsiveness in context with network activity for optimizing response time of revenue and productivity-impacting applications such as online ticketing and passenger check-ins.

- Align telecommunications costs with business use of the network, such as VoIP initiatives vs. streaming audio.

Now that they can see all the application utilization with ongoing trending and peaks for each remote site, the company can quickly optimize business applications enterprise-wide, reducing the time it takes to troubleshoot problems and improving service delivery to their end users.

For more information on this topic and others like it CLICK HERE or visit www.netscout.com
The nGenius® Solution is comprised of nGenius® Performance Manager, nGenius® Probes and for specialized situations, additional appliances including nGenius® Flow Collector and nGenius® Flow Recorder.

nGenius Performance Manager is a software application that analyzes the information collected by nGenius Probes as well as other network devices, and delivers the features and functions of multiple performance management disciplines in a single product.

nGenius Probes are hardware monitoring devices that are the industry’s most advanced sources for identifying, collecting and analyzing application-level traffic data across the enterprise.

nGenius Flow Collectors are dedicated hardware devices optimized for collecting application conversation data via NetFlow records produced by leading network infrastructure devices.

nGenius Flow Recorder is an appliance that couples storage for large packet trace captures and graphics-based data mining software. It continuously records all traffic and produces a network audit trail for post-event forensics requiring full packet payload details.

©2005 NetScout Systems, Inc. All rights reserved. NetScout and the NetScout logo, nGenius and Quantiva are registered trademarks of NetScout Systems, Inc. The CD-0 logo, MasterCare and the MasterCare logo are trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.

CC-0170-04