Monitoring Performance in MPLS Networks from the Service Provider Perspective

nGenius® Solution provides Networked Application Visibility into the Customer Facing part of the Network

Multi-Protocol Label Switching (MPLS) is fast becoming the choice of both enterprises and government agencies to transport their IP multimedia, business applications and customer services across the Wide Area Network (WAN). To attract this new business from long sought after Fortune 1000 and Global 2000 customers, telecommunications providers are responding with new, highly scalable, multi-tiered, subscription-service offerings, and to retain those hard won new customers, carriers need to protect the quality of the user experience. In MPLS environments, the challenge is how to monitor, troubleshoot and traffic engineer the network to ensure a quality experience for those end users – each and every time. This application note offers recommendations to carriers on how they can use the *nGenius* Solution to collect and analyze network and application performance information over MPLS IP-based networks that transport voice, video and data traffic in different priority delivery service classes.

MPLS Monitoring Challenges

To attract new customers and satisfy demands of existing customers for more secure, cost-effective transport of their converged voice and business applications, most telecommunications providers are introducing service offerings over MPLS. Enterprises are taking advantage of service offerings that break out delivery for voice and video into a high priority class such as a "Platinum Class," and tiered choices for their more latency tolerant business services into "Gold, Silver, and Bronze" offerings. But in doing so, carriers are uncovering a variety of new challenges:

- They need real-time, application level analysis of activity across the MPLS cloud
- They require a way to optimize the performance of key business services that they have created to market to their customer base
- They must distinguish traffic between individual customers and locations
- They have to track routing activity as an integral part of their traffic engineering tasks
- They need to identify and track standards based prioritization methods, such as Type of Service (ToS) bits or Differentiated Services Code Point (DSCP) per RFC 2474 and 2475.

The network teams at many carriers are asking for more extensive instrumentation. Using NetFlow or MIBII exclusively to create and secure service assurance to their end users are inadequate as these data sources lack the information necessary to track the routing changes and customer IP addresses in the carrier environment. MPLS carriers need a solution that provides application monitoring and visibility with a network perspective.

Network Considerations

To respond to the challenges listed above, any performance monitoring solution needs to have an awareness of how the traffic is transported across the MPLS environment. A public MPLS network will adhere to the RFC 2547bis standard that defines the way service providers deliver their IP backbone and provide VPN services to customers. An MPLS/BGP network creates VPN tunnels based on MPLS labels for each customer route between the service provider's edge routers (PEs) and each end connecting to customers' edge routers (CEs).

A customer site is connected to a service provider network via one or more ports, and the service provider associates each port with a specific VPN routing and forwarding identifier known as a VRF. Since each customer likely uses internal IP addresses, which may be duplicates of other customers', a performance monitoring solution needs to examine and distinguish individual customer's traffic at the egress point of the PE for the providers; otherwise, they cannot differentiate the traffic on a per customer basis. Figure 1 (next page) provides an illustration of a simple MPLS network deployment.

Two basic traffic flows occur in a BGP/MPLS VPN. The first is a control flow that is used for VPN route distribution and label switched path (LSP) establishment. The second is the actual data flow that is used to forward customer data traffic. Any MPLS monitoring solution a carrier deploys will need to leverage information from both traffic flows to troubleshoot and capacity engineer their customer facing network.

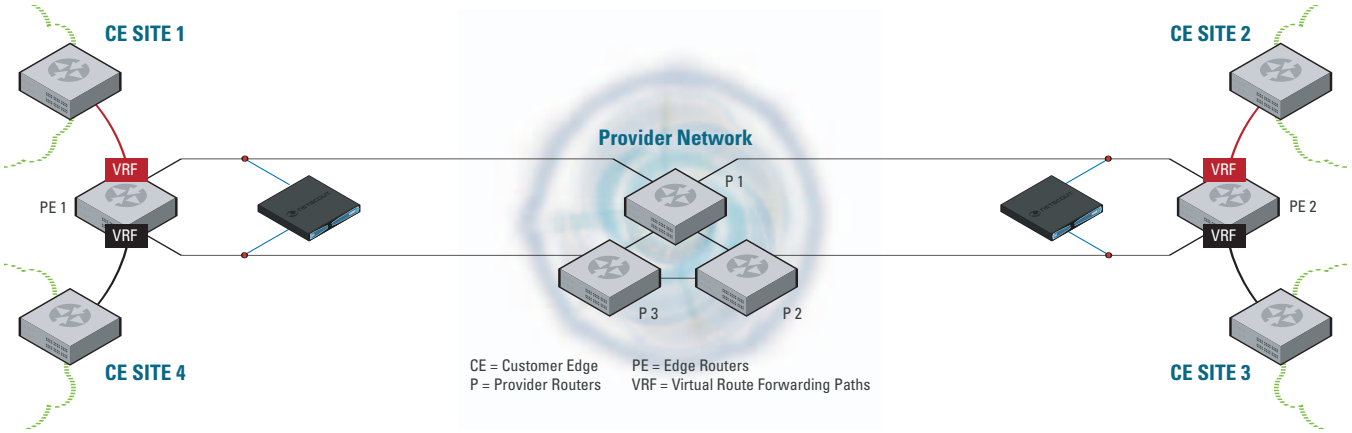

Figure 1: The diagram illustrates a typical network topology where a single service provider delivers a BGP/MPLS VPN service to multiple enterprise customers. In this simple example there are two PE routers connected to four different customer sites.

Meeting the Need

The *nGenius* Performance Management Solution includes capabilities that have been designed specifically to meet the network and application monitoring needs of carriers to ensure optimal performance in their customer facing MPLS networks. In order to segregate each customer's traffic, the *nGenius* Probe looks at the innermost MPLS label attached by the first Provider Edge (PE) router when the packets enter the network. Each customer and the routes their traffic traverses are unique; further, the labels are unidirectional and may change if the routes change. Thus the MPLS labels for each associated customer and PE router will be unique and can change as routes do, as well.

In order to track, monitor, analyze and trend any customer data for both ingress and egress traffic that may have different labels from each end of a route, the *nGenius* Probe maps the individual labels to a Site and maintains a state table in its memory similar to the VRF (Virtual route forwarding) table maintained by each PE router. The VRF tables are updated when the routes change or when the PEs boot up using BGP protocol. The PEs send BGP updates to other PEs it maintains routes with by advertising its labels that are tied to each customer. The BGP updates are also sent to a BGP route reflector device.

The *nGenius* Probes monitor the BGP update messages and track the MPLS Label, Router Distinguisher and Address prefix information. The *nGenius* Probe uses this information to create the VRF sites for tracking the VPN traffic. Virtual Interfaces are created based on the Router Distinguisher (RD) and the Physical Interface or Trunk with one virtual interface being created for each RD on a trunk. In *nGenius* Performance Manager, each site is represented using the VRF of the RD. See figure 2.

Benefits to Service Providers to MPLS Monitoring

Service Providers want and really need visibility into their MPLS traffic flows for a variety of reasons. Competition is fierce, particularly given the nature of a subscription service. Should a Fortune 1000 or Global 2000 customer become dissatisfied with the service quality of an existing provider, contracting with another is a very manageable alternative.

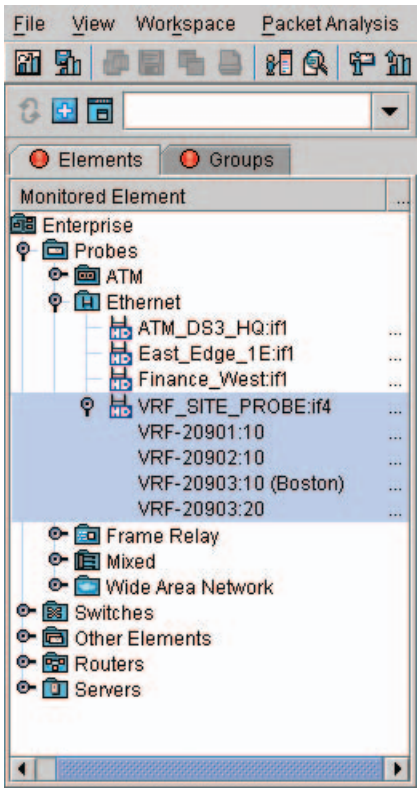

Figure 2: VRFs identified by the *nGenius* Probe from BGP updates are represented for tracking using the individual VRFs.

When using the *nGenius* Performance Management Solution, activities are likely to fall into several categories: troubleshooting internally discovered or customer reported problems, evaluating service response times to assist in customer contracted agreements, and traffic engineering and capacity planning projects. The following are some common, everyday type tasks the *nGenius* Solution enables:

Real-Time Troubleshooting

- Quickly identify a "bandwidth hog" in the MPLS segment by viewing a network segment and multiple individual VRFs assigned to it simultaneously.

- Effectively police network use with granular resolution of difficult to distinguish applications such as peer-to-peer ones or computer viruses that may be propagating throughout the carrier network, impacting bandwidth consumption as well as customer response time analysis.
- Perform in-depth, packet level troubleshooting with data capture and sophisticated decode analysis. Apply filters for protocols, applications or even VRFs to analyze activity and discover root cause of problems.

Proactive Fault Management

- Set and receive utilization thresholds, such as 70% utilization on a key customer segments for proactive management of impending congestion problems before end-user customers are impacted.
- Define and view time over threshold alarms, such as 60 seconds over 60% utilization on an important MPLS circuit to collect information on the top applications and users contributing to the increased traffic.
- Integrate device mapping and alarm management with a third party management application such as Hewlett Packard's HP Openview, IBM Tivoli or Mercury BAC.

Long-Term Capacity Planning

- Automate daily, weekly, monthly reports that highlight the most utilized trunks in the customer facing part of the network with other trended information. You can visually see when traffic patterns are different than they historically have been which may necessitate a change in traffic engineering.
- Share specific *nGenius* NewsPaper articles that focus on most utilized circuits -- the section where the individual VRFs will be analyzed and reported. This information may reveal that further changes in bandwidth to accommodate specific "power consumer" customer locations might be necessary.

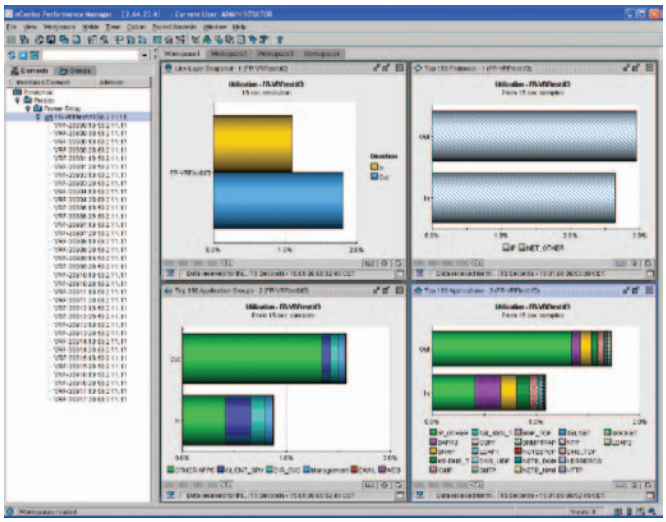

Figure 3: VRFs in real time illustrate application activity both inbound and outbound.

- Drill-down from specific *nGenius* NewsPaper articles on the applications that are contributing to the utilization of trunks and/or circuits. This information can facilitate discussions with the account on new prioritization recommendations for particular services such as Voice, Video, and Business Data services versus standard email or web surfing within the account.
- Customize and schedule reports leveraging on-demand capabilities supply by real-time views to track and trend specific activity or troubleshooting for a customer location with intermittent problems requiring attention.

Any or all of these particular tasks may become a regular activity as part of monitoring MPLS traffic flows in a service provider network. The *nGenius* Solution offers a robust set of capabilities to address these typical troubleshooting and capacity planning tasks in a flexible, customizable fashion.

Definitions

PE – Service Providers' Edge Routers that connect to CEs. PE routers also exchange routing details with CE routers using static routing, RIPv2, OSPF, or EBGP. They maintain VPN routing information, but typically only for the VPN routes of the VPNs to which it is directly attached. They exchange VPN routing information with other PE routers using IBGP.

CE – Customers' Edge device (either a router or a Layer 2 switch) that connects to, and generally establishes an adjacency to the directly connected service provider edge router (PE). Once the adjacency is made, the CE router advertises the site's local VPN routes to the PE router and learns remote VPN routes from the PE router.

P Routers – any router in the provider's network that does not attach to CE devices. They function as MPLS transit LSRs when forwarding VPN data traffic between PE routers. Since traffic is forwarded across the MPLS backbone using a two layer label stack, P routers are only required to maintain routes to the provider's PE routers; they are not required to maintain specific VPN routing information for each customer site.

LSRs – Label Switch Routers that forward VPN data traffic between PE routers.

VRF - VPN routing and forwarding (VRF) table, also known as the VPN routing table. Each PE router retains a VRF for each of its directly attached sites. Each customer connection is mapped to a specific VRF, which results in a port on the PE router, not a particular site.

RFC 2547bis – the standard that defines how service providers use their IP backbone to provide VPN services to customers.

Case Study

Recently a fixed-line operator and wireless provider (PTT) with a dominant presence in Europe and holdings in telecom operations and mobile phone carriers throughout Europe, as well as Central and South America, began an MPLS roll-out. Their specific challenge was to create and secure service assurance to customers as they converted the network and moved their customers over to a new MPLS network. Simultaneously, the PTT was in the process of migrating their corporate employees over to the MPLS network for inter-company communications. Their objective is to eventually deliver MPLS and/or Internet service to all their customers.

The IT team asked for more extensive instrumentation in order to create and secure the service assurance that customers would demand over the new network. The team knew that NetFlow or MIB II reporting for service assurance to their end users would be inadequate as they needed the BGP route table updates which are not maintained by these data sources. They needed to analyze in real-time, at the application level the individual customer's activity across the MPLS cloud as well as to optimize the performance of key business services within the network for their own customer orders, email, and billing activities.

The PTT selected the *nGenius* Performance Manager in combination with strategically deployed *nGenius* Probes as part of a phased in plan for managing and analyzing application traffic flows through the MPLS network. They started with site monitoring on the critical customer edge portion of the network, were moving to service assurance in the POP, and eventually to deploying monitoring and analysis in their data centers.

The PTT has discovered a number of key benefits to the *nGenius* Solution including:

- The *nGenius* Solution has been effective in monitoring critical customer paths across MPLS networks. Most importantly, the *nGenius* Probes can track which customer was represented by which MPLS label at a given time, store the information, collect BGP updates, and mix and match labels to identify the customer. The solution can then be integral in providing service assurance and troubleshooting capabilities on a per-customer basis.
- The *nGenius* Solution is vendor independent, and can easily support whatever infrastructure devices are in the carrier network, including Cisco and Juniper.
- The *nGenius* Solution's carrier class, highly scalable three-tier architecture supports multiple *nGenius* Performance Manager Servers deployed in a distributed manner. When implemented, the Global Manager serves as the master to the Local Servers as slaves where information between the two (or more servers) can be shared and accessed seamlessly to provide both real-time analysis and historical reports. For instance, the Most Utilized Segments report will analyze information from all servers to complete the report for an MPLS Network-Wide view -- or alternatively on a per-customer basis.
- *nGenius* Performance Manager can look at multiple network quality of service classes and display (or report on) who is at what class, what applications are in that class, and if there is a need for alternative paths for the QoS class to optimize their traffic engineering activities.
- The *nGenius* Solution's carrier class architecture with accessible *nGenius* Standby Server provides an insurance policy to the PTT with responsibility to deliver high availability in its backbone.

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, Flow 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* Flow Collectors:** Dedicated hardware devices that collect application conversation data via NetFlow records.
- ***nGenius* Application Fabric Monitors:** Appliances that combine *nGenius* Flow Recorder and *nGenius* Probe functionality for high performance, high reliability, high capacity recording and infrastructure monitoring.
- ***nGenius* Analytics:** Appliance-based software that delivers automated, proactive early detection and 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
Regus House
268 Bath Road
Slough, Berkshire,
SL1 4DX UK
Ph: +44 1753 725561
Fax: +44 1753 725562

Asia/Pacific Headquarters
Room 105, 17F/B, No. 167
Tun Hwa N. Road
Taipei, Taiwan
Ph: +886 2 2717 1999
Fax: +886 2 2547 7010

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