White Paper

Monitoring Service Delivery in an MPLS Environment

A growing number of enterprises depend on (or are considering) MPLS-based routing to guarantee high-bandwidth capacity for the real-time applications that require it. No matter where you are in the process of migration (either looking to deploy, installing the infrastructure, or working with service providers to use their infrastructure), understanding traffic patterns on your network can ensure you spend your organization's IT budget effectively.

Why MPLS?

Traditional Layer 3 routing protocols, in addition to being processor-intensive, have no way to determine Layer 2 characteristics such as bandwidth saturation and the reliability of connections.
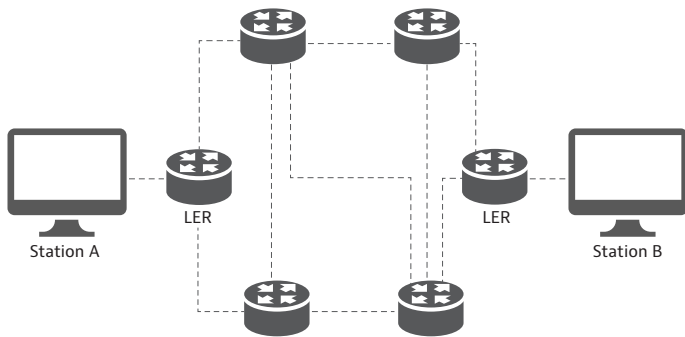
Asynchronous Transfer Mode (ATM) and frame relay technology were developed to address these problems, but these older technologies were not designed for the large frame sizes made possible by optical links.

Multi Protocol Label Switching (MPLS) was designed to preserve the traffic-shaping and out-of-band control provided by ATM/Frame Relay, while eliminating the cell-switching and signaling protocol overhead of these legacy technologies.

How It Works

As its name signifies, MPLS uses labels (sometimes called tags) to specify routes and Quality of Service (QoS) priority within the MPLS mesh. The routes themselves are based on QoS requirements of the traffic and bandwidth availability. This is in contrast to standard IP routing protocols, which most commonly use the Open Shortest Path First (OSPF) algorithm to build and maintain routing tables between sources and destinations.

When entering the MPLS mesh through a Labeling Edge Router (LER), the LER adds one or more labels to the packet that specify its path through the mesh. The labels are typically inserted between the Layer 2 and Layer 3 headers, which is why MPLS is sometimes referred to as a "Layer 2.5" protocol.

This label-based approach to routing has two main advantages over traditional IP routing:

The first benefit is faster, more scalable routing. Rather than each router having to examine the IP layer to determine the next hop, the path need only be assigned once upon entry into the mesh. This means less processing along the path, because each router is given the next hop rather than having to calculate it or look it up from a table. This can speed up routing considerably, and this architecture remains robust as traffic increases and more network infrastructure is deployed.

This single-point path assignment is also much easier to control than a route that can change from hop to hop. You can design a network to assign traffic priority based on point-of-entry into the network by port or by router, for example.

Insuring the MPLS Value Proposition

MPLS isn't right for every organization or every link. Before issuing an RFP for MPLS deployment there are some questions to answer about your network and the business processes that depend on it. Even after determining that MPLS is right for your network or for a subset of critical links, there is still a need to monitor the behavior of the MPLS mesh. A commercial-strength network analysis tool is key.

Pre-Deployment Analysis and Benchmarking

When assessing the benefits of MPLS for your enterprise, you should answer the following questions:

- **How dispersed is your network?**
  If your enterprise has a central office and a few branches, the MPLS value proposition (i.e., route efficiency and traffic shaping capability) is less compelling. MPLS is designed to manage dispersed traffic, such as many spread- out clients depending on multiple application services that are also dispersed.

- **What protocols consume the most bandwidth?**
  You may think you know, but the only way to verify is to look at the bits on the wire with a network analyzer.

- **Which of the more critical links are approaching bandwidth saturation?**
  Again, a network analyzer is the only tool that can give you an accurate answer. You may also discover that bandwidth is being consumed by misconfigured, chatty devices or inappropriate network usage.

- **What level of convergence has your organization reached,or is it planning to deploy?**
  Adding voice and video to already stressed networks can cause existing services to suffer, and not deliver the necessary quality of service for the new bandwidth- hungry applications.

Most of these questions should be easy to answer if you are actively managing your network using tools powerful enough to monitor the enterprise: commercial-strength network analysis appliances capable of full-duplex capture and analysis.

Ongoing Monitoring Requirements

After MPLS deployment, consider how you are going to maintain visibility. Depending on how the deployment is being managed, there are two scenarios:
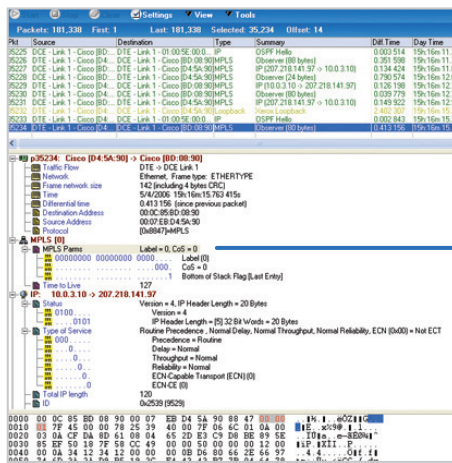
- If you are deploying MPLS in-house as part of your enterprise network strategy, you will be able to see and manipulate the tags. In fact, such visibility is required to verify that the MPLS mesh is working as designed.

- If the deployment is service-based (the MPLS mesh routers reside at a 3rd party carrier site), you may or may not have access to MPLS tags, and routing issues (beyond the application performance you can measure) will perhaps be made invisible to you.

In either of these scenarios, the need for sophisticated network monitoring tools remains undiminished.

Monitoring In-House/Enterprise MPLS Deployments

When deploying MPLS in-house, your monitoring tools should be able to decode, display, and aggregate reports based on MPLS labels. This capability is invaluable in verifying that the MPLS mesh is working as planned. You can't manage router behavior that you can't see.

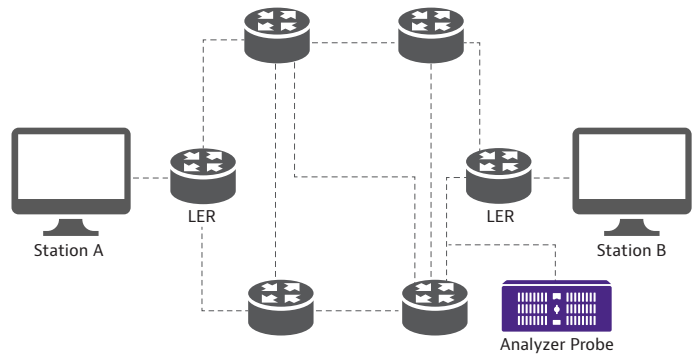

MPLS label between MAC and IP headers

Protocols sorted by MPLS "Class of Service" (CoS)

Without this capability, the MPLS labels are invisible to local network engineers, making it difficult to diagnose and solve problems in the mesh such as failing or misconfigured MPLS routers, or unexpected behavior from a labeling scheme that is working as it was designed.

Probe Placement for In-House/Enterprise MPLS Networks

Placing a full-duplex analyzer probe between the edge router and the MPLS mesh will allow your MPLS-aware analyzer to see the behavior of the mesh (how packets are labeled and how individual MPLS routers are manipulating the labels). Because MPLS labels are stripped from packets before being passed to the local network, you will not be able to see them by tapping or mirroring local switch traffic.

Only a dedicated MPLS-aware analyzer that is compatible with the MPLS media can provide insight into the health of the MPLS mesh. The Observer® Performance Management Platform provides all the tools you will need to monitor your local networks and MPLS routers, in a flexible architecture that is both affordable and scalable.
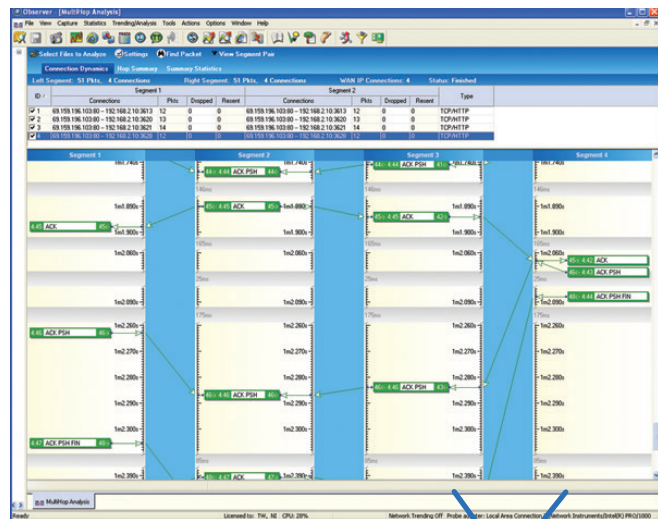
Monitoring 3rd Party/Service-Based MPLS Networks

Because service providers usually strip MPLS labels from packets before routing them to customer networks, a network analyzer deployed at the customer site won't be able to "see" MPLS behavior directly. This is less of a problem than it may appear. While decoding MPLS tags can be interesting, it isn't really necessary to see that level of detail unless you are managing the MPLS routers yourself (see the next section). Assuming that your network analyzer has the right set of features, you can monitor MPLS performance indirectly by looking at application performance and local network performance in detail.

When tasked with maintaining service delivery across networks both inside and outside the enterprise, the network analyzer should be capable of isolating and reporting on all sources of delay and latency: local networks, problems with the carrier, and how much delay is generated by the applications themselves. Application analysis and connection dynamics displays, for example, can let you easily identify delay problems and determine whether they are caused by the application, the local network, or the MPLS mesh.

In this screenshot (from Observer MultiHop Analysis), the connection between segments 3 and 4 is via MPLS through a service provider. This analysis shows excessive delay between these segments, which should be investigated further to ensure that the service provider is meeting the performance requirements of the SLA.
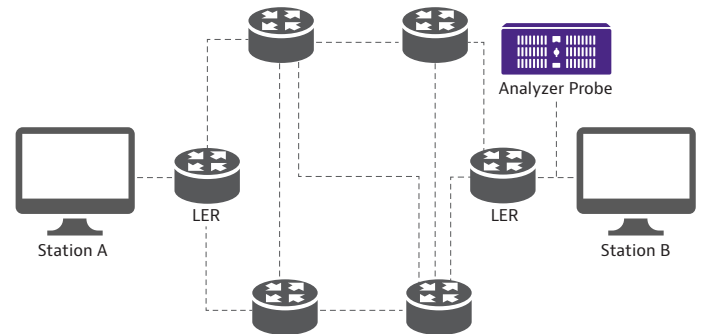
Without such detailed analysis, it is impossible to keep the carrier honest. This makes it difficult to accurately diagnose and solve local network and application problems.

MPLS portion of route

Probe Placement When Monitoring 3rd Party/Service-Based MPLS Networks

Placing a full-duplex probe at all points of ingress/egress to the MPLS mesh will give you enough visibility to isolate problems with the MPLS mesh that require resolution from the carrier.

Conclusion

As voice, video, and data converge on your network, deploying MPLS routers can help guarantee adequate bandwidth to each of these applications. But to truly ensure quality of service, you must understand your network, whether the MPLS is directly under your control, or under that of a contracted service provider. Both scenarios require sophisticated network analysis tools to isolate problems to specific parts of the infrastructure. If deploying MPLS in-house, an analyzer that can see and decode MPLS labels is essential to successful deployment and maintenance.