

Migrating to MPLS-based networks: *Avoiding the mistakes your peers have made*

Over the past several years, few topics have gained as much attention as Multi-Protocol Label Switching (MPLS). MPLS-based networks have been received as the new industry-leading transport technology for enterprises across the world. Heralded as the next big thing, MPLS-based transport penetration has been increasing substantially as organizations begin the migration from existing frame relay, ATM or private line (point-to-point circuits) networks. While MPLS-based networks have many great features, there are also new pitfalls that can occur with Class of Service and IP-based connectivity. This white paper will focus on how to avoid potential serious issues when you deploy an MPLS-based solution.

[Table of contents](#)

Overview	2
MPLS-based networks: what changes?	2
Why MPLS adoption has been substantial . 2	
What is a connectionless connection?	3
Prioritization can actually make things worse	3
It still exists even if you don't see it.	4
Multiple classes should mean different performance.	4
Do not exceed carrier thresholds	4
Best practices in managing MPLS-based networks.	4
Retail enterprise example	6
Leverage the benefits – minimize the risks	6
About Fluke Networks.	7

Overview

With the rapid adoption of MPLS-based networks, many organizations on the bleeding edge found major new challenges compared to traditional packet-based transport. MPLS-based networks promise improved performance with class of service-(CoS) based prioritization and enhanced flexibility with any-to-any connectivity.

However, organizations that were not prepared for the migration have actually seen performance degrade, sometimes substantially, even though the enhanced features of MPLS-based networking can, and should, improve overall performance. The negative impacts are caused by trying to leverage the improved functionality without a complete understanding of how the changes and CoS prioritization affect applications and network performance.

While other enterprises have endured pain and difficulty migrating to MPLS-based networks, the good news is your organization can learn from the mistakes of others. With proper planning and visibility, you can take advantage of the new feature set and improve overall network and application performance management.

MPLS-based networks: what changes?

For organizations with a current wide-area network (WAN), it is highly probable it includes or is exclusively based on frame relay or ATM. In the early 1990s, most networks were private line (or point-to-point), meaning a physical circuit had to be provisioned between locations to communicate. If a headquarters location needed to communicate with 10 other locations, the location needed 10 separate private lines.

In the mid-1990s, the adoption of frame relay soared, and ATM followed a few years later. With frame relay and ATM, the big difference was a “logical” connection for direct communications between locations. Now headquarters could communicate with 10 remote locations over a single physical connection to the carrier’s “cloud.” Logical connections would allow communications between locations. In the frame relay world, these were called permanent virtual circuits; ATM connections were called virtual circuits. This greatly reduced communication costs.

With MPLS-based networks, also commonly referred to as private IP VPNs, the connections change from virtual circuits to IP subnet-based connectivity. Instead of having a virtual circuit between locations, the carrier’s core switches or routers use MPLS to create a private IP network. This network provides any-to-any connectivity based on IP subnetting. The benefits, and new challenges, of IP subnet connectivity will be discussed in more detail later in this article.

In addition, MPLS-based networks add a Class of Service (CoS) feature that allows organizations to choose and prioritize the most business-critical or time-sensitive applications. CoS has great potential, but also creates new challenges in monitoring and managing multiple classes of service across an enterprise.

Why MPLS adoption has been substantial

When organizations switched from private line to frame relay or ATM networks, the primary driver was reducing transport cost – sometimes by more than 50%. With MPLS and private IP VPNs, there may be a hard dollar cost savings, but more than likely, the savings also include new benefits such as disaster recovery, application prioritization, reduced complexity, and any-to-any connectivity.

For disaster recovery, enterprises require multiple connections between locations in case of down or severely degraded circuits. In a frame or ATM-based world, this is possible by provisioning additional virtual circuits. While this does provide redundancy, it also adds a great deal of cost and complexity. With private IP networks, the network automatically provides any-to-any connectivity that makes a disaster recovery implementation much easier and cost effective.

With the CoS capability, organizations can let the service provider's core switches/routers do the "heavy lifting" of prioritizing applications, rather than relying on individual hardware-based shapers at each location. This allows the IT organizations to focus resources on the most critical or time-sensitive application.

With the elimination of the multiple virtual circuits, the complexity of day-to-day management and monitoring are greatly reduced. Removing partially or fully meshed frame relay architecture greatly reduces the workload for the IT staff when changes or additions are required. With the number one cause of downtime being human error, any opportunity to reduce the number of touches limits potential negative impacts.

For enterprises with distributed applications, a traditional hub-and-spoke network can compound existing problems. Every request from every remote location must go through the main site. This also increases the risk of a single point of failure. With an MPLS-based network, remote locations can communicate directly to each other, which minimizes the additional delay of going to the main location and the burden of all traffic hitting a central site.

What is a connectionless connection?

For IT and networking personnel who have been, managing WANs for years or decades, it took a while to go from private lines to the DLCI-to-DLCI connections of frame relay. Even though the circuits are virtual, they follow the same permanent path between locations, so there is a comfort associated with knowing each and every virtual circuit.

The "connectionless connection" of IP subnets makes it difficult for unprepared organizations to monitor, manage and troubleshoot performance across multiple connections. Since the data follows the best available path between locations based on the IP addressing, understanding what is causing performance impacts becomes much more challenging with any-to-any connectivity.

Prioritization can actually make things worse

Will prioritization improve network and application performance?

Most IT professionals would answer "yes." It makes intuitive sense that setting priority for critical applications would improve their performance. In a general sense, this is correct. However, with MPLS-based networking, prioritization can actually cause adverse effects because of CoS.

For most service providers, the customer purchases an MPLS-based circuit and with each circuit, the carrier typically breaks the bandwidth into three to five different classes of service. For example, a T-1 circuit with a specific carrier may receive 700 Kbps of gold traffic, 500 Kbps of silver traffic and the rest bronze.

As long as the enterprise stays below the threshold for the highest CoS setting, the prioritization should improve performance. However, the challenge and negative impacts can occur when usage exceeds the threshold on the highest, or real-time, class of service.

If a customer exceeds the threshold for the highest priority traffic, the service provider usually does one of two things. The provider either discards the packets above the threshold, or sets them at a lower priority level. For the enterprise, both of these scenarios are negative because the highest priority traffic may have been discarded or set to a lower priority level which can negatively impact performance for business-critical or time-sensitive applications.

This is where most customers encounter problems. Some enterprises have actually seen worse performance with prioritization than they did with the “first in, first out” method of many best effort networks. The good news is with proper visibility, enterprises can make the correct decisions to leverage the benefits of IP-based connectivity and CoS prioritization.

It still exists even if you don't see it

With the any-to-any and connectionless connection issues discussed earlier, managing and troubleshooting remote locations can become a greater challenge for enterprises. Historically, most IT groups are centrally located at the headquarters or data center, or at a few critical locations, because the vast majority of all traffic must flow between these locations. For remote offices or branches, there is limited IT support and resources.

Suddenly, if remote locations can communicate directly because of any-to-any connectivity, IT organizations could be completely blind with little or no visibility into what is happening between those locations. They do not have the expertise or tools to identify and pinpoint the cause when problems occur.

Multiple classes should mean different performance

Since the carrier is providing between three to five different classes of service based on prioritization, it is correct to assume the service level performance should vary between the highest and the lowest priority.

Many enterprises that have deployed a private IP network lack the visibility to see exactly what the performance delta is between multiple classes. Most organizations rely on a service level report from their vendor to measure performance. This approach can skew the data by aggregating every location for every hour for an entire month. This does not help pinpoint if the service level performance of the carrier is impacting real-time application such as VoIP.

Do not exceed carrier thresholds

For most enterprises that have already had negative impacts on performance with CoS, the most common cause was exceeding the carrier thresholds. As discussed early, when exceeding the highest priority class threshold, the packet may be discarded or set to a lower class. Both of these are very bad for most enterprises.

Adding to the challenge for most IT groups is a limited understanding of usage by application. It can be difficult enough to have a granular view of usage by individual application, but with CoS, the problem is compounded. To make the job even harder, many organizations run multiple applications on a single class of service setting.

For example, an enterprise may put voice, video, SAP and two custom applications all on the highest priority class setting. Instead of having to understand just one bursty application, the IT staff must understand what happens when combining five bursty applications on a single location. An abnormal spike in SAP could cause voice packets to be dropped which negatively impacts call performance. The increased challenge for most organizations is the dynamic nature of applications, usage and performance.

Best practices in managing MPLS-based networks

The key to implementing a best practice in migrating to an MPLS-based network is tied closely to granular visibility. A solid approach to implementing a private IP network deployment requires granular visibility to baseline, deploy, manage, troubleshoot and optimize performance.

For enterprises with an existing WAN, baselining the performance before the deployment of a private IP network is critical. It is critical to understand what is happening with the applications on the network before any changes are made. If the organization does not understand performance before deploying MPLS, it will be much harder, more expensive and more time consuming to pinpoint the performance issues between the legacy infrastructure and the migration to MPLS.

If the IT organization understands what is occurring today, the next step should be a slow deployment to MPLS-based networking. With a slow transition, the staff can use the previous baseline to verify the starting point and monitor any changes afterward.

When it comes to ongoing management, it is extremely critical for the IT staff to understand both the IP subnet-based connectivity as well as the CoS prioritization and usage. In order to properly troubleshoot potential issues between multiple locations, it is imperative to have visibility between the locations.

Once an organization is comfortable identifying and viewing performance on IP-based connectivity, the class of service is the next key to implementing MPLS successfully. In order to properly prioritize applications with CoS, there are several sequential steps the IT staff should take: 1) inventory all applications, 2) understand individual application usage, 3) determine priority, 4) monitor usage based on class, and 5) optimize settings.

1) Inventory all applications

Every organization should know each and every application on the network, but most IT staffs have knowledge of only about 40 to 60% of their applications. Without an accurate understanding of all applications on the network, it is virtually impossible to successfully implement CoS.

2) Understand individual application usage

The second component is understanding the usage of individual applications including average, minimum and maximum. It is important to understand the bursty nature of individual usage. If an application is truly critical, most IT staff will base the decision on the maximum usage to avoid unnecessary downtime.

3) Determine priority

The biggest challenge for many IT organizations is determining which priority each application should receive. What makes this so difficult is virtually every user will deem their application the most critical. The IT organization should take into account the business-criticality as well as the time-sensitiveness of each application. For example, a custom application may be the most business-critical, but really is not delay sensitive. Therefore, a voice or video application may be placed on a higher priority based on its time-sensitivity while the most critical business application may be placed a tier lower. This is counter-intuitive for many IT professionals at first.

4) Monitor usage based on class

Monitoring usage and performance by application and class of service, or more correctly, the inability to monitor by application and class of service, is likely the number one cause of MPLS performance issues. As discussed earlier, it can be challenging to understand the bursty nature of a single application, let alone trying to group five different applications in a single class of service and then monitor usage and performance every second, real-time, to ensure you do not exceed the carrier thresholds.

5) Optimize settings

If there is a performance issue for critical applications, enterprises typically have two choices for improvement. Additional bandwidth may be added to handle excessive utilization, but this adds cost for every upgraded circuit or location. The second choice is to fine-tune which applications receive each CoS setting. If a particular location is exceeding the threshold with five applications on the highest priority, the staff could change the number of highest priority applications to two or three to stay below the threshold.

The key for either decision is having the very granular visibility. Without a granular view, most IT staffs guess at what is best. However, if the organization has a solid understanding of usage and performance of individual applications, classes and locations, it can make the best decision for the organization, whether it is adding bandwidth, reallocating applications or taking a different approach.

Finally, the best practice should include a continual monitoring and managing process. A one-time snapshot or change is not enough for complex networks. The usage, applications, users and locations tend to be very dynamic. Ideally, the changes made during the initial optimization should be much greater than the fine-tuning that should occur months or years after deployment.

Retail enterprise example

A real-world example focuses on a retail organization, where remote stores are connected for inventory and logistic requirements. A customer wants to buy a particular item, but it is out of stock at one store. With a custom application, the store can check any other store in a 25-mile radius for availability. Having any-to-any connectivity for this critical application would be beneficial since the locations are pulling information from the other branches, not the headquarters. These requirements could be met with a private IP network.

One day, a local store is out of a particular item during a busy time. While trying to use the application to see if another store has the item, the application is extremely slow and unresponsive. Now that customer is forced to wait longer, which impacts their customer satisfaction as well as every other person in line. During a critical holiday season, most retailers cannot risk losing sales or aggravating customers.

The IT manager sitting at corporate headquarters receives a ticket and starts troubleshooting. However, since the application is not coming through the headquarters location, the manager has no visibility. At this point, most organizations would have to dispatch a technician to solve this problem. In addition, if the problem is tied to CoS thresholds, it becomes virtually impossible to fix the problem quickly. The mean time to repair in this scenario could be hours or even days. Depending on the organization, there could be a high risk to lost revenue and reduced customer satisfaction.

If this retail organization followed the best practices, the IT manager would have immediate visibility into each store, with the ability to pinpoint any problem. With granular visibility, the manager could make the control decisions to fix the problem. Maybe there was an excessive increase in another application usage, which was impacting the custom inventory application. The manager could quickly make the configuration changes to fix this problem. Visibility is key to identifying, isolating and resolving any outage or degradation.

Leverage the benefits – minimize the risks

There are several key reasons why MPLS-based networks have been gaining in popularity as organizations revisit their network architecture. With any-to-any connectivity and CoS offerings, there can be substantial cost savings and improved productivity with a successful deployment of private IP networking.

To reap these benefits, organizations must understand how MPLS-based networks are implemented. With granular visibility during and after the deployment, enterprises will greatly reduce the risk of reduced performance and greatly increase the likelihood of success. The key is understanding what views are needed and following the best practices during implementation so your enterprise can avoid the mistakes other have made.

Fluke Networks has the industry-leading solution which enables enterprises to leverage the benefits of MPLS and minimize the risk. With Visual Performance Manager, enterprises that deploy MPLS-based networks can monitor end-to-end connectivity across every location in the network. The solution also has the capability to auto-discover applications network wide so users can properly assign CoS settings for each and every application. With up to one-second granularity, Visual Performance Manager monitors individual CoS performance including service level metrics to insure performance meets or exceeds the requirements of the business.

The key to leveraging the benefits of MPLS-based networks is to have the visibility to understand the changes in the architecture and performance. Visual Performance Manager provides the critical visibility to optimize the benefits of MPLS-based networks.

Fluke Networks: Strong partners, superior performance.

Our history of innovation, product quality, and customer service began in 1948. Today, Fluke Networks is part of Danaher Corporation, a growing Fortune 500 company and leading manufacturer of professional instrumentation, industrial technologies, tools and components with revenues of more than \$9 billion (USD) annually.

Our technology offerings are used by major carriers including AT&T, Global Crossing, Sprint, Verizon Business and others to run their managed services. Our global reach of sales offices, laboratories, factories, and home and retail environments spans six continents and more than 50 countries and gives customers the peace of mind that they made the right choice in partnering with Fluke Networks for all of their Enterprise Performance Management needs.

Contact Fluke Networks: Phone 800-283-5853 (US/Canada) or 425-446-4519 (other locations). **Email: info@flukenetworks.com**.

NETWORK SUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to www.flukenetworks.com/contact.

©2007 Fluke Corporation. All rights reserved.
Printed in U.S.A. 12/2007 2821099 A-ENG-N Rev B