Key Considerations for MPLS IP-VPN Success
Key Considerations for MPLS IP-VPN Success

Contents

Abstract  2
Introduction  3
Types of IP VPNs  4
Why Migrate to MPLS-based Private IP VPN?  6
  Class of Service (CoS)  6
  Automatic Redundancy/Disaster Recovery  7
  Fully Meshed Infrastructure  8
  Reduced Complexity  8
Key considerations for an MPLS migration  9
  Prioritizing Applications  9
  Verifying CoS Settings  10
  Managing CoS Thresholds  11
  Measuring Service Level Agreements  12
  Optimizing Bandwidth Requirements  12
  Managing the Network Migration  13
Network Visibility for MPLS IP-VPN Migrations  14
Conclusion  15
Abstract

There are a number of drivers behind the growth of MPLS IP VPN networks, and its benefits are already being realized by many enterprises. In addition to maximizing performance while minimizing costs, MPLS VPNs offer the ability to prioritize applications such as VoIP by class of service (CoS), create and improve disaster recovery infrastructures, utilize a fully meshed infrastructure that replaces outdated hub and spoke architecture, and reduce complexity to simplify network management in an increasingly complex landscape.

When considering a migration to MPLS VPN, there are several key considerations that can significantly impact the process of planning, implementing and managing the network, as MPLS has some unique requirements and tasks associated with managing and administering the network. This white paper will explore some of those considerations and discuss how they can be addressed.

Introduction

The benefits of MPLS VPNs are being realized across a wide market, and have been for a few years. Based on IDC survey data, 30% of all ports were IP VPN, which is several percentage points above legacy private line, the second-largest segment. In MPLS IP VPN services, market revenue is expected to nearly double from $5,523.2 million to $10,784.4 million in the span from 2009-2014.

In addition to maximizing performance while minimizing costs, MPLS VPNs offer the ability to prioritize applications such as VoIP by class of service (CoS), create and improve disaster recovery infrastructures, rely on a fully meshed infrastructure that replaces outdated hub and spoke architecture, and reduce complexity to simplify network management in an increasingly complex landscape.

When considering a migration to MPLS VPN, there are several key considerations that can significantly impact the process of planning, implementing and managing the network, as MPLS has some unique requirements and tasks associated with managing and administering the network.

---

Types of IP VPNs

An abundance of IP VPN ‘flavors’ can make it difficult to sort through service provider offerings and technologies. In general, private IP VPNs can be categorized as CPE-based or network-based.

CPE-based IP VPN

A CPE-based VPN uses the public Internet as the core backbone. Enterprises may use dedicated Internet connectivity, cable, wireless, DSL, satellite, and dial-up as different means to connect. Enterprises then typically use CPE (VPN gateway, router, etc.) to create a VPN, with tunnels and encryption, allowing remote sites to communicate directly and securely with headquarters and other remote sites.

The primary benefit for site-to-site IP VPNs is tied to low cost and ubiquity. Traditionally, Internet connectivity is less expensive than frame relay or ATM—and the difference grows substantially when connecting international locations. Ubiquitous Internet connectivity is a major benefit, as IP is IP, whether it is dial-up, dedicated, domestic, or international.

While there are cost savings associated with site-to-site IP VPNs, the total cost of ownership can be higher. CPE is needed at every site to create the VPN. The potential exposure of using the public Internet for business-critical traffic is extremely high. And Internet architecture was not designed with business-grade applications and requirements in mind, nor it does not offer strong SLAs for the enterprise.

MPLS-based Private IP VPNs

Private IP VPNs, often MPLS-based, use a service provider’s private infrastructure—occasionally Frame Relay and ATM and more frequently, Ethernet—as the backbone of the VPN. MPLS is a solution that allows the provider’s core routers to transition from layer 2- to layer 3-based connectivity.

In a private, IP-enabled transport network the carrier’s routers use MPLS to communicate between locations in the network via IP addressing, not limited to individual permanent virtual circuits (PVCs). Tunneling and encryption are generally not required for the enterprise because the network is on the private carrier’s backbone, not the public Internet. Additionally, the carrier’s core routers create the VPN, not the enterprise’s customer premise equipment (CPE).
Traditional Network vs. IP Enabled Network

In a traditional Frame Relay network, a dedicated permanent virtual circuit (PVC) is required for communication between remote sites. The traffic follows the path for every transaction between two sites.

In an IP enabled network, the service provider’s routers use MPLS routing to communicate between locations in the network via IP addressing (not limited by individual PVCs).

Comparing CPE and Network VPNs

<table>
<thead>
<tr>
<th>CPE-based IP VPN (Public Internet VPN)</th>
<th>Network-based VPN (MPLS-based IP VPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Public Internet as core backbone</td>
<td>• Service provider’s offering as core backbone (Frame Relay, ATM, Ethernet)</td>
</tr>
<tr>
<td>• Access via dedicated Internet connectivity, cable, wireless, DSL, satellite, dial-up</td>
<td>• MPLS allows the service provider’s core routers to transition from layer 2 to layer 3-based connectivity.</td>
</tr>
<tr>
<td>• CPE (VPN gateway, router, etc.) creates a VPN with tunnels and encryption</td>
<td>• Security inherent in private infrastructure</td>
</tr>
<tr>
<td>• Low cost, ubiquitous access</td>
<td>• Carrier’s core routers create the VPN.</td>
</tr>
<tr>
<td>• CPE required at every site can result in higher TCO and high complexity</td>
<td>• Reduced complexity</td>
</tr>
<tr>
<td>• High potential exposure in using public Internet for business traffic</td>
<td>• Class of Service (CoS) used to prioritize traffic</td>
</tr>
<tr>
<td>• Internet architecture not designed to support business-grade applications</td>
<td>• Automatic redundancy/disaster recovery</td>
</tr>
<tr>
<td>• No strong SLAs</td>
<td>• Fully meshed infrastructure</td>
</tr>
</tbody>
</table>
Why Migrate to MPLS-based Private IP VPN?

The desire to move toward a more cost-effective network that supports voice, video and data is among the primary drivers behind the move to MPLS VPN services, with a number of other technological and financial drivers drawing enterprises in that direction as well. Among these are:

- Class of Service (CoS): provides ability to prioritize applications, such as VoIP
- Automatic redundancy/disaster recovery: create and improve disaster recovery infrastructures
- Fully meshed infrastructure: replace outdated hub-and-spoke architectures
- Reduced complexity: one network platform supports all application traffic—including VoIP and data applications

A key advantage worth noting for businesses migrating from Frame Relay and ATM to private IP is that, for most service providers, there is no need to provision new circuits, Frame Relay and ATM is still Layer 2 access—and routers may not need to be replaced.

Class of Service (CoS)

The ability to prioritize applications by Class of Service (CoS) has been a key driver for many enterprises in rolling out private IP networks. Instead of using critical router resources to shape traffic or buying an expensive traffic shaper to prioritize applications, the service provider’s core routers do the heavy lifting in prioritizing different classes of service in private IP networks.

To execute CoS, an enterprise must identify its most business-critical or delay sensitive applications, and then assigns priorities through CoS settings. Service providers frequently offer three to six classes of service, with naming conventions that vary depending upon the provider. The CoS setting assigned to an application dictate its priority in traveling the network. For each class of service, the service provider specifies a bandwidth threshold, or maximum, depending on total circuit size, number of classes and contract agreement.

In one enterprise, VoIP and Oracle might be the most business-critical applications set for the highest priority, with e-mail and Web browsing receiving lower assignments. The customer configures its router to tag the correct class in the IP header—DiffServ or TOS bit settings—and pass the data to the service provider’s edge router. The provider’s router looks at the IP header for the class setting and polices the traffic. The policing from the source site—or ingress—ensures the threshold of bandwidth is not exceeded for each class setting. The core router then sends the traffic across the network with prioritization.

At the destination location—or egress— the provider’s router queues the prioritized traffic from each site and delivers the highest priority first. With the capability of CoS, a prioritization schedule can easily be implemented across the enterprise so the most mission-critical applications receive the highest priority.
Automatic Redundancy/Disaster Recovery

The demand for infrastructure redundancy has grown as more enterprises drive revenue, reduce costs, or provide services based on applications on the WAN. If a credit card authorization site is down, a retail enterprise may lose sales because today’s consumers carry less cash. If a manufacturing company cannot transmit its stocking order to a plant, the vendor might impose penalties. These two examples are common scenarios that are exacerbated when there is a single point of failure in the infrastructure.

That does not always mean the network itself is the cause of the problem; it can be any portion of the infrastructure that does not allow the business transaction.

If a transaction cannot be completed at the primary location, enterprises can forward it to a back-up location for completion. In a Frame Relay or ATM environment, this is typically handled by provisioning additional PVCs between critical sites. While this architecture is viable, it can be extremely expensive, depending on the size and scope of the network. Managing tens or hundreds of PVCs at multiple sites can be a logistical and managerial nightmare—especially at remote locations with no networking support staff. Enterprises must determine if the exposure to lost revenues and incurred costs exceeds the extra resources and complexity for a disaster recovery infrastructure.

A private IP network is fully redundant, based on its Layer 3 connectivity—IP subnet-to-IP subnet. With each site in the network given access to every other site, implementing a disaster recovery/back-up strategy is much easier and more cost-effective since dedicated PVCs are no longer needed at each location.

---

Bandwidth: Frame Relay CIR versus private IP CoS

- In Frame Relay, two criteria govern bandwidth: port size and committed information rate (CIR). In private IP, the criteria are Committed Access Rate (CAR) and thresholds by class of service (CoS).

- Port size in Frame Relay and CAR in private IP are similar, dictating maximum bandwidth allowance for a single circuit/location.

- The differences lie between Frame Relay CIR and private IP CoS. In Frame Relay, enterprises purchase CIR per PVC as a way to guarantee bandwidth from the service provider. In Private IP VPNs, a CoS capability lets the enterprise specify classes of prioritization, each a percentage of CAR. CoS is more application-focused than CIR, since enterprises can select which applications are the most critical or delay-sensitive and assign them the highest priority. The network-based VPN policies and queues the classes instead of deploying traffic shapers to prioritize the traffic.
**Fully Meshed Infrastructure**

In a hub-and-spoke environment, traffic from a remote site must traverse a host location before it is routed to the destination address. As Web-based applications or time-sensitive applications like VoIP become more prevalent, the hub-and-spoke architecture becomes more stressed.

A fully meshed architecture—where every site can communicate directly with any other site without first having to run through a hub/host location—has two key benefits for most enterprises: improved site-to-site performance and fewer burdens on host locations.

When an application such as VoIP is used between two remote sales offices, there is no benefit to “home-running” the application back to the host location, a scenario that adds extra steps and distance to complete the application transaction. With a fully meshed network, a VoIP call between two offices in London will flow directly between the locations, instead of routing through a hub site in Los Angeles. In a private IP network, the steps and physical distance alone can be greatly reduced.

In conjunction with improving parameters with a fully meshed network—including delay or jitter—reducing host site bandwidth usage is also a major benefit. If the organization no longer has to bring all traffic back to the host site, bandwidth requirements at a host location could be greatly reduced, performance across the entire infrastructure could be enhanced.

**Reduced Complexity**

The complexity of managing a frame relay or ATM network grows exponentially with network size and the number of virtual circuits. Managing hundreds of sites and thousands of PVCs is a daunting task for many enterprises just to handle moves, adds, and changes on a daily basis.

As discussed earlier, IP subnet addressing is used to connect every site in the network. PVCs no longer provide the connection between sites. Instead of managing a port for every site and tens, hundreds, or thousands of individual PVCs, the private IP network has a single port for each site and then uses IP addressing to connect to every other site. This architecture is much less complex, meaning it is easier to administer and allows enterprises to focus limited resources on more important activities.
Key considerations for an MPLS migration

Migrating to private IP VPN offers a host of benefits, but the process deserves some up-front planning and forethought before taking the dive. The enterprise will have some new tasks and methodologies to grapple with, and gaining an understanding of these and planning for them can help glean the full benefit of all that MPLS has to offer—convergence, performance, cost-efficiencies, security and privacy—as well as smooth the way for implementation and managing the new network in the future.

Among these considerations are:

• Prioritizing Applications
• Verify CoS Settings
• Managing CoS Thresholds
• Managing SLAs
• Optimizing Bandwidth Requirements
• Managing the Network Migration

Prioritizing Applications

Identifying top business-critical applications is the first step in the CoS process. This determination can be easy enough—through management’s input, trial and error, or simply observing which application generates the most complaints when there are performance issues. But beyond the top few critical applications, many enterprises have a difficult time categorizing those with medium to low importance. Often compounding the problem is a lack of visibility into the network—it’s impossible to prioritize applications if you don’t know what’s there.

A related challenge for network managers is the addition of new, powerful applications to an existing MPLS network. If an enterprise decides to implement Oracle or SAP in the next six months, it is important to consider what the impact will be of the new high-priority application on the existing high-priority applications. Networks and applications are continuously evolving and changing, and CoS settings will need to be tuned to ensure the continued performance of applications.

Application performance management tools can help in two critical aspects of prioritization: determining what applications are on the network, and, after CoS assignments are made, whether applications are prioritized correctly. Tools that auto-discover applications across an entire infrastructure can provide knowledge of total application usage and allow for a more complete assignment of CoS settings.
Verifying CoS Settings

After all applications across the network are prioritized and each IP header configuration is set, an application performance management tool can help verify that all settings were made correctly.

Throughput by Protocol (kbps)

Network managers must take steps to ensure that applications are assigned correctly. Oracle, Routing, and Web are shown in this graph as having the highest settings. Web traffic, which should be classified as a low priority, was misclassified as high priority and is using up valuable resources needed by mission-critical applications.

Two Common Pitfalls in the CoS Process

There are two common pitfalls in the CoS process: setting the IP header configurations incorrectly, and placing applications in the wrong class.

One enterprise without clear visibility into its network had classified VoIP as a critical application, one that should receive the highest class setting. However, as the network engineer was configuring the 80 sites, he made a simple mistake when setting the DiffServ for one location, and VoIP calls were impacted as a result. Without visibility into network, identifying the problem was extremely difficult. The team believed that VoIP was receiving the highest priority, so they ruled it out as a potential cause and began troubleshooting other parameters, including CPE.

After an application performance management tool was deployed, the network engineer was able to look at the site impacted by poor VoIP quality. It was clear that a significant amount of traffic was categorized as unknown. Using deep-packet inspection and the traffic capture feature, the misconfigured application was identified in minutes.

Usage is measured for each CoS setting, including unknown and misconfigured applications.
Managing CoS Thresholds

Managing CoS thresholds is a critical and ongoing process. MPLS IP VPN service providers may assign a bandwidth threshold, or maximum, to each class of service. Monitoring is critical to make sure that bandwidth thresholds set by the service provider are not exceeded, a situation that can significantly compromise mission-critical applications.

Because of the “bursty” nature of data traffic, an enterprise could be well below its allocation for the majority of the day, but exceed the threshold at peak times. If the network is congested, and the enterprise exceeds its highest priority class threshold, the traffic may drop to the lowest priority—or may be discarded altogether. Suddenly, the most mission-critical applications are most at risk.

Another risk comes from new application rollouts. When the new application is assigned a CoS, its can produce a domino effect in the network and impact other applications. For example, a new, custom financial application might push the highest priority class to exceed the threshold, causing another application in the same class to drop one class lower, and so on.

Application performance management tools can be used to monitor utilization for each individual CoS, and measure whether usage is above or below threshold allocations. Exceeding a threshold allocation requires the enterprise to either upgrade its circuit for additional bandwidth or move one or more applications to another CoS.

These and other considerations for managing CoS thresholds can be addressed with application performance management tools.

Determine if your actual usage is exceeding your policing threshold.
Measuring Service Level Agreements

To guarantee quality of service (QoS) and provide assurance that its network can handle a customer’s applications, contractually binding Service Level Agreements (SLAs) are often used.

From a service provider point of view, measuring SLAs often means delivering a monthly report with weighted averages across the entire infrastructure for delay, throughput, and availability. Private IP eliminates traditional virtual circuits, as well as layering on multiple classes of service.

Even before private IP, it was difficult for many enterprises to proactively monitor service level parameters from an end-to-end point of view. Now, with added complexity in the network, some enterprises find it extremely difficult to measure SLA parameters across IP subnets and by individual classes of service. This lack of visibility makes it more difficult to leverage the day-to-day benefits of SLAs.

Optimizing Bandwidth Requirements

Optimizing bandwidth is a critical for many enterprises. While enterprises need to ensure they have sufficient bandwidth to meet the needs of applications and end-users, over-provisioning every circuit in the network is not a viable solution from a cost perspective. At the same time, as application performance becomes more important, the enterprise must ensure sufficient bandwidth resources.

The cost of bandwidth alone is said to comprise as much as 60 to 70 percent of total networking budgets for some enterprises. With limited resources, optimizing bandwidth is a key step toward maximizing network and application performance. With the new Layer 3 connectivity—IP addressing—instead of Layer 2 connectivity—PVCs—utilization will change in a private IP environment.

Adding CoS capabilities also throws a new wrinkle into the equation. With the bursty nature of traffic, it is important to understand the impact of usage on a private IP environment.
Managing the Network Migration

In migrating from Frame Relay or ATM to private IP, organizations can leverage existing Layer 2 infrastructure and CPE. Despite this advantage, an enterprise shouldn’t expect to have 75 sites converted from Frame Relay to private IP overnight.

The network must be managed throughout the migration. During a private IP implementation, there will likely be a period of time where multiple technologies—such as Frame Relay, ATM and private IP—run over the network. With a mixed network, it is mandatory to maintain visibility into the performance of the network and applications. It will be difficult to manage the networks without visibility into the performance of both.

Ideally, enterprises would baseline performance based on existing technology and, as the migration progresses, IT staff would see the changes and impact of Layer 3 connectivity and CoS.

An application performance management tool can provide visibility into interworked environments so you can still see end-to-end, even if one site is Frame Relay and the other is private IP. It provides the ability to monitor PVCs in a frame relay environment or meet the challenge of managing IP-subnet pairs in a private IP network.
Network Visibility for MPLS IP-VPN Migrations

MPLS-based private IP networks offer a host of benefits for the enterprise that range from increased performance to reduced cost and complexity. In some case, it also changes the infrastructure that IT managers have administered for years.

A holistic application performance management tool, one that offers network and application performance management like XO Applications Performance Management, can facilitate the migration process and post-implementation management of the network.

XO Applications Performance Management is a suite of analytical tools to help businesses optimize the performance of their XO MPLS Wide Area Network (WAN) service, and all of the critical business applications that run over those networks including Voice over IP (VoIP). XO has one of the industry's most comprehensive, application-aware solutions for increasing applications and network performance.

XO Applications Performance Management can help with a number of assessment, implementation and deployment tasks involved in migrating to an MPLS IP VPN network.

Prioritizing Applications: Auto-discovery of applications across an infrastructure. Total application usage is provided for all applications across the network. Once the applications are prioritized, the tools can be used to determine if CoS settings for each are properly configured.

Manage Class of Service Thresholds: Monitors utilization for each individual CoS to determine whether usage is above or below the threshold allocated by the service provider. Additional considerations for managing CoS thresholds are all readily addressed with XO Applications Performance Management.

Measuring SLAs: XO Applications Performance Management is a leader in SLA verification, providing independent analysis and measurements from an end-to-end perspective. Provides up-to-the-minute views of service level parameters—including availability, delay, and throughput—critical for isolating the cause of performance issues. And, no waiting for a monthly report.

Optimizing Bandwidth Requirements: The Burst Advisor in XO Applications Performance Management measures actual usages in one-second increments so that circuits can be sized properly. Armed with this information, an enterprise networking team has the information it needs to optimize the network and right-size bandwidth by increasing bandwidth for critical locations or moving bandwidth from less-utilized sites to over-utilized sites.
Managing Network Migration: XO Applications Performance Management offers a unique opportunity to manage the transition to private IP. With Frame Relay or ATM as a baseline, XO Application Performance Management provides a single platform to manage network application integrity as enterprises migrate to private IP. XO Application Performance Management offers end-to-end performance visibility for interworked environments, where one site is Frame Relay and the other is private IP. Now, the enterprise can monitor PVCs in a Frame Relay environment, or tackle the harder challenge of managing IP-subnet pairs in a private IP network.

As the market migrates to MPLS VPNs to take advantage of the network’s ability to support traffic prioritization through class of service, there is a growing focus on network and application performance monitoring tools. Both these tools are critical for the success of MPLS VPN implementation as customers make the move to a converged architecture and demand more control over the applications they wish to run on the network. Frost & Sullivan

Conclusion

MPLS-based private IP networks offer a compelling proposition to today’s enterprise looking to simplify and reduce costs for its networks. Several key considerations are important in thinking about a migration in order to gain the full benefit that the network can provide and make the transition as smooth as possible.

Many enterprises are already taking advantage of the converged architecture, cost savings, and ability to support QoS—particularly for voice and video.

Although the key considerations must still be addressed, powerful application management and network management tools, like XO Applications Performance Management, can help migrate to MPLS IP VPN and manage that network into the future.

About XO Communications

XO Communications is a leading nationwide provider of advanced broadband communications services and solutions for businesses, enterprises, government, carriers and service providers. Its customers include more than half of the Fortune 500, in addition to leading cable companies, carriers, content providers and mobile network operators. Utilizing its unique combination of high-capacity nationwide and metro networks and broadband wireless capabilities, XO Communications offers customers a broad range of managed voice, data and IP services with proven performance, scalability and value in more than 85 metropolitan markets across the United States. For more information, visit www.xo.com.


For XO updates, follow us on: Twitter | Facebook | Linkedin | SlideShare | YouTube | Flickr