



# Best Effort gets Better with MPLS

Superior network flexibility and resiliency  
at a lower cost with support for voice, video  
and future applications



# Best Effort gets Better with MPLS

Superior network flexibility and resiliency at a lower cost with support for voice, video and future applications

---

## Executive Summary

Enterprises of all sizes are outsourcing their voice and data traffic to service providers who have the technology and expertise to deliver secure and reliable, high-performance IP communications. These top service providers leverage the routing flexibility, fast fault recovery and multiservice capabilities built into their Multiprotocol Label Switching (MPLS)-enabled Wide Area Networks (WANs) to benefit their small and medium-sized business (SMB) customers. As a result, SMBs worldwide can capitalize on the many advantages of using a converged IP network to support their voice and data applications. These enterprises are benefiting from reliable, cost-effective solutions that are easy to implement and backed by Quality of Service (QoS) guarantees.

## The Evolution of Wide Area Networking

All kinds of organizations rely on WANs to support instantaneous communications between their own locations and a wide variety of customers, suppliers and distributors. The vital role WANs play in supporting business activities means that WAN design must be driven by business need.

### Four key trends are driving the way organizations design their WAN infrastructures:

- **Pace of Business Change** – It is quite common for a company to make frequent changes to its set of suppliers and distributors, gain new customers, and add or change locations. As a result, the enterprise WAN needs to be extremely flexible and responsive to change.
- **Linkage to Business Goals** – The growing linkage between a robust network infrastructure and achieving business goals places new demands on the network for greater resiliency and scalability. Today's successful SMB now must communicate data of various types – inventory, sales, financial, etc. rapidly in order to remain competitive.
- **Network Convergence** – Businesses are consolidating a wide variety of technologies, protocols and traffic types (i.e. data, voice, and video) onto a single network infrastructure. Supporting a single converged infrastructure is notably less costly than supporting multiple networks. However, a converged network infrastructure does introduce some significant challenges. In particular, organizations that deploy a converged infrastructure must ensure that the network can effectively and efficiently meet the demands of disparate traffic types.

- Traffic Isolation - In the evolution of WAN design, enterprises are looking to isolate traffic based on the organization responsible for the traffic. The isolation of traffic serves two purposes — it increases security and network stability.

WANs based on traditional technologies have been too costly and difficult to establish and maintain for many SMBs. However, a new approach based on MPLS offers enterprises a simple and cost-effective path for evolving their network infrastructure in response to these trends.

### **MPLS Basics**

MPLS was designed to add a superset of key capabilities to the IP protocol, particularly around areas like network virtualization, resiliency, and traffic engineering. MPLS does this by separating the control and forwarding planes. At the edge of the network, this separation allows complex routing calculations based not only on Layer 3 (IP) information but also Layer 2 characteristics such as bandwidth, latency, and utilization. In the core, this separation simplifies switching and improves the IP packet exchange.

MPLS uses virtual circuits, known as Label Switched Paths (LSPs), to transport a wide variety of traffic across the IP network. These LSPs are established using signaling protocols, such as Label Distribution Protocol (LDP) or Resource Reservation Protocol with Traffic Engineering (RSVP-TE), based on possibly complex path constraints.

IP routing and forwarding occur in a normal fashion at the edge of the MPLS network, utilizing standard protocols and procedures. The IP routing protocols view the LSPs across the MPLS network as single-hop links the same way they would view ATM or Frame Relay virtual circuits. If needed, LSPs can be tunneled inside other LSPs to consolidate and simplify traffic engineering and to allow large-scale VPN services to scale within the core.

### **The Attraction for Service Providers**

The basic purpose of MPLS is not to replace IP routing, but to enhance IP service capabilities with traffic engineering, guaranteed QoS, and VPN support.

MPLS gives IP network operators the ability to guarantee and control bandwidth for identified packet flows. Operators can use MPLS to provide finely tuned levels of QoS to accommodate multiple different IP traffic types — giving them a great deal of service flexibility. More importantly, MPLS enables a service provider to maintain these priority settings across its entire backbone. Should link failures or network congestion occur, the network will preserve the applications assigned the highest priorities.

### **How MPLS Enhances IP Service Capabilities**

Service Providers can use MPLS to create cost-effective, efficient networks that deliver three primary capabilities:

1. Traffic Engineering
2. IP Quality of Service
3. Private IP VPN support

#### **Traffic Engineering**

High availability is of utmost importance to anyone concerned with deploying and managing a network. An important advantage of MPLS is its ability to engineer traffic flows across a network. Traffic engineering allows service providers to control network traffic in a predictable manner by establishing predetermined paths based on a possibly complex set of specified path characteristics. When multiple paths are available, traffic engineering calculates the shortest path through the network that meets the traffic's priority, bandwidth and link utilization requirements and assesses network constraints to balance the traffic load across various links, routers, and switches.

Internet traffic engineering facilitates efficient and reliable network operations while simultaneously optimizing network resource utilization and traffic performance. While moderate amounts of jitter and packet loss are acceptable for some applications, they are not acceptable for today's collaborative applications. Effective traffic engineering manages the paths taken by voice, video, data, or general Internet packets to ensure acceptable levels of delay, jitter, and packet loss for all applications.

#### **IP Quality of Service**

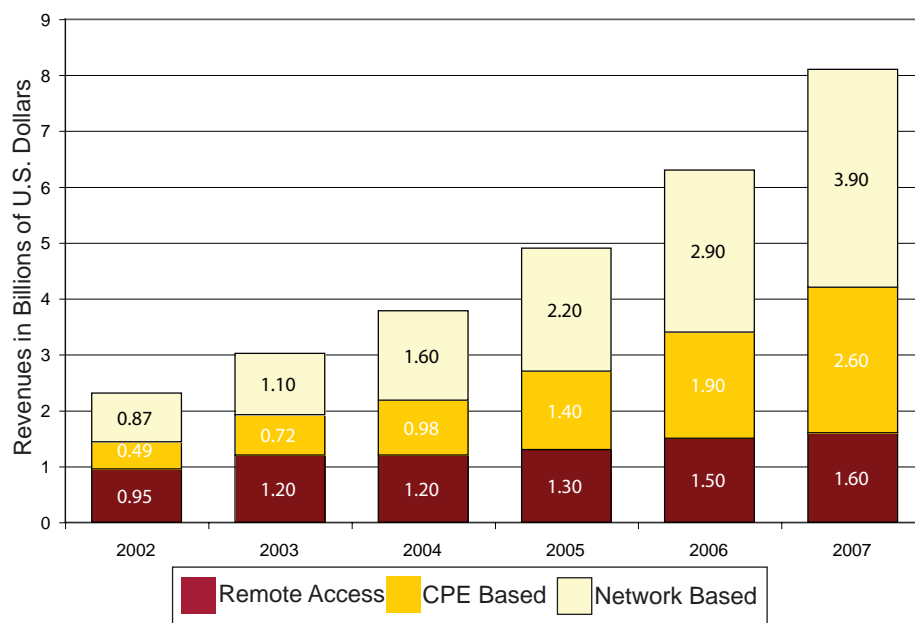
QoS is a key capability that the most advanced service providers implement in their IP networks to benefit their customers. MPLS enables carriers to offer an IP service type that guarantees performance with metrics on latency, packet loss and jitter. Customers that desire high-priority IP packet exchange across their WAN for time- and latency-sensitive applications will subscribe to this service for their mission-critical IP traffic. By giving preferential treatment to voice, video and other high-priority traffic, essential VPN applications stay up and running despite bursts of network activity or failures that may congest the network.

Service providers organize traffic by CoS to ensure that their VPN or Voice over Internet Protocol (VoIP) customers, for example, receive the QoS appropriate for each of their network applications. As they implement end-to-end QoS, these service providers are transforming IP networking from Internet-style, best-effort, take-what-you-get service into a secure, reliable transport system that is as available and resilient as carrier-grade circuit-switched networks – at a reduced cost.

## Private IP Virtual Private Networks (VPNs)

Finally, service providers can use MPLS to create VPNs to securely transport private data across a customer's WAN. A Private IP VPN can replace traditional Point-to-Point, ATM, and Frame Relay networks while offering an equivalent level of security. Although there are a number of ways enterprises can implement VPNs, this paper focuses on network-based VPNs. Network-based Private IP VPNs carry traffic only between designated customer sites over a service provider's IP infrastructure with no visibility to other customers or sites outside of the given VPN. The result provides what is effectively a private network for each VPN customer that is logically separate from the public Internet.

As service providers have invested in the infrastructure required to deliver high quality network-based VPNs, business customers are increasingly using them for large portions of their data and voice traffic. Private IP VPNs are already the most popular class of VPNs tracked by the Yankee Group. In their 2004 Forecast for North American IP VPN Services, the Yankee Group projected that the trend toward network-based IP VPNs would accelerate (see Figure 1).



**Figure 1. \*Yankee Group Forecast for North American IP VPN Services.**

### **The Case for Private IP VPNs**

As this section describes, the value of Private IP VPNs for business customers includes lower costs and ease of deployment, which are reason enough to embrace this approach. However, the ways in which Private IP VPNs are implemented yield additional benefits that will become increasingly important to support voice, video and other latency-sensitive applications.

#### **Less expensive than legacy networks**

With Private IP VPNs, the Customer Premise Equipment (CPE) can be more basic and less expensive because the network intelligence is supplied by the service provider's equipment. Basic routers are less complex with fewer set-up tasks, so less is required of customer staff. Further, IP bandwidth costs have decreased substantially, especially versus legacy Frame Relay and Private Line connections.

#### **Reduced staffing requirements**

Private IP VPNs reduce the customers' needs for expertise in network traffic engineering, selecting and maintaining routing protocols, managing address space, troubleshooting outages, and implementing rapid re-routes around problems; instead, they can leverage the service provider's staff expertise in these areas.

MPLS also reduces the overall network complexity, making it easier to scale and manage the network. A large number of enterprise IT organizations are now beginning to see the potential benefits MPLS brings to their network infrastructure, particularly in the areas of scale, resiliency, availability and security.

#### **Automatic future-proofing**

All modern, enterprise-wide applications are IP-enabled and new applications are seizing the full potential of MPLS over IP networks. For example, many companies are investing in enterprise-wide IP PBXs to serve multiple satellite locations and soon come to realize that Best Effort Internet access does not provide the Quality of Service necessary to support business voice communications. This and other emerging IP-based business applications offer exciting ways to improve productivity and reduce telecommunications costs.

Because the ability to perform such essential business tasks as placing and receiving telephone calls depends on the continuous availability and security of the data network, IT leaders are increasingly working in partnership with service providers that have the technology and expertise needed to make it all work reliably over a Private IP VPN.

Emerging future applications will require IP networks that are increasingly fast, smart, reliable, and secure. These characteristics along with low latency, minimal jitter, and high availability are the hallmarks of today's best Private IP VPNs. Continuing investments by leading service providers ensure that the VPNs they build and maintain will provide their customers with state-of-the-art data transport.

### **Private IP VPNs Provide Enhanced Quality of Service**

In a carrier's network, general Internet traffic employs the same routers and links as the traffic from Private IP VPNs. However, the carriers manage their customer VPNs separately, enabling them to receive preferential treatment throughout the network. These operators use the VPNs to subdivide their networks in the most logical and cost-effective manner for their enterprise customers.

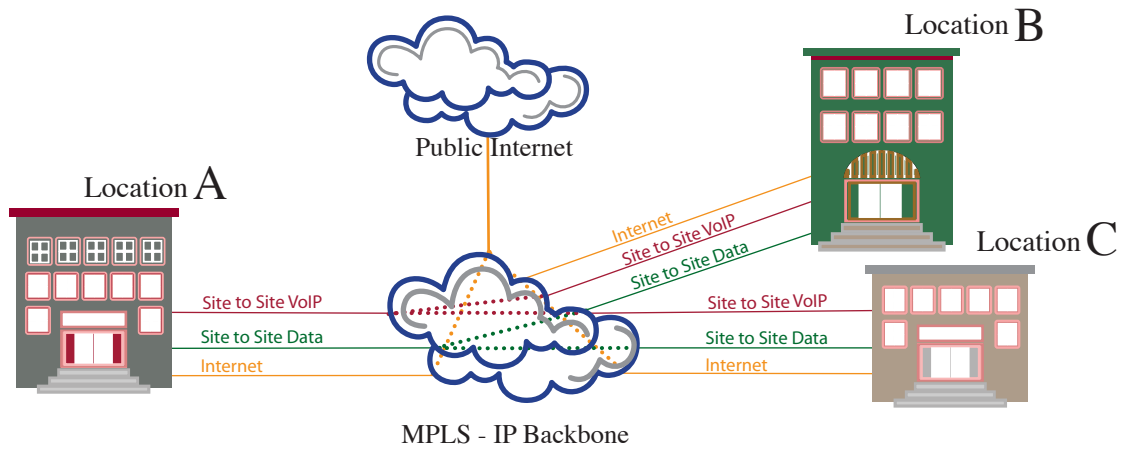
### **Resiliency and Security**

An automatic benefit of Private IP VPNs is that every customer site is connected to every other site in a full-mesh configuration. Organizations that replace their Frame Relay networks with Private IP VPNs will enjoy better performance between remote sites, and the multiple alternate paths that they provide increase resiliency. Additionally, less bandwidth will be needed at former hub sites since there are no hubs in a full-mesh configuration.

One of the main reasons providers now use MPLS throughout their networks is to take advantage of the protocol's many resiliency features. Resiliency is a particular boon to Private IP VPNs.

Customers who entrust their voice and data traffic to a single network must be assured that it will remain private and secure. Private IP VPNs meet these requirements because each VPN is kept logically separate from every other VPN and from general Internet traffic.

When combined with CoS, label-switching enables providers to give their VPN customers extra advantages. In the world of Private IP VPNs, customers whose sites are interconnected with network-based VPNs have hundreds – even thousands – of ways that their data can traverse the network. On networks implementing end-to-end CoS, their data is given priority treatment during times of network congestion.



- High Priority
- Medium Priority
- Low Priority

**Figure 2. A Sample Customer MPLS-enabled IP Network**

The diagram in Figure 2 depicts multiple traffic types traversing a MPLS-enabled IP network that uses CoS designations. In this example, the customer is a small chain of retail stores that has three locations. The customer purchases a VoIP-enabled telephone system at each location and wants to transfer sales and inventory data securely between locations. With MPLS IP service types designated for certain applications, the customer will use a mix of real-time, high priority, medium priority and low priority services as described in the following chart.

<b>CLASS OF SERVICE DESIGNATION BY APPLICATION</b>	
<b>Class of Service</b>	<b>Application</b>
High Priority	Inbound/Outbound and inter-office telephone calls
Medium Priority	Transmit private, secure data traffic among locations
Low Priority	Best effort Internet access for basic web surfing and email

## Conclusion

Deploying a multi-site IP network with the performance and resiliency needed to run applications such as voice can be a difficult and expensive proposition even for large enterprises with sizeable resources. Top carriers are taking advantage of the routing flexibility built into their MPLS-enabled networks to provide their customers with premium VPN services that ensure that each application gets the QoS it requires. As new applications arise for IP-based communications, SMBs are increasingly working with Service Providers that have the technology and expertise to provide all of the benefits of dedicated networks at a lower cost.

Contact: Broadview Networks  
1.800.Broadview  
[www.broadviewnet.com](http://www.broadviewnet.com)

Contact: Juniper Networks  
1.888.Juniper  
[www.juniper.net](http://www.juniper.net)

Copyright © 2006, Broadview Networks, Inc. All rights reserved. Broadview Networks and the Broadview Networks logo are trademarks, registered trademarks or service marks of Broadview Networks, Inc.

Juniper Networks and the Juniper Networks logo are registered trademarks of the Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Broadview Networks or their respective owners.

This document is provided for information purposes only and the contents and specifications are subject to change without notice. Broadview Networks assumes no responsibility for any inaccuracies in this document or for any obligation update information in this document. Broadview Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.