MPLS VPNs: A Current Look

Executive Summary

The Webtorials Editorial/Analyst Division surveyed nearly 400 Webtorials subscribers online about their current and planned MPLS VPN deployments in the second half of 2008. Geographically diverse respondents from various industries participated.

MPLS VPN services appear to be thriving. Seventy percent (70%) of respondents said they already use the services and another 18% anticipate using them. Just 12% said they had no plans to use MPLS VPNs.

However, MPLS VPNs enterprises weren't running the services exclusively. Ethernet, Internet VPNs and other services remain in use in many organizations for WAN access and for serving discrete applications within the long-haul network.

Real-time applications, such as voice over IP (VoIP), streaming communications and various unified communications and collaborative applications are driving MPLS VPN use. The quality of service (QoS) and any-to-any routing characteristics of MPLS VPNs are particularly well suited for these applications and scored high on enterprise priority lists, as discussed in the Key Findings section below.

> **MORE TO COME!**
> This report is Part 1 of a three-part series. The second report zeroes in on the first key finding, examining application deployment and security service usage trends. In Part 3, a Webcast, lead analysts Joanie Wexler and Steven Taylor discuss where enterprises and industry perspectives matched up, where they didn't, and the possible reasons why.

For additional information on the Webtorials survey methodology and respondent demographics visit Webtorials*.*

Key Findings

The Webtorials survey response information broke down into five primary research findings:

1) A high percentage of real-time and latency-sensitive applications are now deployed on – and will continue to join – MPLS VPNs.

When asked what applications they were using or anticipate using within the next year on their MPLS VPNs, respondents who had already deployed an MPLS VPN ranked VoIP (76%), collaborative applications (51%) and streaming communications (50%) at the top of their lists. With such applications on net or on deck, it was no surprise that they also pointed to MPLS's QoS capabilities and any-to-any connectivity as their two top reasons for adopting MPLS VPNs.

2) Network performance is the most important MPLS VPN service attribute in the eyes of customers. In general, the industry is doing a good job delivering.

The highest number of respondents (43%) ranked network performance as one of two service variables they consider most important. These results reflected the applications they intend to use. Performance directly impacts user experiences with real-time and streaming applications, many of which can't tolerate even moderate levels of delay, jitter (variance in the amount of delay) and packet loss. The good news is that, when asked how satisfied they were with network performance, 40% of respondents said they were most satisfied with this service attribute.

3) Ethernet access services are the most deployed for connecting to the MPLS VPN cloud, though native IP/MPLS connections are growing.

More than half (55%) of respondents said they use high-bandwidth Ethernet services to connect to their MPLS services, followed by T1 private lines (54%). Surprisingly, 49% said they are using native IP or MPLS (Layer 3 routing interfaces) for accessing the cloud. Historically, enterprise concern about sharing internal IP Border Gateway Protocol (BGP) routes with their service provider, which is necessary for direct customer premise-to-carrier network MPLS connectivity, has hindered the use of these interfaces.

4) In the long-haul network, Ethernet and Internet VPN services are frequently deployed, often for specific applications.

Next to MPLS VPNs, Ethernet tops the charts for WAN use for a number of applications. Among them are separating workgroups (53%), use as a distributed engineering network (53%), database synchronization (51%) and site-to-site data center backup (50%). Internet VPNs are used frequently for transactional business-to-business networking (53%) and branch office-to-regional site connectivity (47%).

5) Enterprise and service provider responses differed in their usage forecasts of managed and network-based security services.

For example, 34% of enterprises see themselves using managed services "mostly or totally" in the foreseeable future. The industry was much more bullish, with 53% of service providers and equipment makers expecting enterprises to soon largely use managed services. These findings will be more fully explored in a Webcast between lead analysts Joanie Wexler and Steven Taylor.

## Applications Drive Service Attribute Priorities

New network applications that are real-time and collaborative in nature are making QoS important. Nearly half (48%) of all respondents cited QoS as one of the two top reasons they deployed MPLS VPN service. Real-time applications are also increasing the appeal of MPLS's any-to-any routing capability; 39% of survey respondents cited this feature as a top service priority.

More than three fourths (76%) of enterprises using MPLS VPNs said they were using or would soon use VoIP on their MPLS VPN networks. Unified communications (integrated telephony-centric applications), videoconferencing, streaming communications and even life-like telepresence conferencing were among other real-time and collaborative apps on enterprise usage radars.

Figure 1 demonstrates the top applications for MPLS VPNs.

The top applications to be deployed by users who are currently not using MPLS VPN service but plan to use it are similar. Those respondents cited the same QoS and any-to-any network requirements. For example, 71% among this user segment anticipate using VoIP; 56% anticipate using unified communications; and 50% anticipate using streaming communications.

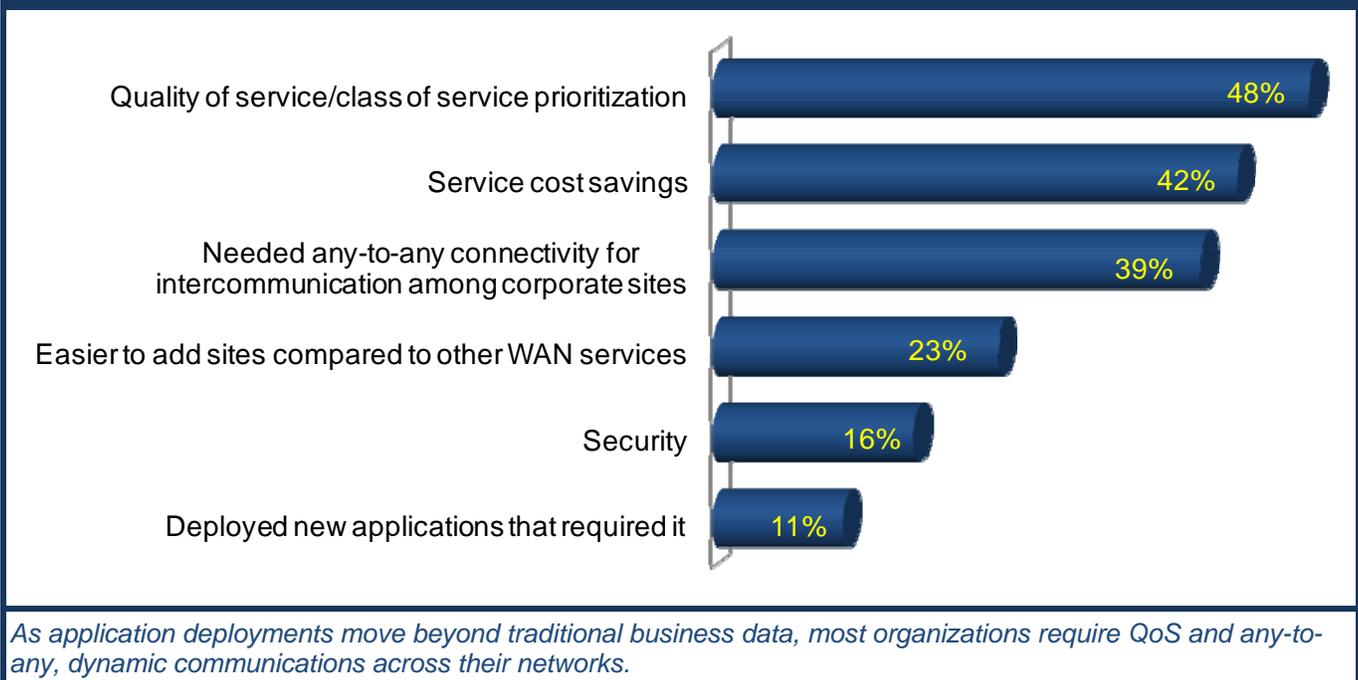### Figure 1. Current and Planned Application Usage
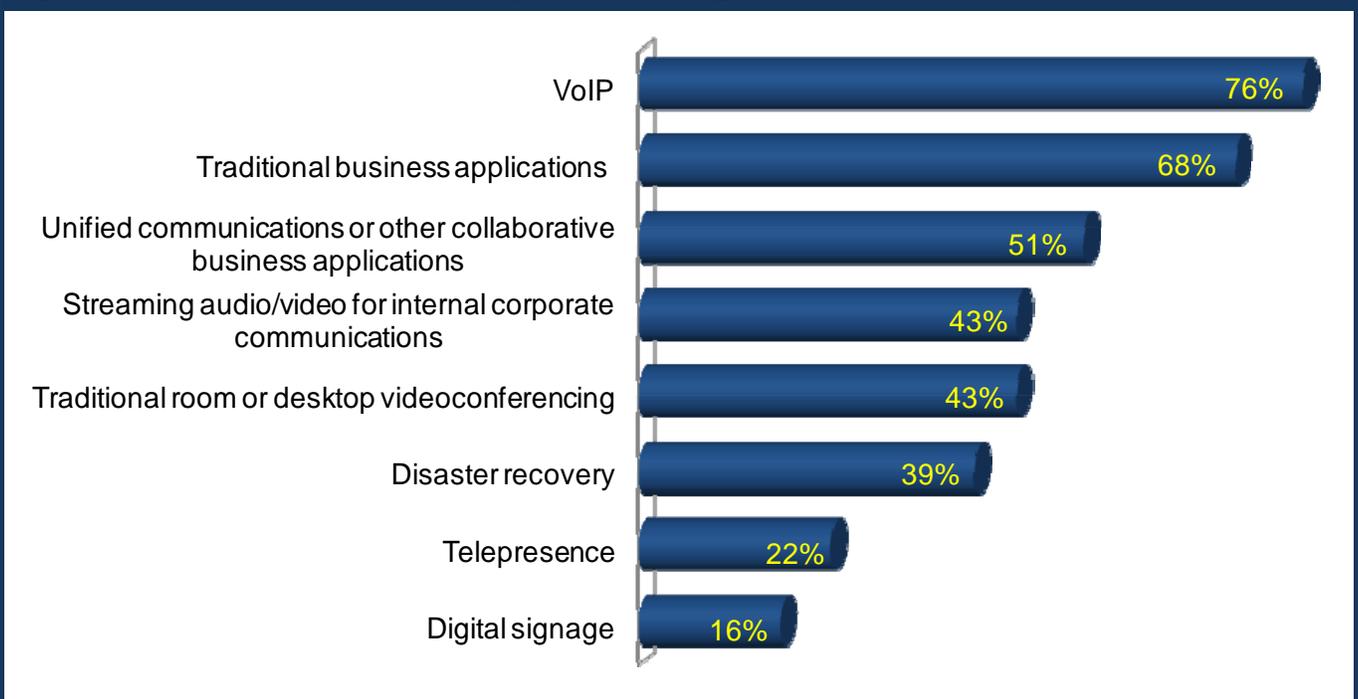
A variety of collaborative applications are joining traditional data on MPLS VPNs.

It follows that QoS and any-to-any network connectivity capabilities would be important (see **Figure 2**), in that voice and other real-time traffic is sensitive to packet delays, jitter and packet loss. Prioritizing VoIP packets ahead of data packets and transmitting them directly between sites, for example, rather than through a central hub site, significantly reduce delivery delays. As such, QoS and direct routing are critical components for delivering reliable and high-performance service. They are also important factors in allowing enterprises to dynamically manage application performance from any location on the WAN.

Those who haven't deployed MPLS VPNs and have no plans to use them cite the lack of relevant applications to merit deploying the technology (43%). Obviously, the nature of applications and their behavior drive the selection of the underlying network infrastructure.

Figure 2. Deployment Drivers

Driver	Percentage
Quality of service/class of service prioritization	48%
Service cost savings	42%
Needed any-to-any connectivity for intercommunication among corporate sites	39%
Easier to add sites compared to other WAN services	23%
Security	16%
Deployed new applications that required it	11%

As application deployments move beyond traditional business data, most organizations require QoS and any-to-any, dynamic communications across their networks.

Cost: Always a Factor

Because MPLS VPNs, like other long-haul services, have monthly recurring services charges, cost always comes under scrutiny. Cost ranked second in importance (33%) to network performance among survey takers, and 31% said cost was one of the two service attributes with which they were most satisfied. However, nearly a fourth (24%) said it was one of the two attributes with which they were least satisfied. Overall, then, the industry is not delivering as well on cost as on performance.

In theory, MPLS VPNs should be less costly than many legacy long-haul services. The reason is that MPLS technology allows for a single virtual circuit from the user site to the MPLS WAN "cloud." From there, the cloud simply routes traffic based on IP address. This setup yields the any-to-any connectivity enterprises want without having to purchase and configure separate virtual circuits or physical circuits

between each pair of sites requiring direct links. In this way, the MPLS configuration helps enterprises conserve on their monthly recurring charges and in operational staff costs and time.

Expertise Considerations

Still, there might be hidden costs in MPLS. Staff expertise – or the perception of required MPLS expertise – is one. Of those respondents with no plans to deploy MPLS VPNs, "lack of technology expertise on-staff" ranked second to lack of applications as the reason(s) why; of that group, 22% cited MPLS expertise as a problem.

In truth, however, companies should take note that if they use other CPE interfaces to connect to the MPLS network, they don't require extensive expertise with MPLS technology. They do need expertise in the WAN interface technology they use – be it T-carrier technology at Layer 1, Ethernet or frame relay at Layer 2 or IP technology at Layer 3.

If using IP, enterprises interested in QoS will require expertise in marking IP's standard Differentiated Services Code Point (DSCP) packet-prioritization policies. These markings are then mapped to MPLS prioritization tags at the edge of the carrier network for end-to-end QoS.

Service Availability

Nearly a third of enterprises using MPLS services (31%) said that availability of MPLS VPN service across multiple far-ranging sites was a key MPLS VPN service attribute. Those with WAN connectivity needs in places where MPLS VPNs aren't offered might need to substitute a different service. Maintaining more network types adds to operational costs and possibly diminishes volume discounts available with any given service, depending on how the contract is negotiated.

Comparison to other WAN Services

Though many respondents want ubiquitous MPLS availability, hybrid WAN service use is common. Most involves the use of Ethernet and Internet VPNs alongside MPLS VPNs. There are a few reasons.

Ethernet

Ethernet access connections to MPLS VPN services offer several attractive characteristics. They provide LAN-like bandwidth, overcoming the "last mile" access network performance bottleneck problem. From an expertise perspective, the Ethernet WAN interface basically becomes just another LAN interface to manage. Though cost is dependent on speed specified, Ethernet generally has an overall lower total cost of ownership (TCO) associated with it because of its maturity level, economies of scale and universal availability of skill sets.

IT staffs also like long-haul Ethernet services because they allow them to extend their virtual LAN (VLAN) configurations over their WANs. They can do this using a "pure" Ethernet WAN service, generally involving use of an end-to-end fiber infrastructure, or by overlaying their VLANs on an Ethernet access service connected to MPLS. The second approach extends VLANs into "one large LAN" across the WAN in a service usually referred to as a virtual private LAN service, or VPLS.

The biggest strike against Ethernet services is their relative lack of ubiquity. Carrier-class Ethernet services require fiber to the building. Fiber penetration, however, is just over 15% of U.S. commercial buildings with 20 or more employees, according to Vertical Systems Group.

Internet VPNs

By contrast, Internet-based IP VPNs are popular for their ubiquity and because they are a relatively inexpensive way to quickly add new sites to the network. In this way, they work well for occasional or temporary business-to-business (B2B) connections, whereby business partners may wish to have some level of communication but do not want a partner to be a full-fledged member of the corporate intranet.

Because they use strong encryption, they are considered secure VPNs. Their potential drawback is performance. Since IP VPNs might traverse more than one service provider's infrastructure, QoS markings may not be valid across carrier borders. It's recommended, then, that businesses procure IP VPN services intended to carry any B2B real-time traffic from a single Internet provider, who can manage end-to-end performance.

Legacy Services

Finally, legacy services, such as frame relay, private lines and even moribund ATM, continue to find applications alongside MPLS VPNs. Frame relay is most often used for hub-and-spoke connectivity such as in branch office to regional site connectivity (32%) and B2B networking (31%). ATM is still in use as a distributed engineering network (34%), for relaying broadcast signals (32%) and for connecting distributed sites to consolidated data centers (30%).

The use of legacy services rarely dies. Legacy services, particularly those that are most fundamental and mature, will remain for niche uses. Private lines (whether based on T-carrier or SONET technologies) are likely to persevere indefinitely, as there will always be uses for an unshared network. Frame relay is likely to remain in place as a convenient access interface into the WAN cloud, as it already has accumulated squatting rights in this application.

ATM will continue to find niche uses, but as the legacy service that was least enthusiastically accepted, it is likely to be replaced by MPLS, at least by attrition. ATM was attractive initially for its class-of-service qualities in multimedia networking environments; MPLS offers that, along with the dynamic ability to switch traffic on the fly between sites, including those of business partners and disaster recovery centers. These capabilities require the burdensome creation of separate virtual circuits in an ATM environment. With a simpler alternative available, most enterprises will likely allow most of their ATM connections to die a natural death.

Managed and Network-based Security Services

Mature managed router services and network-based firewall service types remain more popular than newer types of services, primarily because they are known and trusted. Newer managed services that move the carrier further onto the enterprise, for example, as well as non-firewall network-based security services are having a tougher time catching on as enterprises struggle with the appropriate mix of which tasks to retain in-house and which to outsource.

Conclusion

It is clear that businesses select applications based on their merit and business requirements and then match the appropriate network infrastructure to those applications. The rise of real-time applications along with respondents' stated desire for QoS, direct inter-site connections and high network performance with minimal latency, jitter and packet loss reflects this premise. Meantime, hybrid WANs remain in use to

solve different types of application requirements, led primarily by Ethernet and Internet VPN services. Some legacy services, particularly private lines, will remain a staple in enterprise WANs, though ATM uses are likely to wane the fastest as new MPLS VPN installations bring the required bandwidth, QoS and dynamic linkages to the table.

Part 2 of this series dives more deeply into the current state of collaborative applications, including unified communications and telepresence, and how they are likely to develop in the near term. It also evaluates the impact of these applications on the network and the likely impact of the current down economy on application and service deployments.

Part 3 examines the difference in enterprise and industry expectations with managed and network-based services.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward-looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

The primary author of this Webtorials State-of-the-Market report is Joanie Wexler, an independent technology writer and analyst based in Silicon Valley.

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.