MPLS: Has It Achieved Critical Mass?

Zeus Kerravala

Service providers are committed to the technology, but they still have work to do before customers buy in.

There is absolutely no doubt that Multi-Protocol Label Switching (MPLS) has achieved a critical mass in the marketplace. At least, this is what service providers are likely to tell you. From a telecommunications carrier perspective, there is no turning back the tide; in fact every regional Bell operating company (RBOC) and Tier 1 interexchange carrier (IXC) in North America has embraced MPLS as the cornerstone of its IP-VPN strategy—including Sprint, which previously carried a reputation for being the anti-MPLS carrier.

On the other hand, looking at the results from The Yankee Group's recent *2003 VPN Deployment Strategy Survey* of 258 enterprise IT managers, I can only conclude that these "gung ho" service providers, in their frenzied enthusiasm for MPLS, are perhaps not really listening to their customer base.

The single most salient data point in the survey is that IPSec has become the preferred carrier-managed VPN tunneling mechanism by nearly a 6:1 ratio over MPLS (Figure 1). This clearly is not rosy news for service providers, who are making multimillion-dollar capital investments in converged IP infrastructures with MPLS as the technology foundation.

On the flip side, carrier-managed VPNs were identified in the survey as the long distance WAN solution of choice in the next 12 to 24 months, chosen over internally managed VPNs and, even more conspicuously, over frame relay. Obviously, there is demand for managed VPNs, but what are the variables that enterprise managers should consider when deciding between IPSec and MPLS VPNs?

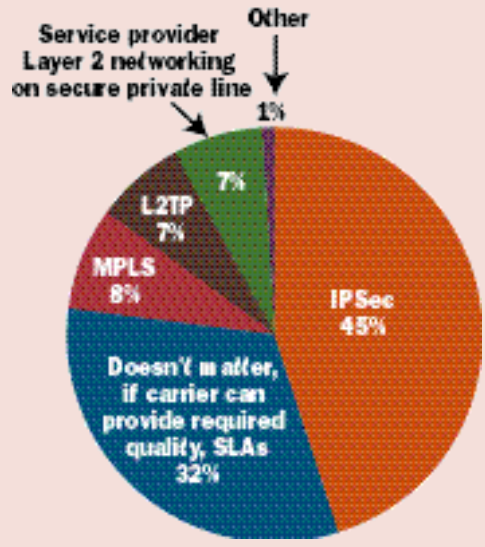
My conclusion is that service providers must begin with some market education on fundamental MPLS-related concepts. I base this on the fact that in almost every instance where I have heard a carrier propose MPLS VPNs to their enterprise audience, the positioning presumes a basic knowledge set that does not exist on the part of the enterprise.

The irony is that service providers are leading with technology (as opposed to emphasizing the discernible business benefits that do exist), yet they fail to illuminate for their customers the essential elements of this technology—elements that enterprises must understand when making their buying decisions. So let me attempt to move the process forward.

Layer 3 MPLS VPNs

The predominant carrier MPLS VPN service deployed today is known in Internet Engineering Task Force (IETF) circles as RFC 2547, and is more commonly referred to as Layer 3 MPLS VPN. However, the heart of this function is not MPLS, but rather routing (hence the reference to Layer 3). In fact, the element most central to the service is a private routing instance known as the VPN Routing and Forwarding table (VRF), which is created independently for each enterprise that subscribes to the service.

FIGURE 1 Preferred Tunneling Technology For Carrier Managed IP-VPN



Zeus Kerravala is vice president of the Yankee Group's Enterprise Infrastructure Planning Service. His areas of expertise include working with enterprise customers to solve their business issues through the deployment of technology solutions.

A VRF is created for the enterprise on every carrier edge router to which the customer is attached. With the advent of the VRF—unlike in traditional Layer 2 WAN services like frame relay—the service provider becomes involved with the routing of its enterprise customers' IP packets.

To offer a very high-level overview, the VRF directly communicates with the customer premises equipment (CPE) router on the access side. On the trunk side, the VRF will propagate VPN routing information into the Border Gateway Protocol (BGP) instance of the edge router, which will then advertise the VPN routes to all other edge routers supporting that VPN affiliation. The RFC 2547 routing elements establish the control plane for the VPN, and the MPLS Label Switched Paths (LSPs) are the tunnels within which actual VPN data traffic flows.

The result of these functions is a fully network-based service where the primary VPN routing function and the VPN tunnel itself are both within the service provider's domain. One of the distinct advantages of this solution as opposed to CPE-based IPSec VPNs is that no incremental device needs to be added to a given customer site for it to participate in the VPN. In fact, the overall complexity of the end nodes on a customer location can be dramatically reduced in this new routed architecture, especially when the VRF becomes the foundation for other virtualized services above and beyond VPNs, such as network-based firewall services.

Unfortunately, carriers tend not to lead with this first-order benefit. Instead, they commonly focus on the inherent any-to-any connectivity and/or IP-aware quality of service (QOS) capabilities of Layer 3 VPNs. Clearly, these offer distinct advantages over a frame relay WAN service, but not necessarily over a managed IPSec VPN solution.

The muddled positioning is a consequence of market education material derived from the carrier and enterprise IP leader, Cisco, which has a strong interest in minimizing the fact that CPE can become much simpler in a network-based VPN world. Because so many service providers use the exact same technology (i.e., Cisco's) and target the exact same customer base, enterprise managers should be explicitly aware of where these messages are coming from and why.

The Cloud Or The Tunnel?

Once service providers have explained the nature of a Layer 3 MPLS VPN, the next step is to explain why an enterprise should choose a cloud-based VPN tunnel when they can get a secure end-to-end IPSec tunnel. Conveniently, the concise answer is aligned directly with the top two decision criteria that enterprises have for selecting a managed VPN, as noted in our survey: Cost and reliability.

Lower cost and higher reliability are distinct advantages that can only be derived from the network-based MPLS model. A centralized IP-VPN residing on an edge platform comes with a much lower capital cost through shared economies and higher operational efficiency than can be achieved with CPE. The primary sources of this higher efficiency are centralized provisioning and management.

Bundling broadband access and MPLS VPNs could be an effective RBOC strategy

Ultimately, all these benefits to the carrier can be passed down to the enterprise as a lower-cost service than a managed CPE IPSec solution, while at the same time guaranteeing higher reliability. Higher availability is also achieved via carrier-class routing devices with advanced fault-tolerance and network restoration capabilities; CPE devices are inadequate on this front. I cannot stress enough the importance of enterprise managers pushing service providers on these well-developed, yet simple benefits, which are often glossed over during the sales process.

International providers have had more luck in driving volume market adoption for MPLS-based VPNs. However, it is not the "bells and whistles" that are fostering adoption overseas, but rather the strong availability of broadband access technologies, particularly DSL, in Europe and Asia; when bundled with the VPN, these access services result in a very price-attractive WAN connection. Enterprise network managers in the U.S. can and should push their service providers for these kinds of service bundles.

This kind of bundled offer could help overcome the number one obstacle to managed VPN adoption that enterprises identified in our survey: cost of service. Cost is a particularly sensitive issue because enterprises experimenting with managed VPN usage are seeking economic incentives to do so.

A bundled broadband-plus-VPN service presents an excellent opportunity for providers like SBC and Verizon, who are trying for the first time, with their new IP/MPLS networks, to compete with the likes of AT&T and Sprint for nationwide WAN business. As the owners of the broadband local loop with no real national WAN legacy to protect, they can bundle economically aggressive solutions that resonate with enterprises in a way that conventional long-haul carriers cannot. In

fact, enterprises may wish to push for a broadband MPLS VPN remote office solution and/or a back-up WAN connection, which would allow for a mutually beneficial service for both carrier and enterprise.

Beyond Price

Nevertheless, price alone cannot carry the day, if for no other reason than carriers surely do not seek to commoditize what they are all touting as their premier WAN service moving forward. And there are other elementary reasons. For example, service providers have yet to completely shift MPLS VPNs out of the technology sandbox and into the mainstream as a full-blown WAN service.

Many of the conversations I have with service providers revolve around how they are still in the early stages of supplementing IP WAN connectivity with the deep list of *a la carte* service options that are part and parcel of their frame relay and ATM packages today. Two particularly prominent options are performance monitoring and back-up dial access. Without making these options available, a service provider would be hard-pressed to position what they are selling as a robust, outsourced, managed service offering. The good news is that service providers are now addressing customer concerns about the absence of these key features in the initial offerings.

Another service option is to combine MPLS and IPSec to better serve scattered enterprise locations

Performance monitoring is not to be understated, as all frame relay solutions have a managed option that comes with third-party applications like Visual Networks' Uptime product. The purpose is to provide the enterprise with insight into various aspects of the service level agreements (SLAs) they are paying to have upheld. Finally, service providers are merging the advances they have made via their own homegrown customer network management (CNM) portals with off-the shelf reporting technologies to portray the right level of detail in the right format for MPLS WAN services.

Back-up dial access is an equally significant though fairly recent service add-on, especially for enterprises that are giving serious consideration to MPLS as their lead WAN solution. Without an automatic back-up mechanism in place for when/if a primary connection fails, enterprises will certainly be reluctant to make any significant WAN migration.

MPLS And Convergence

The timing is right for these new service options, especially in light of our survey results, which indicate that enterprises will see a considerable upswing in convergence over IP over the next 24 months. IP voice and video will see the largest shift in adoption among major applications, so making sure that the network can meet their notably rigid SLA requirements will be of paramount importance.

The emergence of IP voice and video as mainstream enterprise applications will help carriers market the value of an MPLS-based VPN. The truth is that only a MPLS VPN can help realize the benefits of the converged IP application infrastructure that is being sought.

Any-to-any connectivity as a service function does have resonance in the context of voice over IP (VOIP). And with the ability to tightly bind DiffServ Code Points (DSCPs) with MPLS LSPs, carriers can deliver rich application-level QOS and SLAs. Supporting these capabilities are MPLS traffic-engineered backbones (IP or ATM) that ensure the integrity of committed performance metrics from edge to edge.

As a point of clarification, MPLS and IP QOS are separate technologies, despite widespread perception to the contrary. The two can be bound together, but it certainly is not a default option. That said, the notion of the converged infrastructure will ultimately compel enterprises to look beyond the classic frame relay and ATM.

How Will Carriers Differentiate Themselves?

Service providers are competing against each other with the same arsenal of features, constrained by the functionality of the Cisco/Juniper routers they are using within their networks. As a result, they must find other ways to differentiate themselves.

This is where other network-based IP services can be added to enrich their bundled service portfolios and appeal to the broad networking needs of the enterprise. These network-based services, which include managed firewall, IP address management and secure remote access, are promoted by traditional IP services equipment vendors like CoSine Communications as well as the edge router vendors. Just like MPLS VPNs, over time these services can supplant the capabilities that traditionally reside within CPE devices.

Carriers may also be able to differentiate themselves by combining VPN technologies. That's because solutions based on MPLS alone only tackle site-to-site IP WAN challenges, which are just a subset of an enterprise IT manager's concerns. In contrast, managed CPE IPSec VPN/firewall devices deliver much more functionality to enterprises, because they can be used to connect individual remote users—not just office sites—to the main network.

As a result, service providers like Equant, KT (formerly Korea Telecom) and Sprint are blending the two VPN technologies in their service offerings. Equant makes significant use of complementary network-based services, with a particular emphasis on IPSec-to-MPLS interworking. The interworking improves on a standalone Layer 3 MPLS VPN-only solution in two ways:

- It can integrate secure remote access and site-to-site VPNs seamlessly to support anytime, anywhere connectivity for enhanced end-user productivity. In this model, a remote access client tied to a PC or a PDA can be securely brought into the MPLS WAN (or the frame relay WAN for that matter) using any access method.
- Secondly, and of equal importance, is the blending of off-network VPN sites with on-net MPLS sites. Folding IPSec into the service overcomes the current constraint that there are only a handful of inter-carrier Network-to-Network Interface (NNI) MPLS agreements in place among the providers.

For example, despite having the world's largest MPLS network, with a presence in more than 150 countries, Equant is still very focused on extending its reach. With IPSec in place, enterprises can leverage the ubiquity of the Internet, and any location in the world can be incorporated (via a local ISP where Equant lacks a presence) into a site-to-site WAN infrastructure that nevertheless is primarily MPLS-based.

In addition, a number of carriers have taken to using split tunnels to bundle secure localized Internet access with their MPLS VPNs that use network-based firewalls. For example, KT enables this service by default with every VPN-attached location, providing differentiation in its highly competitive marketplace.

In this manner, the enterprise gets two services for roughly the price of one by enabling intranet WAN and public Internet service connections to both be achieved over a single access circuit. Again, this offers a simple yet compelling value proposition.

Conclusion

The state of the VPN market is appreciably different today than it was during the early years of the hype cycle. In some ways, MPLS has lived up to its billing, and in others it has not.

What is clear is that MPLS—now backed by the largest carriers in the world—is going to be the heart of all major data investments moving forward. Not only will it be the VPN of choice among both carriers and enterprises, but carriers are also planning to have their MPLS backbones become the cornerstone infrastructure over which all traffic will run.

However, carriers need to listen to their enterprise customers and, likewise, enterprise managers need to educate themselves about what is possible with this flexible technology. Market education and a strong focus on compelling service bundles are going to be essential to making the promise of MPLS a reality□

Companies Mentioned In This Article

AT&T (www.att.com)
Cisco (www.cisco.com)
CoSine Communications (www.cosinecom.com)
Equant (www.equant.com)
Juniper (www.juniper.net)
KT (www.kt.com),(www.kt.co.kr)
SBC (www.sbc.com)
Sprint (www.sprint.com)
Verizon (www.verizon.com)
Visual Networks (www.visualnetworks.com)

In some ways, MPLS has lived up to its billing, and in others it has not