

MPLS and MPLS VPNs: Basics for Beginners

Christopher Brandon Johnson

Abstract

Multi Protocol Label Switching (MPLS) is a core networking technology that operates essentially in between Layers 2 and 3 of the OSI model; for this reason, MPLS has been referred to as operating at Layer 2.5. MPLS can overlay existing technologies such as ATM (Asynchronous Transfer Mode) or Frame Relay, or it can operate in an entirely IP native environment; this can allow users to take advantage of existing CPE (Customer Premises Equipment) while making a move towards converging all network traffic, such as data, video and voice, at a pace that users can accommodate and afford. MPLS provides its users a number of advantageous features such as traffic engineering, network convergence, failure protection, and the ability to guarantee Quality of Service (QoS) over IP. MPLS Vans take advantage of the inherent characteristics of MPLS to provide secure data networking, typically for business users, in conjunction with other VPN technologies to help increase scalability while keeping costs at a manageable level. This paper should help to provide a basic understanding of MPLS technology, its advantages and limitations, and its application as an IP VPN.

Introduction to Multi Protocol Label Switching

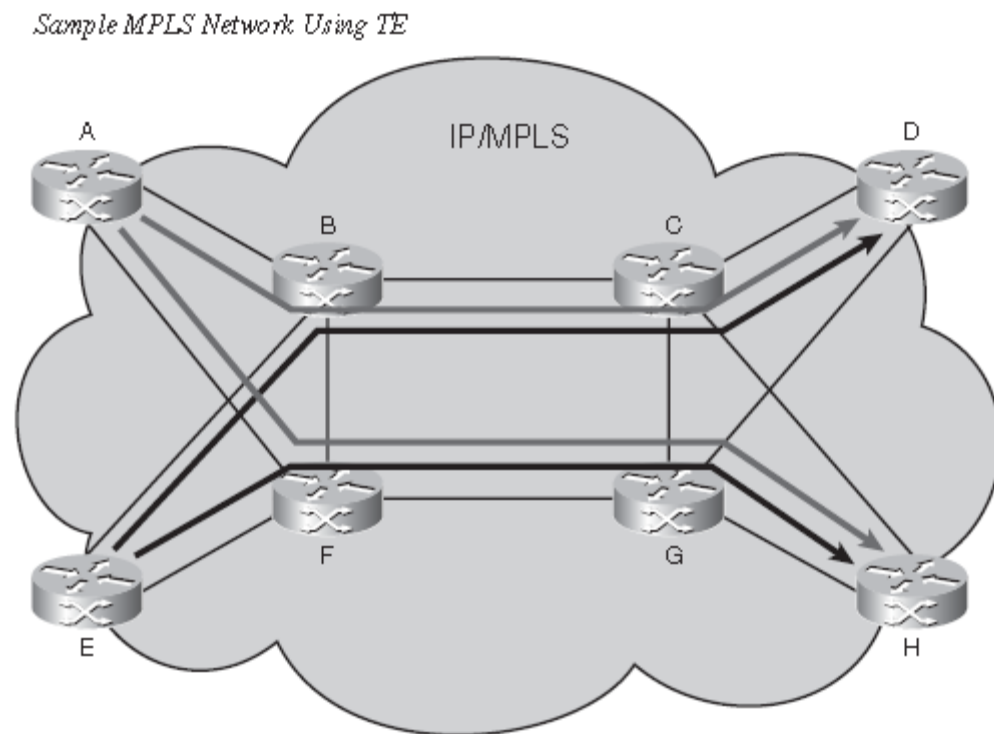
Frame Relay and Asynchronous Transfer Mode (ATM) have been the benchmarks for transmitting data quickly and securely thru point-to-point connections. This is established by utilizing Private Virtual Circuits (PVC's) between all the end user locations, or respective hub locations, creating a mesh topology. This is an effective, secure way to transmit especially when the traffic has specific bandwidth requirements

such as IP Telephony and live video. Unfortunately, provisioning and supporting this type of structure is expensive and does not take advantage of the now predominant IP environment.

Multi Protocol Label Switching (MPLS) is a core networking technology that operates between Layer 2, the Data Link Layer, and Layer 3, the Network Layer, of the OSI model (AT&T Knowledge Ventures, 2007, p. 1). For this reason, MPLS has been referred to as operating at 'Layer 2.5'. This is due in part to the 'shim' label that MPLS routers insert between the layer 2 and layer 3 information. Data enters an MPLS network thru a Label Edge Router (LER). LERs are the most sophisticated routers in an MPLS network as they are responsible for ingress and egress from the MPLS system from and back into a user network or into the greater IP cloud. LER's also known as Provider Edge(PE) Routers or Edge Label Switch Routers add a label to incoming packets and 'pop' a label off of outgoing packets as they enter and exit the MPLS enabled network. The labels that are added to packets in an MPLS network allow the Label Switch Routers (LSR) within the network to determine where and with what degree of importance packets are sent. It is important to note that, since it is the labels that are used for addressing purposes, MPLS provides protocol independent forwarding. Once the packets are in the MPLS network, it doesn't matter whether the packets originated from a Layer 2 device or are native IP; the MPLS network treats them the same, only the edge devices have to know the Layer 2 protocol. MPLS routers utilize a Label Forwarding Information Base (LFIB) instead of routing tables to send packets across the network and Label Distribution Protocol (LDP) to obtain label information from other routers in the network. This allows for faster lookup and addressing.

MPLS also enables Traffic Engineering (TE) within the MPLS core network by mapping traffic to predefined LSP's; either to maximize utilization of bandwidth, prioritize traffic, prevent congestion and bottlenecking or all of the above. Traffic Engineering allows for specific Label Switched Paths (LSP) to be established within the network. Traffic flows can be statically configured to follow certain LSP's so as to more efficiently allocate bandwidth, avoiding overusing some paths and under using others.

Figure 1 – Example of Label Switched Paths



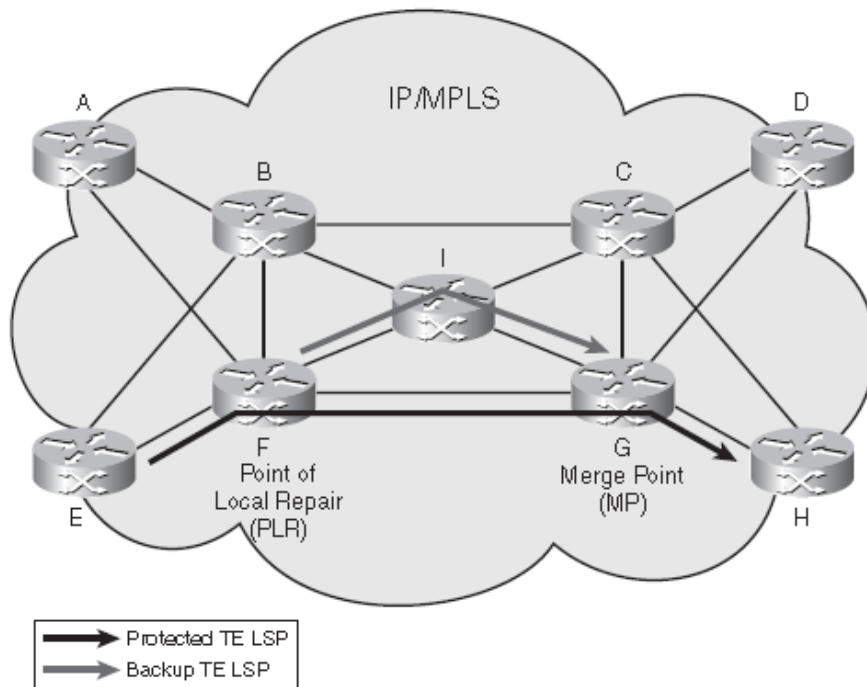
. In Figure 1 above, routers A, D, E and H are LER's while the interior routers would be considered LSR's; Figure 1 also shows a representation of LSP's within the network. The pre-engineered paths within the MPLS network allow for traffic to avoid congestion and bottlenecks that are sometimes inherent in traditional IP clouds. The LSR's utilize the LFIB to determine which hop the packet will take next, the label that

the packet arrived with is swapped out for a new label, and the packet is sent on its way along the predetermined path. Also, this feature allows for higher priority traffic (VoIP, Video, broadcast) to follow certain paths while lower priority traffic takes others. In this way MPLS can enable users to achieve Quality of Service (QoS) over IP that is equivalent to the Private Virtual Circuits (PVC) that were formerly established over Frame Relay or ATM technology. Before we move forward, QoS can be understood as a certain guaranteed performance level of the network (in a provider managed MPLS network it is backed by Service Level Agreements) determined by certain metrics such as packet loss, latency and jitter (Sprint Nextel, 2006, p. 4). This is a feature that is, for the most part, lost in traditional IP networking due to the fact that IP is a, connectionless, best-effort delivery technology; regardless of the importance of the traffic or its specific bandwidth requirements, it will be treated much the same as all other traffic traversing the IP network. This is a key advantage of MPLS that retains the ‘connection oriented’ QoS of legacy Layer 2 technologies. For the same reasons that MPLS can provide traffic engineering for maximum utilization of bandwidth and to provide QoS by differentiating the importance of different types of traffic, MPLS provides its users with remarkably swift disaster recovery via methods such as Fast Reroute (FRR). FRR allows for traffic to be rerouted down backup LSP’s with rapid failover time, 50 ms or less to be comparable to SONET rings and reliably support bandwidth requirements of real-time applications (Cisco Systems, 2005, p. 9), until the node or link failure is repaired. The node that detects a failure, known as the Point of Local Repair or PLR, either sends notification back to the headend to reroute the traffic around the failure, or the PLR reroutes traffic until the failure is repaired, then returns the path to normal. These

methods are known as global and local restoration; global is generally preferred as the headend LSR usually has a better overall view of the network resources (Cisco Systems, 2006, p. 73). Figure 2 below provides a graphical example of protected LSP's where FRR could be utilized to prevent traffic disruption.

Figure 2 - Failure Protection Utilizing FRR

MPLS Network Using FRR



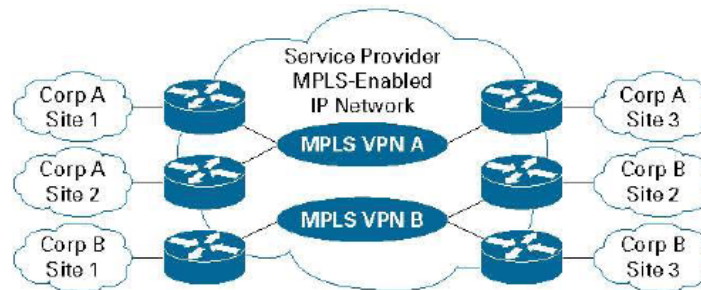
(Cisco Systems, 2006, p. 72)

In addition to the TE and QoS, MPLS adds increased scalability. As we discussed earlier, Layer 2 technologies need a fully meshed environment to enable any-to-any communication. In these point-to-point networks, end-to-end peering is complex and time consuming to support. In addition it can take a great deal of time to provision virtual circuits. With the addition of new network sites, all other sites must be peered with that site, which can be much more time consuming and expensive in a Layer 2 environment. With MPLS, there is only one edge router that peers with the MPLS

network, and this is true for the other physical locations on the network as well. So, when additional network locations are added, only one interface is necessary to connect to the MPLS network, and connectivity with the entire network can be established in much less time. This also helps to prevent traffic bottlenecks that could occur with traditional hub-and-spoke configurations, where all remote sites communicated through a central site (Cisco Systems, 2005, p. 3). Figure 3 below illustrates how, instead of peering with individual sites directly, network sites have any-to-any connectivity via the MPLS enabled network utilizing the LER's.

Figure 3 – An example of Site to Site Connectivity with MPLS (VPN)

Site-to-Site MPLS-Based VPN



(Cisco Systems, 2004)

Even with the predominance of IP and the advantages that MPLS offers, it still has some limitations. For example, remote access users will still have to utilize some form of connectivity to access the MPLS network. The biggest limitation of MPLS is that since it is a core networking technology, an MPLS backbone is required for users to tap into the features and benefits that it offers. If a corporation built their own MPLS network from the ground up it would be a significant investment. For this reason, historically, mid-sized and larger companies have been the key users of MPLS technology. However, MPLS enjoys a strong support base from the industry. Cisco

Systems has been a proponent and enabler of the technology from its beginnings as Tag Switching, and many of the most capable providers of MPLS network infrastructure utilize Cisco equipment. With more global network providers than ever increasing the reach of their MPLS networks; the availability of MPLS services to all types of customers as well as true any-to-any connectivity is moving closer to reality (AT&T Knowledge Ventures, 2007, p. 2).

MPLS VPN: Building on the Basics

MPLS VPN is the logical next step in utilizing MPLS technology to securely transport data over IP. A multitude of service providers are now offering enterprise MPLS VPN service in a number of different flavors based on the needs of small to global corporations, existing investment in CPE, and the available infrastructure. Since MPLS provides protocol independent forwarding, MPLS VPN's can be implemented utilizing varying customer edge equipment allowing the customers to leverage their existing investments while benefiting from the advantages of MPLS.

MPLS, by its very nature, provides traffic separation with its addressing methodology – the labels used to move traffic via MPLS can be easily used to provide separate traffic ‘tunnels’ for multiple VPN's across an MPLS core network. By ‘stacking labels’ MPLS creates logical traffic separation because only the top-most label is used for addressing the packet; any information that is contained beneath the addressing label is invisible to all devices except the intended destination. This is the same type of security provided by Layer 2 technologies such as Frame Relay or ATM. The LER, or in the case of a VPN a Provider Edge or Customer Edge Router, is the only device which accesses the VPN network directly. This provides fewer access points into the network and only

this router must have the highest level of security. Traffic is separated at the Provider Edge (PE) utilizing Virtual Routing and Forwarding Instances (VRF's) which are assigned to each VPN accessing the provider's MPLS network individually (Cisco Systems, 2004, p. 2). The VRF's are unique to each VPN so all other VPN's using the network are transparent to each other, as well as any other Customer Edge (CE) devices.

MPLS VPN's provide a number of advantages based on the inherent characteristics of MPLS networks. MPLS VPN's provide security thru traffic separation, are highly scalable, and they provide QoS based on varying numbers of classes of service (CoS). The number of CoS and the specific QoS guarantees are defined and backed by Service Level Agreements (SLA) with individual service providers (Cisco Systems, 2004, p. 4). MPLS VPN's are limited by the core network, however, and remote users must utilize some other VPN method, most likely IPsec, to peer with the network securely (AT&T Knowledge Ventures, 2006, p. 2). Also, MPLS VPN's do not enable encryption of data on their own, so if encryption is necessary, IPsec, for example, can be used over MPLS to encrypt data before it enters the VPN network. In this way, while reducing the scalability and cost advantages somewhat, a user could take advantage of the TE available with MPLS while utilizing IPsec data encryption for optimal security.

Conclusion

MPLS is a rapidly expanding technology that provides a number of advantages to its users such as scalability, security, redundancy and QoS. The limitations of the technology lie in the expense of constructing MPLS backbones with the intelligent devices to enable the TE and the bandwidth to support it. However, with tremendous industry support, and the ability to utilize MPLS over almost any transport technology

from Frame Relay to fiber, these limitations may be overcome in the future by global service providers utilizing integrated networks to provide small and large business customers cost effective, secure VPN solutions.

References

AT&T Knowledge Ventures. (2007, July 25). *Transitioning to an MPLS Network*. Retrieved November 19th, 2007, from http://www.business.att.com/nx_resource.jsp?repopid=Topic&rtype=Whitepaper&rvalue=eb_fpoc_navigating_to_mpls_enabled_networks&repoitem=vpns&segment=ent_biz

AT&T Knowledge Ventures. (2007, August 31). *Understanding VPN Technology Choices: Comparing MPLS, IPSec and SSL*. Retrieved November 19th, 2007, from http://www.business.att.com/nx_resource.jsp?repopid=Topic&rtype=Whitepaper&rvalue=understanding_vpn_technology_choices&repoitem=vpns&segment=ent_biz&guid=4BFDAE84-C61B-416F-886A-F606E9678B1C;08905D72-1FE7-450C-8EA5-B5F1565DD558

Cisco Systems, Inc. (2004). *Managed VPN – Analysis and Comparisons of MPLS-Based IP VPN Security*. Retrieved November 18th, 2007, from http://www.cisco.com/en/US/netsol/ns465/networking_solutions_white_paper09186a008020c5a6.shtml

Cisco Systems, Inc. (2004). *Managed VPN – Comparison of MPLS, IPSec, and SSL Architecture – Comparing MPLS, IPSec, and SSL*. Retrieved November 19th, 2007, from http://www.cisco.com/en/US/netsol/ns465/networking_solutions_white_paper0900aecd801b1b0f.shtml

Cisco Systems, Inc. (2004). *Managed VPN – Van Wijnen and Versatel*. Retrieved November 19th, 2007, from http://www.cisco.com/en/US/netsol/ns465/networking_solutions_customer_profile0900aec801aa3f5.html

Cisco Systems, Inc. (2005). *From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task*. Retrieved November 18th, 2007, from http://www.cisco.com/en/US/netsol/ns458/networking_solutions_white_paper0900aecd8017a894.shtml

Cisco Systems, Inc. (2006, June). *Understand MPLS Technology. MPLS TE Technology Overview*. (chap. 2). Retrieved November 19th, 2007, from <http://downloads.techrepublic.com.com/thankyou.aspx?authId=uqqOzCBTkk7ekSZjOPwgf9Z5C6ZJWyXLNmi0MVnKEACzi6IN9H2AHB5e56BBkJxn&q=MPLS%20TE%20overview%20cisco&docid=177738&view=177738&load=1>

Layer 2 MPLS VPN. (2007, October 20). In *Wikipedia, The Free Encyclopedia*. Retrieved 18:03, November 18, 2007, from http://en.wikipedia.org/w/index.php?title=Layer_2_MPLS_VPN&oldid=165912463

Martini draft. (2007, April 2). In *Wikipedia, The Free Encyclopedia*. Retrieved 18:03, November 18, 2007, from http://en.wikipedia.org/w/index.php?title=Martini_draft&oldid=119746107

Multiprotocol Label Switching. (2007, November 7). In *Wikipedia, The Free Encyclopedia*. Retrieved 18:04, November 18, 2007, from http://en.wikipedia.org/w/index.php?title=Multiprotocol_Label_Switching&oldid=169803565

Pseudo-wire. (2007, November 17). In *Wikipedia, The Free Encyclopedia*. Retrieved 18:01, November 18, 2007, from <http://en.wikipedia.org/w/index.php?title=Pseudo-wire&oldid=172121304>

Juniper Networks. Traffic Engineering for the New Public Network. http://www.omimo.be/magazine/00q4/2000q4_p054.pdf

Sprint Nextel, Inc. (2006, January). *Sprint Global MPLS VPN IP Whitepaper*. Retrieved November 19th, 2007, from <http://whitepapers.techrepublic.com.com/thankyou.aspx?authId=uqqOzCBTk7ekSZjOPwgf9Z5C6ZJWyXLNmi0MVnKEADJ90SewjXUM22n4A2PUWMB&&q=Sprint+Global+MPLS+VPN&docid=273906&view=273906&load=1>

Verizon, Inc. (2006, December). *MPLS VPN Networking and Migration Considerations*. Retrieved November 18th, 2007, from <http://whitepapers.techrepublic.com.com/thankyou.aspx?&q=MPLS+VPN+Networking+and+Migration+Verizon&docid=284829&view=284829>