MPLS - A Choice of Signaling Protocol

Muhammad Asif[1], Zahid Farid[2], Muhammad Lal[3], Junaid Qayyum[4]

**[1]Department of Information Technology and Media (ITM), Mid Sweden University
Sundsvall 85170, Sweden.**

**[2]School of Electrical and Electronics Engineering, Universiti Sains Malaysia (USM)
Penang 14300, Malaysia.**

**[3,4]Department of Information Technology, Gandhara University of Sciences
Peshawar 25000, Pakistan.**

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. This paper covers MPLS, Label Distribution, Explicit Routes, Constrained Routes, Resource Reservation, Traffic Engineering, Service Level Contracts, Virtual Private Networks and Modern Networks needs. Our Next papers will focus on MPLS Traffic Engineering Overview and Differences and Similarities between RSVP and CR-LDP.

Keywords Multi Protocol Label Switching (MPLS), OSI model, ATM (Asynchronous Transfer Mode), CPE (Customer Premises Equipment), Quality of Service (QoS), VPN (Virtual Private Networks), Traffic Engineering, Resource ReSerVation Protocol (RSVP), Constraint-based Routed Label Distribution Protocol (CR-LDP).

1. Introduction

MPLS is a new technology that offers to open up the Internet by providing many additional services to applications using IP. MPLS forwards data using labels that are attached to each data packet. These labels must be distributed between the nodes that comprise the network. Many of the new services that ISPs want to offer rely on Traffic Engineering functions. [1] There are currently two label distribution protocols that provide support for Traffic Engineering: Resource ReSerVation Protocol **(RSVP)** and Constraint-based Routed Label Distribution Protocol **(CR-LDP)**. Although the two protocols provide a similar level of service, the way they operate is different, and the detailed function they offer is also not consistent. Hardware vendors and network providers need clear information to help them decide which protocol to implement in a Traffic Engineered MPLS network. Each protocol has its champions and detractors, and the specifications are still under development. Recognizing that the choice of label distribution protocol is crucial for the success of device manufacturers and network providers, this White Paper explains the similarities and important differences between the two protocols, to help identify which protocol is the right one to use in a particular environment. Data Connection's DC-MPLS family of portable MPLS products offers solutions for both the RSVP and CR-LDP label distribution protocols. Multi-Protocol Label Switching (MPLS) is a new technology that will be used by many future core networks, including converged data and voice networks. [2] MPLS does not replace IP routing, but will work alongside existing and future routing technologies to provide very high-speed data forwarding between Label-Switched Routers (LSRs) together with reservation of bandwidth for traffic flows with differing

Quality of Service (QoS) requirements. MPLS enhances the services that can be provided by IP networks, offering scope for Traffic Engineering, guaranteed QoS and Virtual Private Networks (VPNs). The basic operation of an MPLS network is shown in Figure 1.

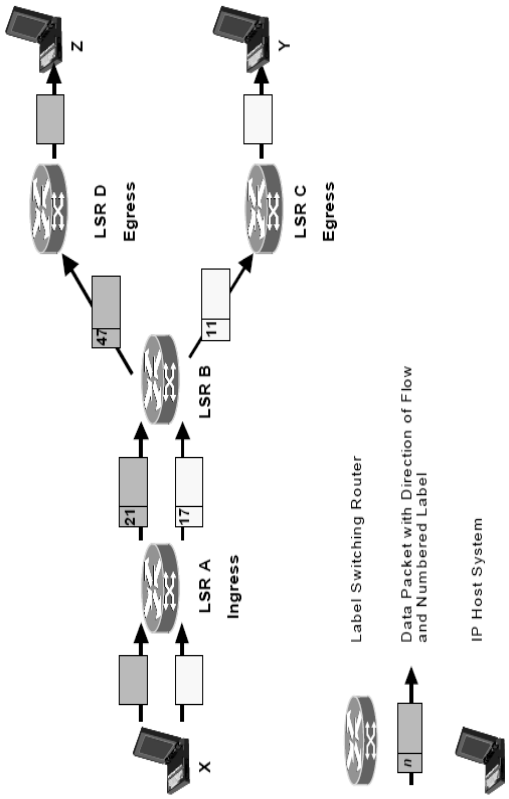

Figure 1 (Basic operation of MPLS)

MPLS uses a technique known as label switching to forward data through the network. A small, fixed-format label is inserted in front of each data packet on entry into the MPLS network. At each hop across the network, the packet is routed based on the value of the incoming label and dispatched to an outwards interface with a new label value. The path that data traverses through a network is defined by the transition in label values, as the label is swapped at each LSR. [3] Since the mapping between labels is constant at each LSR, the path is determined by the initial label value. Such a path is called a Label Switched Path (LSP). At the ingress to an MPLS network, each packet is examined to determine which LSP it should use and hence what label to assign to it. This decision is a local matter but is likely to be based on factors including the destination address, the quality of service requirements and the current state of the network. This flexibility is one of the key elements that make MPLS so useful. The set of all packets that are forwarded in the same way is known as a Forwarding Equivalence Class (FEC). One or more FECs may be mapped to a single LSP. Figure 1 shows two data flows from host X: one to Y, and one to Z. Two LSPs are shown.

- LSR A is the ingress point into the MPLS network for data from host X. When it receives packets from X, LSR A determines the FEC for each packet, deduces the LSP to use and adds a label to the packet. LSR A then forwards the packet on the appropriate interface for the LSP.

- LSR B is an intermediate LSR in the MPLS network. It simply takes each labeled packet it receives and uses the pairing {incoming interface, label value} to decide the pairing {outgoing interface, label value} with which to forward the packet. This procedure can use a simple lookup table and, together with the swapping of label value and forwarding of the packet, can be performed in hardware. This allows MPLS networks to be built on existing label switching hardware such as ATM and Frame Relay. [4] This way of forwarding data packets is potentially much faster than examining the full packet header to decide the next hop. In the example, each packet with label value 21 will be dispatched out of the interface towards LSR D, bearing label value 47. Packets with label value 17 will be re-labeled with value 11 and sent towards LSR C.

- LSR C and LSR D act as egress LSRs from the MPLS network. These LSRs perform the same lookup as the intermediate LSRs, but the {outgoing interface, label value} pair marks the packet as exiting the LSP. The egress LSRs strip the labels from the packets and forward them using layer 3 routing. So, if LSR A identifies all packets for host Z with the upper LSP and labels them with value 21, they will be successfully forwarded through the network.

Note that the exact format of a label and how it is added to the packet depends on the layer 2 link technology used in the MPLS network. For example, a label could correspond to an ATM VPI/VCI, a Frame Relay DLCI, or a DWDM wavelength for optical networking. [5] For other layer 2 types (such as Ethernet and PPP) the label is added to the data packet in an MPLS "shim" header, which is placed between the layer 2 and layer 3 headers.

2. Label Distributions

In order that LSPs can be used, the forwarding tables at each LSR must be populated with the mappings from {incoming interface, label value} to {outgoing interface, label value}. This process is called LSP setup, or Label Distribution. [6][7][8] The MPLS architecture document (draft-ietf-mpls-arch) does not mandate a single protocol for the distribution of labels between LSRs. In fact it specifically allows for multiple protocols for use in different scenarios**.** Several different approaches to label distribution can be used depending on the requirements of the hardware that forms the MPLS network, and the administrative policies used on the network. The underlying principles are that an LSP is set up either in response to a request from the ingress LSR (downstream-on-demand), or pre-emptively by LSRs in the network, including the egress LSR (downstream unsolicited). It is possible for both to take place at once and for the LSP to meet in the middle. In all cases, labels are allocated from the downstream direction (where downstream refers to the direction of data flow, and this means that are advertised towards the data source). Thus, in the example in Fig.1, LSR D informs LSR B that LSR B should use label 47 on all packets for host Z. LSR B allocates a new label (21), enters the mapping in its forwarding table, and informs LSR A that it should use label 21 on all packets for host Z. Some possible options for controlling how LSPs are set up, and the protocols that can be used to achieve them, are described below.

- Hop-by-hop label assignment is the process by which the LSP setup requests are routed according to the next-hop routing towards the destination of the data. LSP setup could be initiated by updates to the routing table, or in response to a new traffic flow. The IETF MPLS Working Group has specified (but not mandated) LDP as a protocol for hop-by-hop label assignment. RSVP and CR-LDP can also be used.

- In Downstream Unsolicited label distribution, the egress LSR distributes the label to be used to reach a particular host. The trigger for this will usually be new routing information received at the egress node. Additionally, if the label distribution method is Ordered Control, each upstream LSR distributes a label further upstream. This effectively builds a tree of LSPs rooted at each egress LSR. LDP is currently the only protocol suitable for this mode of label distribution.

- Once LSPs have been established across the network, they can be used to support new routes as they become available. As the routing protocols (for example BGP) distribute the new routing information upstream, they can also indicate which label (i.e. which LSP) should be used to reach the destinations to which the route refers.

- If an ingress LSR wants to set up an LSP that does not follow the next-hop routing path, it must use a label distribution protocol that allows specification of an Explicit Route. This requires downstream-on-demand label distribution. CR-LDP and RSVP are two protocols that provide this function.

- An ingress LSR may also want to set up an LSP that provides a particular level of service by, for example, reserving resources at each intermediate LSR along the path. In this case, the route of the LSP may be constrained by the availability of resources and the ability of nodes to fulfill the quality of service requirements. CR-LDP and RSVP are two protocols that allow downstream-on-demand label distribution to include requests for specific service guarantees. Figure 2 Shows MPLS label distribution process.

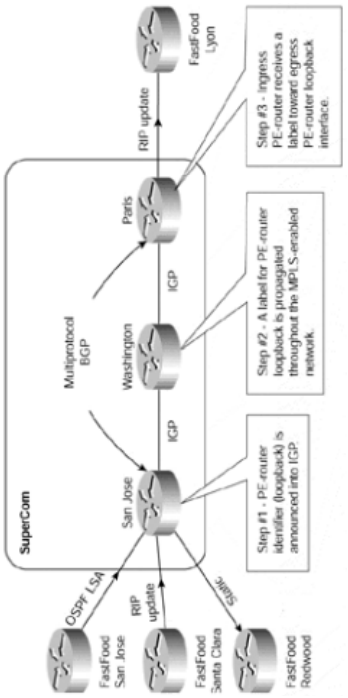

Figure 2 (Label Distribution)

3. Explicit Routers

An Explicit Route (ER) is most simply understood as a precise sequence of steps from ingress to egress. An LSP in MPLS can be set up to follow an explicit path, i.e. a list of IP addresses. However, it does not need to be specified this fully. For example, the route could specify only the first few hops. After the last explicitly specified hop has been reached, routing of the LSP proceeds using hop-by-hop routing. A component of an explicit route may also be less precisely specified. A collection of nodes, known as an Abstract Node, may be presented as a single step in the route, for example by using an IP prefix rather than a precise address. The LSP must be routed to some node within this Abstract Node as the next hop. The route may contain several hops within the Abstract Node before emerging to the next hop specified in the Explicit Route. An Explicit Route may also contain the identifier of an Autonomous System (AS). This allows the LSP to be routed through an area of the network that is out of the administrative control of the initiator of the LSP. The route may contain several hops within the Autonomous System before emerging to the next hop specified in the Explicit Route. An Explicit Route may be classified as “strict” or “loose”. A strict route must contain only those nodes, Abstract Nodes or Autonomous Systems specified in the Explicit Route, and must use them in the order specified. A loose route must include all of the hops specified, and must maintain the order, but it may also include additional hops as necessary to reach the hops specified. Once a loose route has been established it can be modified (as a hop-by-hop route could be) or it can be “pinned” so that it does not change. [9][10] Explicit routing is particularly useful to force an LSP down a path that differs from the one offered by the routing protocol. It can be used to distribute traffic in a busy network, to route around network failures or hot spots, or to provide pre-allocated back-up LSPs to protect against network failures. Figure 3 shows MPLS explicit routes.

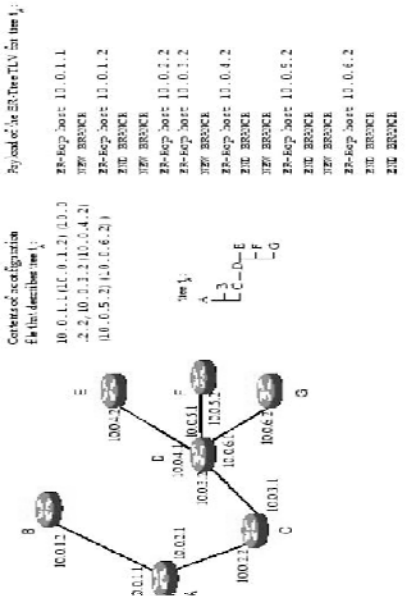

Figure 3 (Explicit Routes)

4. Constrained Routes

The route that an LSP may take can be constrained by many requirements selected at the ingress LSR. An Explicit Route is an example of a constrained route where the constraint is the order in which intermediate LSRs may be reached. Other constraints can be imposed by a description of the traffic that is to flow and may include bandwidth, delay, resource class and priority. One approach is for the ingress LSR to calculate the entire route based on the constraints and information that it has about the current state of the network. This leads it to produce an Explicit Route that satisfies the constraints. The other approach is a variation on hop-by-hop routing where, at each LSR, the next hop is calculated using information held at that LSR about local resource availability. The two approaches are combined if information about part of the route is unavailable (for example, it traverses an Autonomous System). In this case the route may be loosely specified in part, and explicitly routed using the constraints where necessary. Figure 4 shows MPLS constrained route.

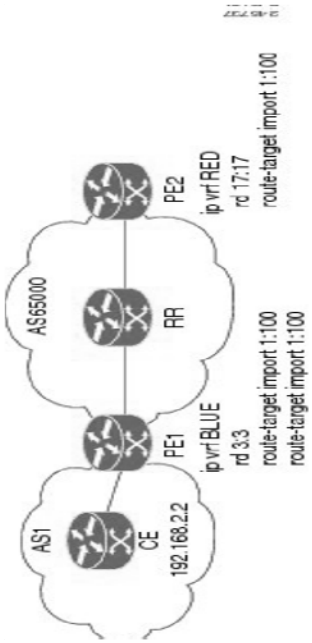

Figure 4 (Constrained Route)

5. Resource Reservation

In order to secure promised services, it is not sufficient simply to select a route that can provide the correct resources. These resources must be reserved to ensure that they are not shared or "stolen" by another LSP. The traffic requirements can be passed during LSP setup (as with constraint-based routing). They are used at each LSR to reserve the resources required, or to fail the setup if the resources are not available. Figure 5 shows MPLS resource reservation process.

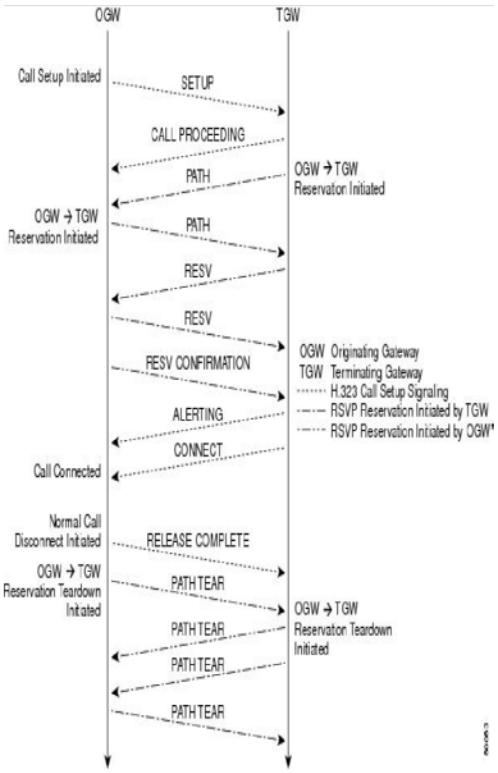

Figure 5 (Resource Reservation)

6. Traffic Engineering

Traffic Engineering is the process where data is routed through the network according to a management view of the availability of resources and the current and expected traffic. The class of service and quality of service required for the data can also be factored into this process. Traffic Engineering may be under the control of manual operators. They monitor the state of the network and route the traffic or provision additional resources to compensate for problems as they arise.[11][12][13] Alternatively, Traffic Engineering may be driven by automated processes reacting to information fed back through routing protocols or other means. Figure 6 below an extensive MPLS traffic engineering.

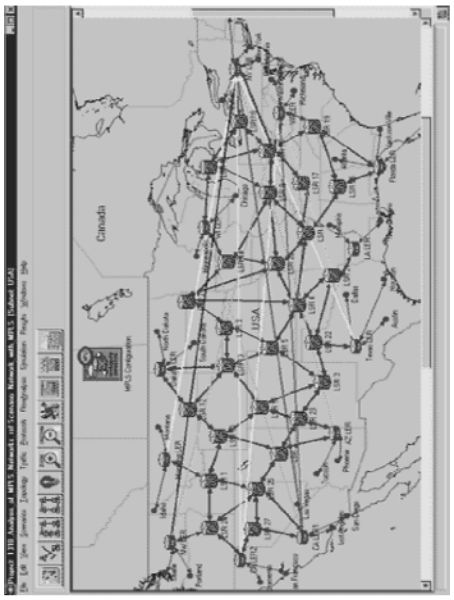

Figure 6 (Traffic Engineering)

7. Service Level Contracts

Many uses of the Internet require particular levels of service to be supplied. For example, voice traffic requires low delay and very small delay variation. Video traffic adds the requirement for high bandwidth. Customers increasingly demand service contracts that guarantee the performance and availability of the network.[14] In the past, in order to meet these requirements, network providers have had to over-provision their physical networks. MPLS offers a good way to avoid this issue by allocating the network resources to particular flows using constraint-based routing of LSPs.

8. Virtual Private Networks

A Virtual Private Network (VPN) allows a customer to extend their private network across a wider public network in a secure way. ISPs offer this service by ensuring that entry points to their network can exchange data only if they are configured as belonging to the same VPN. MPLS LSPs provide an excellent way to offer this service over an IP network.

9. Meeting the Needs of the Modern Network

VPNs have been addressed with additions to the BGP routing protocol, but IP has not provided good solutions to the requirements set out in the previous three sections. There has been no way of providing a guarantee of service, because the network is connectionless. Destination-based routing along shortest path routes tends to overload some links and leave others unused. A popular solution is to use an overlay network, for example running IP over ATM PVCs. This is notoriously hard to manage, because many resources must be configured at each router in the network, and because there are two distinct protocols to be configured. It also leads to scaling issues, with an order of n2 connections needed in a network with n nodes. MPLS allows the use of just one set of protocols in the network. Using MPLS to meet the aims described in the previous three sections while avoiding the problems described above requires a label distribution protocol that supports Explicit Routes and constraint-based routing. There are currently two label distribution protocols that meet this definition: CR-LDP and RSVP. There is a debate about which of these protocols is preferable, which is most suitable for particular scenarios, and whether it is necessary to implement both of the protocols in an MPLS network. Since the LSPs set up to support Traffic Engineering, Service Contracts and VPNs are all configured in the same way for RSVP and CR-LDP (through the Traffic Engineering MIB), they are referred to as Traffic Engineered LSPs.

10. Conclusion

Link failure is a common cause of service disruption in computer networks. Many techniques have been developed to alleviate the consequences of hardware failure in a network like the Internet by rerouting traffic from a failed link to a working or a set of working links. Rerouting is performed automatically in the Internet by recomputing routing tables. However routing convergence may be slow and faster techniques which require expensive hardware have been developed to protect networks from link failures. MPLS is a recent virtual circuit packet switching technology which has been designed to support the forwarding of IP packets over virtual circuits. MPLS Fast Reroute is a traffic engineering technique that is able to reroute IP traffic quickly without the need of additional hardware. Indeed, MPLS Fast Reroute relies on pre-planned backup path to reroute traffic on a link failure and can be implemented in existing routers. An important delivery mode of the Internet is multicasting, where the information sent by a member of a multicast group is received by all other members of the group. A popular example of a multicasting application is teleconferencing. In real-time applications like teleconferencing, if a link failure occurs, it is crucial to repair the multicast routing tree of the multicast communication in a short time. For example, an interruption of service of more than 50 ms is noticeable in a live transmission. Establishing a backup path to protect a multicast routing tree is a resource consuming process. Therefore, it is

desirable to protect a large number of members of a multicast group with a low number of backup paths. In this thesis, we presented an algorithm which is able to choose such a backup path, and the design and implementation of an MPLS-based rerouting mechanism adapted to the protection of multicast routing trees. We now review our contributions and expose possible future work.

References

[1] 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_profile0900aecd801aa3f5.html

[2] 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

[3] 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

[4] 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%20T

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

[10] Sprint Nextel, Inc. (2006, January). *Sprint Global MPLS VPN IP Whitepaper*. Retrieved November 19th, 2007, from http://whitepapers.techrepublic.com.com/thankyou.aspx?authId=uqqOzCBTkk7ekSZjOPwgf9Z5C6ZJWyXLNMi0MVnKEADJ90SewjXUM22n4A2PUWMB&&q=Sprint+Global+MPLS+VPN&docid=273906&view=273906&load=1

[11] 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

E%20overview%20cisco&docid=177738&view=177738&load=1

[5] 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?repoid=Topic&rtype=Whitepaper&rvalue=eb_fpoc_navigating_to_mpls_enabled_networks&repoitem=vpns&segment=ent_biz http://www.ietf.org/html.charters/rsvp-charter.html http://www.ietf.org/html.charters/mpls-charter.html

[6] 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?repoid=Topic&rtype=Whitepaper&rvalue=understanding_vpn_technology_choices&repoitem=vpns&segment=ent_biz&guid=4BFDAE84-C61B-416F-886A-F606E9678B1C;08905D72-1FE7-450C-8EA5-B5F1565DD558

[7] 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

[8] 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

[12] 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

[13] 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

[14] 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=Pseudowire&oldid=172121304