INTEGRATION OF NETWORK TECHNOLOGY MPLS BASED VPN: A MODEL FOR ESTABLISHING VIRTUAL LEARNING FACILITY FOR MULTIPLE LOCATIONS

Mohankumar C. Kaimal*

Abstract:

Multi Protocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs voice, video and data on the internet from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay and DSL. MPLS based Virtual Private Networks (VPN) tie together give the flexibility to transport and route several types of network traffic using the technologies of a MPLS backbone.

Multi Protocol label Switching (MPLS) is a core networking technology that operates between Layers 2 and 3 of the OSI model. Sometimes it is also referred to as a layer 2.5 technology. It is basically a framework for WAN. MPLS is a highly evolved than its predecessors Frame relay and ATM in terms of providing solution for VPN, QOS, network convergence, security, traffic engineering etc. As a result, today MPLS is widely used in supporting applications like voice, video and data on the internet. Most service providers are migrating their backbone network from traditional Frame Relay and ATMs to MPLS. MPLS is a technology which is here to stay for a long time. This report basically deals with the implementation of MPLS as VPN service, how it is implemented, maintained, pros and cons.

Keywords: *Multiprotocol Label Switching, Virtual Private Network, Internet Protocol, Voice, Video, Data, Bandwidth, Network Technology,*

* Assistant Professor, Department of Lifelong Learning & Extension, University of Mumbai.

1. Introduction:

1.1 History of VPN: As the popularity of Internet kept on increasing, Internet Protocol (IP) became the most popular protocol. It started with leased-lines, intranets and extended to Virtual Private Networks as we now fondly call them as VPNs. The success of intranets within business and the success of the Internet as a means for interconnecting different intranets to form a single, global network have played a key role in making many Institutes/Companies create their own VPN to accommodate the needs of remote Colleges and distant Offices. (Lin A & Gleeson B, 2000)

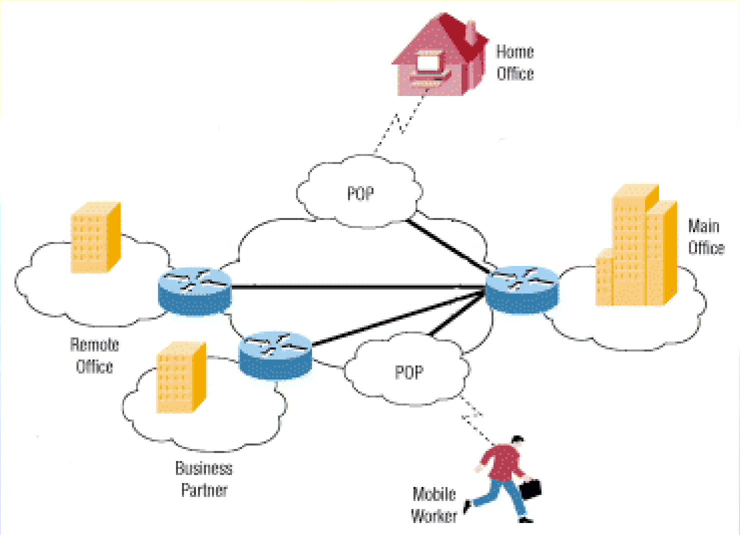

Figure 1: Image courtesy Jeff Tyson on How VPN works

Before the inception of MPLS, the most popular WAN protocols were ATM and Frame relay. These were predominantly layer 2 technologies. The disadvantages associated with this overlay models were

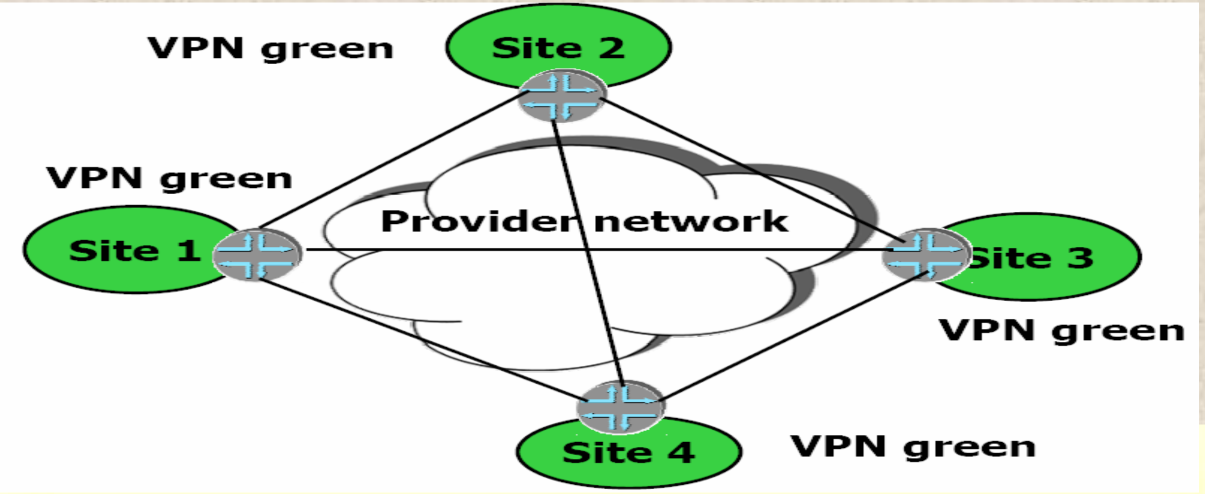

Figure 2 Typical Overlay Model Site 1, Site2, Site3, Site4: Customer network on VPN

1) Frame-relay and ATM needed virtual circuits to be established (Source-Destination path behaves much like a telephone circuit).Typical problems included

- Virtual circuit set up, maintenance & teardown,
- Packet carries virtual circuit identifier and not destination IP address
- High cost, complexity of meshed configuration, network delays, remote access issues

2) Each customer site peers with every other customer site.

Site 1 needs peering with site 2, 3 & 4. Number of connections (n*(n-1)/2)

- If a new site (site 5 is added) it would need to peer with site 1, 2, 3 & 4 and configuration changes on all sites
- Potential configuration issues if multiple (for example 10) new sites to be added
- Increased cost, complexity of maintenance and troubleshooting

1.2 Advantages of MPLS (Ghein, 2006 Nov) (Guichard, 2002 May)

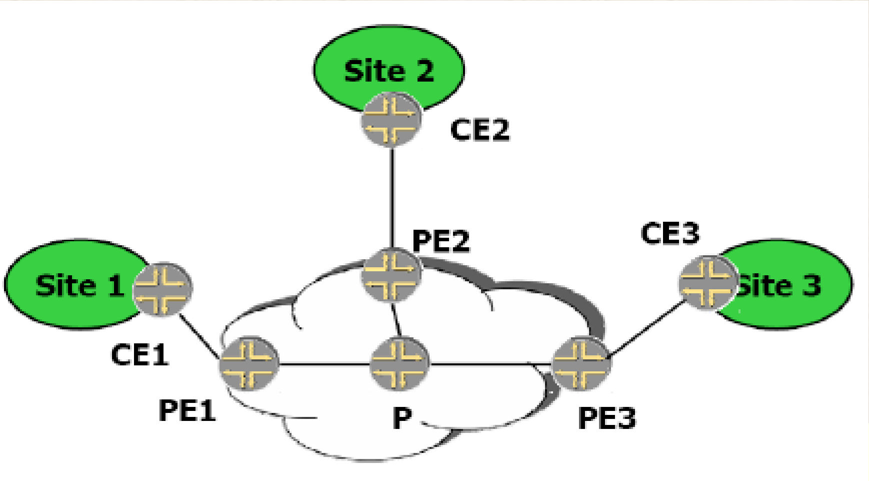

Figure:3 Typical Peer Model

PE1, PE2, PE3: Provider Edge routers CE1, CE2, CE3: Customer Edge routers

Site 1, Site2, Site3: Customer network on VPN

MPLS basically uses a peer model. There are various advantages of using a peer model.

1) Customer router peers with a Provider router and not with other customer routers

- Customer Edge (CE1) router peers only with Provider Edge (PE1) router and not with CE2 and CE3

2) Adding a new site requires configuration only at the Provider edge router

- If a new site (site 4 is added) configuration changes only on Provider Edge (PE)router
- No configuration changes or modifications on CE1, CE2 & CE3

3) No need to establish a dedicated/virtual circuit from source to destination

4) Packet carries following information

- Destination IP address
- Quality of Service(QOS) and Class of Service (COS) parameters

- ❖ Less network delays as no circuit establishment, maintenance and teardown process needed

1.3 Development of MPLS:

MPLS was basically developed to integrate the best qualities of pure packet, frame and cell switching with the best quality of IP routing. Like frame and cell switching, MPLS is based on use of short, fixed length labels in a fixed length packet header. The label summarizes the following information about how the packet travels through the

MPLS network including:

- ❖ Destination address
- ❖ Precedence
- ❖ VPN membership
- ❖ QOS either using RSVP or DSCP

VPN services are a very good example of how to extract optimum utilization of MPLS from both the world routing and switching. The combination of MPLS and multi-protocol BGP (MP-BGP) makes MPLS based VPN service very manageable, straightforward and helps maintain VPN sites along with their membership for customers at multiple locations.

Another important feature of MPLS is that it allows the routing table of internet to be constrained. In the sense only the edge router needs to perform all the routing look-ups and, the core routers just perform task of label switching.

2. <u>MPLS Architecture:</u> (E. Rosen & A Vishvanathan Jan 2001) (Black, 2002 April) (Peter, 2002)

MPLS has two major elements:

1) Control Plane:

It looks after routing information exchange and label binding information exchange. It performs Layer 3 routing or Layer 2 switching in addition to switching labeled packets.

2) Forwarding Plane: It is responsible for forwarding packets based on labels attached. It uses LFIB to forward labeled packets.

Following are the key components of the MPLS architecture -:

1) MPLS Labels

0 19 22 27 31

Label	EXP	BOS	TTL

a) Bottom of Stack (S): This bit is set to one for the last entry in the label stack (i.e., for the bottom of the stack), and zero for all other label stack entries.

b) Time to Live (TTL): This eight-bit field is used to encode a time-to-live value.

c) Experimental Use (EXP): This three-bit field is used for encoding TOS values or DSCP values

d) Label Value: This 20-bit field carries the actual value of the Label. It gives information about next hop to which packet would be forwarded.

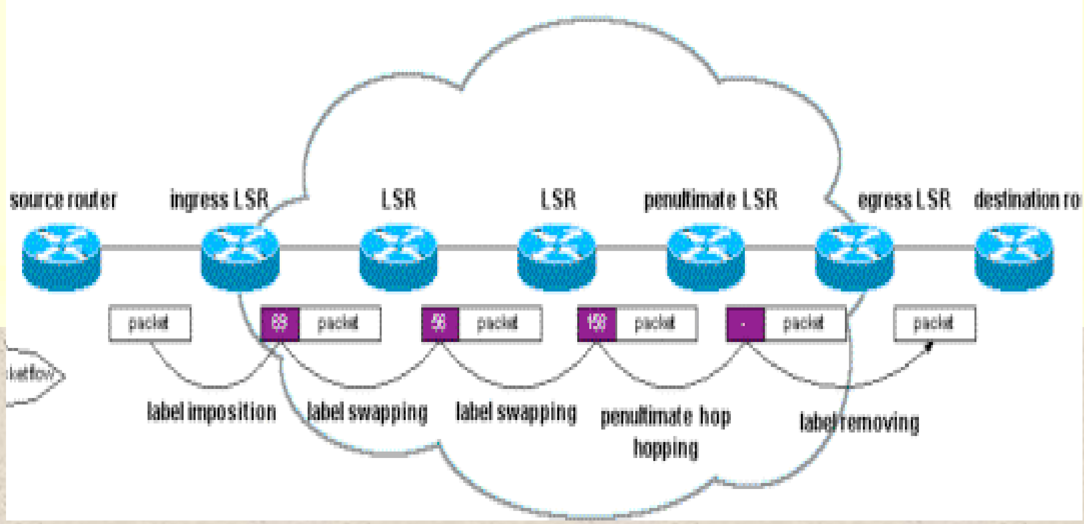

Figure: 4 Label Switched Path

2) Label Switch Path: In MPLS networking, a Label Switched Path (LSP) is a path through an MPLS network, set up by a signaling protocol such as LDP. The path is set up based on criteria in the forwarding equivalence class.

3) Ingress Label Switch Router (LSR): It is basically the router that is on the edge of the network. This router receives a packet from the outside world and assigns a label to it and forwards it on the link.

4) Egress Label Switch Router (LSR): This router is the other end of MPLS network. It receives a labeled packet. It pops the label off and forwards it to destination.

5) Intermediate Label Switch Router (LSR): These are the routers within the MPLS network. They receive a labeled packet and their operation is to only swap labels and switch the packet.

6) Forwarding Equivalence Class (FEC): A Forwarding Equivalence Class (FEC) is a group of destination routes, services, QOS parameters or a combination of these attributes which share a common path in MPLS domain.

7) Label Distribution Protocol (LDP): Label binding information between LSR is exchanged with the help of Label Distribution Protocol (LDP). It is basically run between adjacent LSR and is used to exchange label

–to-FEC mapping. LSR basically establishes a session between them and form peers. After they form pees they exchange information about label assignment on label switched path.

8) Label Information Base (LIB): The LIB stores all the labels that have been advertised by other LSRs in MPLS network. LSR can exchange the mapping of labels using LDP, MP-BGP 9) Label Forwarding Information Base (LFIB): The LFIB cache is used for the actual packet forwarding process. It contains information like incoming label value, outgoing label value, prefix/FEC, next hop. If a MPLS LSR needs to forward a packet it will consult this cache in order to find out on which next-hop interface must the packet be sent.

Label Operation (Ghein, 2006 Nov) (E.Rosen & D. Tappan, 2001)

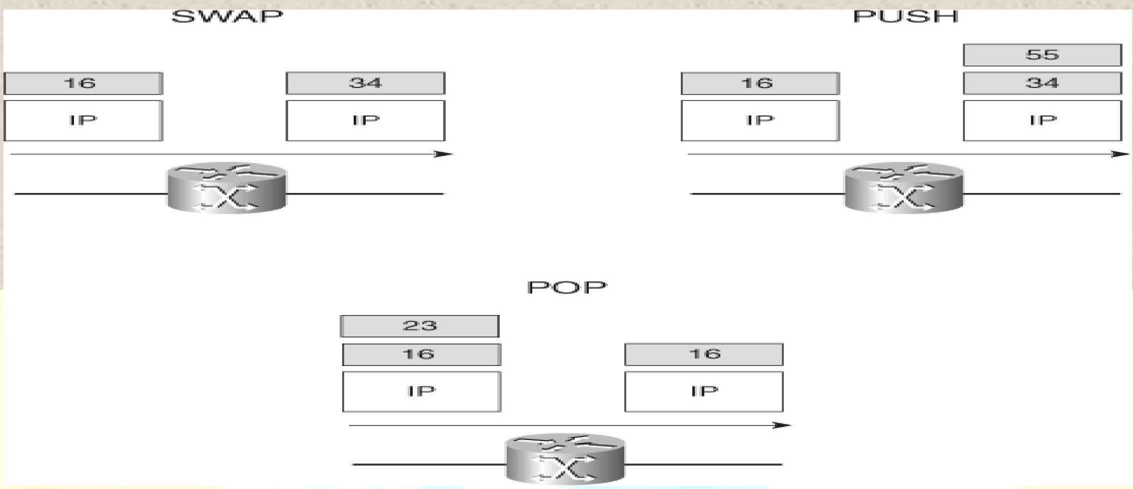

Figure: 5 Label Operation Example

The possible label operations are swap, push, and pop. By looking at the top label of the received labeled packet and the corresponding entry in the LFIB, the LSR knows how to forward the packet.

The LSR determines what label operation needs to be performed—swap, push, or pop—and what the next hop is to which the packet needs to be forwarded. The swap operation means that the top label in the label stack is replaced with another, and the push operation means that the top label is replaced with another and then one or more additional labels are pushed onto the label stack. The pop operation means that the top label is removed.

- Pop—The top label is removed. The packet is forwarded with the remaining label stack or as an unlabeled packet.
- Swap—The top label is removed and replaced with a new label.
- Push—The top label is replaced with a new label (swapped), and one or more labels are added (pushed) on top of the swapped label.
- Untagged/No Label—The stack is removed, and the packet is forwarded unlabeled.
- Aggregate—The label stack is removed, and an IP lookup is done on the IP packet.

2.1 Architecture Example:

The MPLS operation can be explained with help of below diagram. LSR 1----Ingress LSR LSR 2 ---- Intermediate LSR

LSR 3 & 4----Egress LSR

The packet enters the MPLS network through network A. The ingress LSR assigns labels to the packet In the below example destination B, C, D & E are assigned labels 1,9,8 &3. If the packet is destined for Network B, LSR 1 assigns label 1 to it. When the packet reaches LSR 2 it sees the label 1 and performs a lookup in LFIB and if it finds a match, it will swap the label with a new label an appropriate next hop and transmit the packet to LSR.

3 Here the label is swapped from 1 to 5.This packet when reaches LSR 3, as they are egress LSR they remove the MPLS header from the packet and transmit the packet to outside network without any labels.

The Egress LSR performs two functions.

The first is popping the label so the packet goes to outside world without labels and second is routing lookup to forward the packet to appropriate destination.

3. <u>MPLS VPN Terminology</u> (Guichard & Pepelnjak, 2002 May)

1) Provider Edge Router (PE router):

This router is a part of provider network with which the customer router peers. It is the edge router on provider network.

2) Provider core router (P router):

These are the internal/intermediate routers in the provider network. These routers need not have information about the customer routes.

3) Customer edge router (CE router):

This is the edge router on customer network with which the PE router peers.

4) Provider network (P network):

This is the backbone network controlled by service provider

5) Customer network (C network):

The network owned by customer is called C network

6) Site: This is the part or set of sub networks that customer owns. For example a company XYZ has its offices in New York and Washington DC, New York office can be site A and Washington DC office can be site B.

4. Architectural Ingredients of MPLS VPN (Ghein, 2006 Nov)

1) Virtual routing and forwarding table (VRF):

The advent of VRF has been a great added advantage to MPLS VPN. The VRF can be considered as separate routing and forwarding table in PE router. A PE router has a vrf instance for each attached VPN. For example if the ISP has multiple customers suppose ABC XYZ, PQR. Because the routing should be separate and private for each customer, Each customer would have a separate instance of vrf in PE router so thus preventing leaking of routes from one customer to another.

2) Route Distinguisher (RD):

Ipv4 address space is limited. The problem is when customer had overlapping IP addressing, the routing would be wrong. For example most companies use private addressing for their internal network to prevent use of public addresses. It can be quite possible that two companies may have same internal address space 192.168.10.0/24. To prevent the customer routes from getting routed wrongly MPLS consists of 64-bit field called as Route Distinguisher. RD= 16 bit type + 48 bit value

64 bits RD	Ipv4 address 32 bits

The RD is only used to make Ipv4 address unique. Generally (ASN: IP Address) Autonomous system number is included in the RD value field to make an unique 96-bit address for each VPN. 64 bit –RD + 32 bit IP address = Unique VPN route

3) Route Target (RT):

Route Targets are generally used to control the policy of who sees what routes. Typically carried as an extended BGP community. It is a 64 –bit quantity. For example, there are two companies A and B and both have sites X and Y. Sites X and Y of A can talk to each other and similarly for company B but Site X and Y of company A cannot talk to X and Y of B. If in case you need site X of A to talk to site X of B, route target comes into picture. In that case routes will be exported to remote PE and also imported from remote PE in order to make it work.

4) BGP: BGP version 4 is the protocol for the internet. It is well suited to carry thousands of routes and that is why it is a good candidate to carry MPLS VPN routes. As the packet traverses along the MPLS network it has two labels associated with it

a) IGP Label: It is the top label in the stack. It is a label that is bound to Ipv4 prefix in the routing table. It gives the information about next hop to packet.

b) VPN Label: The bottom label is VPN or BGP label. This label usually indicates the next hop a packet should take after reaching egress PE router.

To sum it up IGP label is used to forward the packet to the correct egress PE router while the egress PE router uses VPN label to forward the IP packet to correct CE router.

4.1 Route Exchange between PE and CE routers: (AT&T, 2007 August) The connection between Provider Edge (PE) and Customer Edge (CE) routers can be established in multiple ways. The protocols used to establish connection are

1) Static Route: Customer can use a static route to point to PE edge router and vice-versa for the provider. The main advantage is ease of configuration. This solution would be a good fit if there is only one link from customer site to provider edge.

2) Routing Information Protocol Version 2 (RIPv2): As RIPv2 carries subnet information in the packet; this was the main reason why it was chosen over its predecessor RIPv1. The main advantage is easy configuration and good choice for small sites.

But as its metric is hop count and it has longer convergence time it is not a good fit for large sites.

3) Open Shortest Path First (OSPF):

It is a good choice if existing network of customer is running ospf. So he doesn't have to configure redistribution and other complex stuff. This could be easy on CE edge but PE edge maintains multiple VRFs for various customers. It would consume significant processor memory.

4) External BGP (E-BGP):

This is supposed to be the best choice for CE-PE connection. As BGP is used to maintain communication between different Autonomous systems and also running multiple VRFs on PE router would not affect processor memory if you have BGP running. It can support thousands of routes.

4.2 Route Distribution among PE routers: (AT&T, 2007 August)

PE routers are all located in a single autonomous system, configured as fully meshed and are running internal BGP. The generally run the upper version of BGP which is MP-BGP. They have MP-iBGP session between them. The P routers just perform the work of label swapping and switching. They do not have any information of customer routes. PE routers make us of VPN label which is forwarded by MP-iBGP from PEPE to reach the appropriate customer.

With the help of MP-iBGP it is possible to

1) advertise a feasible route to peer

2) withdraw multiple unfeasible routes

3) advertise next hop to destinations listed in NLRI P routers use IGP label to forward packet to correct PE router.

5. Quality of Service in MPLS VPN: (Cisco Systems, 2006)

QOS is the overall performance of the network supported by SLA. Terms used in discussing QOS includes packet loss, availability, jitter and latency. Any network that is designed must provide secure, predictable, measurable and guaranteed service. Especially you need to take care in applications which are time sensitive. For example if you have voice, video, data, file sharing etc and other traffic in your network. Voice and video being time-sensitive, it cannot withstand a jitter or delay above 150 ms. If voice is given the lowest priority or no prioritization is observed, voice traffic may suffer.

There are different ways to provide QOS in MPLS network:

1) Integrated Services: In this case, applications signal to the network that they require certain QOS parameters. It uses Resource Reservation Protocol (RSVP) to reserve resources for QOS parameters. In these method characteristics such as bandwidth delay and packet loss rates are guaranteed end-end. End-end streams are not established if required QOS parameters are not available.

2) Differentiated Services: It provides high scalability and flexibility in implementing QOS in a network. It helps in designing customized QOS tailoring to customer needs.

The traffic can be classified based upon

- ❖ Incoming interface :
- ❖ IP precedence

- Differentiated services code point (DSCP)
- Source or Destination address
- Application

You can also make use of different queuing algorithms like

- First In First Out (FIFO)
- Priority Queuing
- Round Robin
- Class based weighted fair Queuing
- Low latency Queuing

6. Class of Service (COS): (AT&T, 2007 August) (At&T COS, 2006 Sept)

There should be some mechanism while using MPLS which supports division of (Metzler, 2006 March) bandwidth especially for real time applications without the risk of downtime. This functionality is provided by Classes of Services. Without COS your bandwidth is not allocated meaning a large transmission has the potential to slow other data down. For example a large voice or video transmission could eat up a considerable amount of your bandwidth slowing your other applications. Similarly if you do a large file sharing via FTP, then that file sharing could hold up the bandwidth from other applications. With COS you can set bandwidth limits allocating highest bandwidth to time sensitive applications and remaining bandwidth to share across different applications.

COS allows you to choose a profile that allows you to choose your bandwidth according to your company needs. For example if your company runs most on voice and video applications you can allot most of the bandwidth to these applications The typical profiles into which Class of Service is divided are • Real Time (Voice and Video)

- Video

- Business critical
- Best effort

Class of Service provided by different service providers in the market

6.1 Verizon Business COS Profiles (Metzler, 2006 March) (Fischer)

1) Expedite forwarding (EF): This is the class with highest priority.

Generally voice traffic is allotted this class. Any traffic marked as EF assumes highest priority

2) Assured forwarding (AS4): This is class below EF. Typical applications that fall under this class is video.

3) Assured forwarding (AS3): This is class below AS4. Typical applications that fall under this class are business critical like SAP, citrix

4) Assured forwarding (AS2): This is class below AS3. Typical applications that fall under this class are general data applications, telnet etc.

5) Best Effort: This is class below AS2. Typical applications that fall under this class are email, web surfing. It has lowest priority.

6.2 AT&T COS Profiles: (Metzler, 2006 March) (Fischer)

AT&T typically provides 4 class of service with two classes supporting further sub categorization of service. The typical ones are listed below

1) COS 1: This class is assigned to real time applications like voice and video

2) COS 2: This class is intended for mission critical and bursty data applications with priority AF 31

3) COS 3: This class is intended for mission critical and bursty data applications with priority AF 21

4) COS 4: It is referred to as the Best effort class. The data transmission is not guaranteed.

6.3 Sprint COS Profiles:

1) Platinum Queue : This class carries premium traffic like voice

2) Gold Queue: This class carries video traffic

3) Silver Queue: This class carries business traffic

4) Bronze Queue: This class carries best effort data traffic

6.4 Service Level Agreement (SLA)

A service-level agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish. Many Internet service providers provide their customers with an SLA. The different areas on which SLA is provided are

- Network Availability SLA
- End to End Delay SLA
- End to End packet loss SLA
- End to End Jitter SLA
- Internet AvailabilityTypical values are (Sprint, 2009)
- Committed network Round Trip delay : Less than 55 ms
- Committed network packet Loss :0.30%
- Committed network jitter: Lesthan 2ms.
- Data Delivery rate : 99.7%

7. Drawbacks of MPLS:

7.1 SECURITY (Fischer, 2007) As MPLS is becoming a widely used framework for WAN protocols, as a result security threats are also increasing. MPLS architecture security is a concern for both service provider and customer. There can be several cases of threats not just from outside world but inside threats, unauthorized access etc. MPLS provides excellent VPN service but it does not have any mechanisms to encrypt the traffic and maintain the integrity of traffic. Following are the key locations where attacks are most prone.

1) Protecting the MPLS core structure: The internal structure of MPLS core which consists of PE and P routes should be hidden from the outside world. This information should also not be leaked to customer VPN as customer it can be compromised leading to hacking of the service provider eventually. The only information to be provided must be PE routers IP address to peer with CE router.

2) Label Spoofing: It can happen that wrong labels being inserted into MPLS network from the outside world. This can be typically done from CE VPN. To avoid this PE router must never accept a packet with label from CE router.

3) Label Information base poisoning: Label distribution protocol is generally not encrypted. If MPLS devices accept label routing information from outside world, it may be quite possible that attacker may manipulate the Label information base. With this attacker could achieve Dos attacks.

7.2 SOLUTION:

1) CONFIDENTIALITY:

Confidentiality can refer to a number of areas, including, confidentiality of LIB, traffic passing through infrastructure etc. The solution to this problem is using of encrypted protocols and what better option than IPSEC. IPSEC can be used in conjunction with MPLS to provide high level of encryption.

By using IPSEC you can achieve

- encryption on all or parts of traffic on MPLS core
- Authentication of endpoints
- Integrity of traffic
- Confidentiality of information

2) INTEGRITY:

It is a key thing to maintain the integrity of data of customer that is passing through the MPLS backbone. Also integrity of LIB, LDP must be maintained. In MPLS routing information is exchanged using BGP routing protocol. It offers to deploy MD5 authentication. Wherever possible these authentication mechanisms should be deployed to maintain integrity. With use of MD 5 authentication every packet in TCP session a field is added with MD5 checksum value and cryptographic key. Without knowing the key it is nearly impossible to construct a packet with a valid signature. Other Security Recommendations:

- CE – PE interface: Secure using ACLs
- Static PE – CE routing where possible
- If routing using (BGP) use MD5 authentication
- Implementing strong firewall policies
- Use of Network Address Translation

8. Project on MPLS VPN:

Below is a schematic representation of a project design on MPLS VPN.

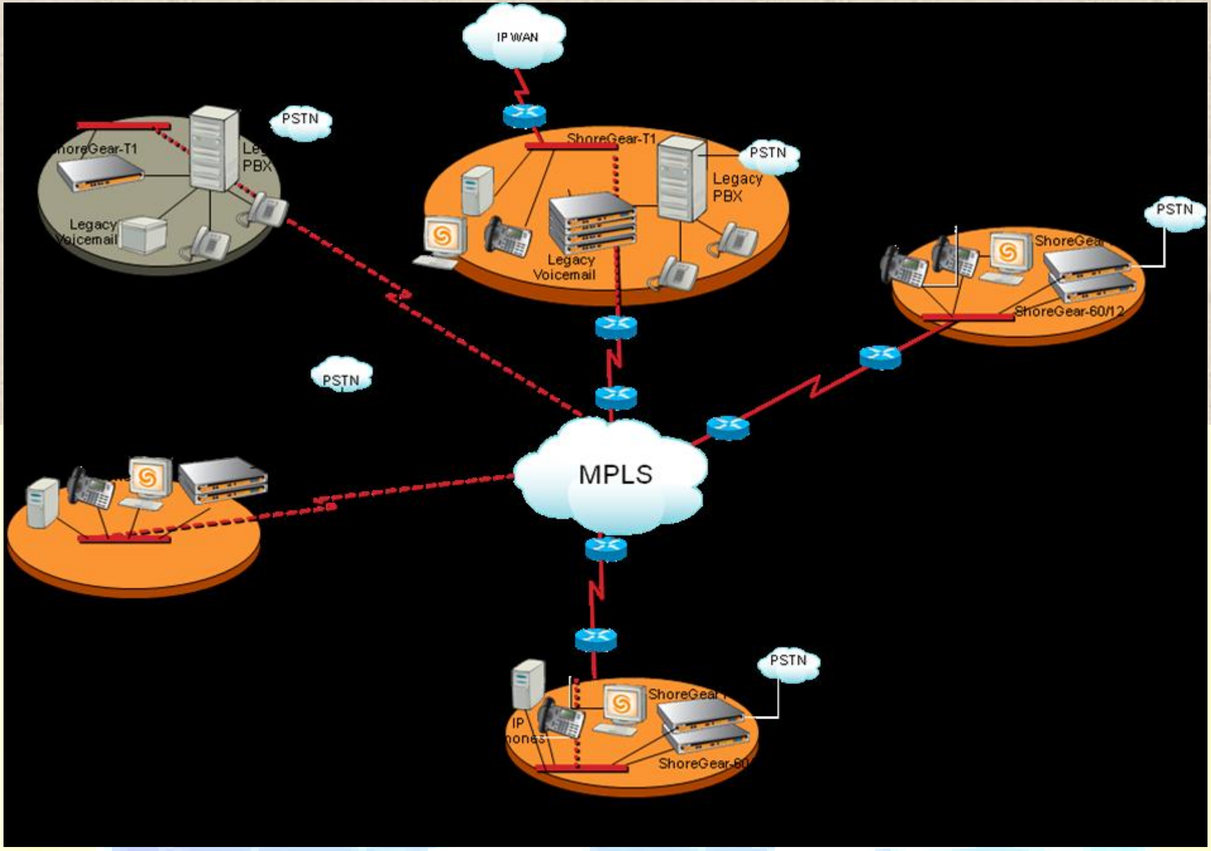

Figure: 7 MPLS Site Connectivity

CONCLUSION:

The main goal of this design is to move the current WAN network of an Institute to MPLS-VPN through the ISP backbone and connect their sites at multiple locations. The existing network may be a Layer 2 VPN and it may be a very good challenge and learning experience if we put together and explore the design into reality. The key values remembered while designing these projects were;

Main objectives and system definition of project and

a) Key Deliverables b) Technical requirements

c) Reviews with the system needs d) Build & maintain a cohesive team

e) Above all PLANNING

To suit the need of an Institute having multiple location as study centre's offering distance and open learning platform and to impart training through virtual classroom and received at multiple locations. The Technology suggested here will be able to connect multiple study canters on the virtual classroom setup enabling students in rich learning experience. A highly interactive platform that uses video conferencing technology and that makes it a most innovative teaching and training method. The high quality services to feel like a real classroom wherein students interact face to face with the professor-seeing, hearing, and asking questions Students' interaction at just 100 kbps bandwidth.

The web based Video Communications with Interactive Streaming of live/recorded sessions with moderated interactivity at very low Bandwidth & with High Quality Resolution. An audio/video feed is supplied from a webcam or a digital camera or a professional camera to the encoder and then the feed is sent to the cloud (connectivity 50-256 kbps). Now, Virtual classroom cloud distributes it among the study canters and thereby student benefit with the live classroom environment. This would also allow distance accessible courses use virtual classroom for learners to interact in real time with both video and audio. Then using a computer watching and listening to a meeting/session or lecture on the internet on interactive mode is all about designing this Integration of Network Technology MPLS based VPN model for multiple locations establishing Virtual learning facility.

REFERENCES MPLS Based VPN

- AT&T. (2007 August). *MPLS Private Network Transport Customer RouterConfiguration Guide Release 4.* AT&T Knowledge Ventures.
- Black, U. (2002 April). *MPLS and Label Switching networks.* Prentice Hall.
- COS, A. (2006 Sept). *AT&T Network Based Class of Service Customer Router Configuration Guide.* AT&T.
- E. Rosen, A. V. (2001, Jan). *Multiprotocol Label Switching Architecture RFC 3031*.Retrieved from http://www.ietf.org/rfc/rfc3031.txt
- Fischer, T. (2007, Dec). *MPLS Security Overview*. Retrieved from White Paper for Public Distribution: http://www.irmplc.com/downloads/whitepapers/MPLS_Security_Overview.pdf

- Ghein, L. D. (2006 Nov). *MPLS Fundamentals.* Indianapolis: Cisco Press.
- Guichard, I. P. (2002 May). *MPLS and VPN Architecture*. Cisco systems.
- Lin, B. G. (2000, Feb). *A Framework for IP Based Virtual Private Networks*. Retrieved from RFC 2764: http://www.ietf.org/rfc/rfc2764.txt
- Management, S. (2005, Jan). *Sprint MPLS VPN IP White paper*. Retrieved from Spring Product Management: http://www.sprintworldwide.com/english/contact/MPLS_VPN_WP.pdf
- Metzler, J. (2006 March). *Innovation in MPLS Based Services.* www.kubernan.com.
- Peter, T. (2002). *MPLS Based VPn.* Prentice-Hall.
- Rosen, E. (2001, Jan). *MPLS Label Stack Encoding RFC 3032.* Retrieved from http://www.ietf.org/rfc/rfc3032.txt Sprint. (n.d.). *Sprint MPLS VPN.* Retrieved from https://www.sprint.net/sla_performance.php
- Systems, C. (2006). *Optimizing Converged Cisco networks Volume 1*. Cisco Press.
- Wu, G. (n.d.). Lecture Notes. http://teal.gmu.edu/~yqwu/bgp/MP-BGP.pdf.