RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of WAN Technologies

Er.Harsimranpreet Kaur [1], Er.Rupinder Kaur Gurm [2]
Research Scholar (M.Tech) [1], Assistant Professor [2]
Department of Computer Science and Engineering
RIMT-IET, Mandi Gobindgarh
Punjab - India

ABSTRACT

This paper shows the performance analysis of three very popular WAN technologies i.e. Dynamic Multipoint VPN (DMVPN), Multiprotocol Label Switching (MPLS) and Frame Relay. DMVPN is slightly different than the other MPLS and Frame Relay as with DMVPN we can connect our sites at different locations over internet while for MPLS and Frame Relay, we typically need to go to ISP to deliver us the services. But with Dynamic Multipoint VPN, we can create a VPN within our different branch sites over Internet. This paper provides the performance analysis comparison between DMVPN, Frame Relay and MPLS. It also provides the Security Analysis.

Keywords **:** DMVPN, MPLS, NHRP, LDP, LSP, LFIB, LIB, LMI, PVC, DLCI, RT, RD, VRF

I. INTRODUCTION

WAN is a type of network that spans a large geographical area which uses Service provider network as a transit point or uses service provider's infrastructure to connect two sites at distant locations. WAN is created to connect two or more LANs at remote locations. WAN Technologies mostly functions at lower layers of OSI Model, For example : Frame Relay, ATM, HDLC, PPP etc works at Data Link Layer, MPLS works at 2.5 layer of OSI Model and has the ability to create both Layer 2 and Layer 3 Virtual Private Networks . Several more solutions for WAN are IPSEC VPN, SSL VPN, DMVPN.

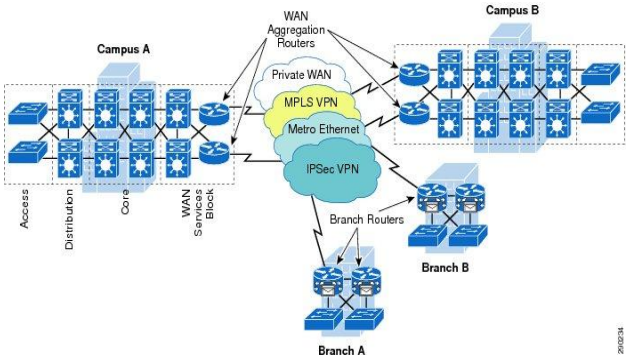

Figure 1.1 - WAN Model

A WAN is mostly owned by a service provider and enterprises pay to them for their branch offices or data centers interconnection. WAN providers can be telephone network company,

cable company etc. Enterprises pay fee to service providers in order to use their infrastructure for interconnection of

their branches or sites to transport data, voice and video. Users can easily connect with their banks, ecommerce sites, e-book libraries etc using Internet.

1.2 ***Dynamic Multipoint Virtual Private Network(DMVPN)*** - DMVPN is a Cisco proprietary solution works on Cisco Devices for creating VPNs in a very easy manner. It is highly scalable and dynamic in nature. It uses IPsec and GRE to create VPNs. DMVPN works with two proven technologies :

Next Hop Resolution Protocol(NHRP) - Below is the fixed header of NHRP captured in Wireshark :

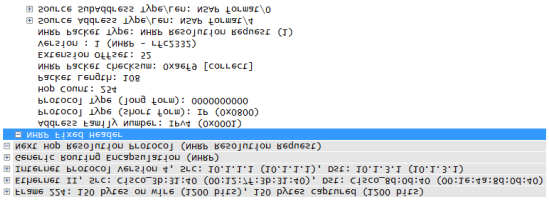

Figure 1.2 - Wireshark capture of NHRP Header

It creates a distributed mapping database of all the spoke tunnels to their public interfaces which has the actual real addresses. Figure below shows the NHRP request - reply illustration :

Figure 1.3 - NHRP Request-Reply Mechanism

Multipoint GRE Tunnel Interface : By default, when a tunnel is created, mode of the tunnel is GRE and it works in point-to-point nature when no changes are made. It has the ability to support multipoint behavior. Therefore a single GRE interface can support multipoint GRE IPsec tunnels, and the best thing with this feature is that it makes configuration less complex and new sites or spokes can be added to the hub site without making any configuration changes in the Hub configuration, which just simplifies the size. Spoke to spoke tunnels are made over multipoint GRE interface. Each spoke having a permanent IPSec tunnel created to hub, all spokes got registered itself to the Hub or NHRP server. When a spoke wants to send a packet to another spoke, it sends a query to the NHRP server for the actual address of the spoke. And when the originating spoke learns the peer address of the destination spoke, it then creates a dynamic IPSec tunnel with the destination spoke. Therefore spoke to spoke tunnels are created on demand whenever some traffic is sent between them. Only the first packets go over the hub afterwards when source spoke learns the outside address of destination spoke and creates a tunnel between them, packets are sent spoke to spoke bypassing hub.

Benefits of DMVPN

- Configuration Reduction - Configuration can be reduced with new sites configuration is needed on the spokes only and no configuration is needed on the Hub Router. Suppose a company named ABC has a single Hub site in New York(USA) and three spokes in Bengaluru(India), Berlin(Germany) and Sydney(Australia). Company ABC plans to start three new branch offices around the world in London(UK), Beijing(China) and Tokyo(Japan), and they want all their offices to be connected with each other, with DMVPN, we need not to do any configuration on Hub Router or other three spokes and configuration is needed to be done only in new three Branch Offices, so it can be like no-touch deployment. Spoke to Spoke traffic can be sent via Hub or it can be sent directly to the spoke with multipoint gre tunnels configured on spokes.

- Supports IPv4/IPv6 Unicast, Multicast, and dynamic routing protocols - DMVPN supports both IPv4 and IPv6 protocols and all the dynamic routing protocols like EIGRP, OSPF, BGP etc.

- Supports Dynamic Spoke-to-Spoke Tunnels for scaling partial or full mesh VPNs - We can easily create full mesh VPNs with DMVPN with multipoint GRE tunnels used on the spokes. Hub and spoke topologies has one big drawback that one spoke if needs to connects with any other spoke can travels via Hub Router. In order to send packets from one spoke to another spoke without having Hub as a transit point, can results in a much better design and proves to be better scalable.

- Works with and without IPsec - By default, DMVPN works without IPsec, and as DMVPN can be created over a public network like internet also, there sending critical data packets or voice packets without any sort of security can never be a very good design idea and can results in insecure delivery of packets over public network from one DMVPN site to other. So to protect GRE tunnel , we can use IPsec. Tunnel Protection is also introduces in Dynamic Multipoint VPN.

- Supports spoke routers behind dynamic NAT and HUB routers behind static NAT.

- DMVPN supports distributed applications that includes data, voice, video, and all these can be done with Quality of Service also. Also as stated above, we can secure every bit of the tunnel with IPsec.

DMVPN Implementation is divided in three phases

Phase 1 (Hub and Spoke Deployment) - In Phase 1, DMVPN topology behaves like a Point-to-Multipoint topology, where multipoint-GRE is configured in the Hub and simple GRE tunnel is configured on all the spokes. In Phase 1, multicast or unicast traffic can travel only between Hubs and Spokes and not travel directly between Spoke to Spoke. Spokes can be registered statically or spokes can also register themselves to the Next-Hop Server i.e. Hub.

Phase 2 (Spoke to Spoke Deployment Model, Partial/Full Mesh) - Here Hubs and Spokes are configured with Multipoint-GRE or mGRE, therefore spokes can talk directly with each other with a dynamic tunnel is created between one spoke to another spoke.

Phase 3 - Phase 3 powers the spokes as they can now respond to the NHRP resolution requests. Phase 2 and Phase 3 are identical with a single difference, that we can use nhrp redirection , with that there is no need for changing the next-hops in case of EIGRP , we can use NHRP redirection in Hub and NHRP Shortcuts in Spokes. IP NHRP REDIRECT message works like an indication that says that current path towards destination is not optimal and receiver of the message should find a better path. IP NHRP SHORTCUT message overrides the routing table only if it receives an "IP NHRP REDIRECT" message.

1.3) *Multiprotocol Label Switching(MPLS)*

MPLS is the prime technology used in Internet Service Provider Core networks for label switching purposes. MPLS uses VRFs to differentiate between routing tables of customers. Each Provider Edge router gets a clean IP packet from Customer Edge router and then adds a label to that packet and packets are forwarded from source to destination with the help of label switching. Label Switching is performed from PE to PE and Label then gets disposed when packet is sent from PE to remote CE again and CE receives a clean IP packet without any Label. MPLS offers various benefits like scalability, different routing tables for different customers, BGP free core etc, but the biggest advantage that MPLS provides is creating Virtual Private Networks(VPNs).

MPLS Header and its placement in the OSI model is shown below :

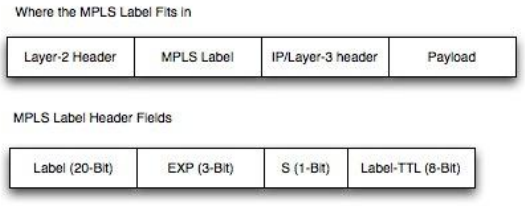

Figure 1.4 - MPLS Label Header and its placement in OSI Model

MPLS Terminology

- **Label** - A 4-byte identifier, used by MPLS to make forwarding decisions.
- **CE Router** - Customer Edge Router, a non-MPLS client/site router connected to the MPLS network.
- **P Router** - Provider Router, a LSR in MPLS VPN terminology.
- **PE Router** - Provider Edge Router, an edge-LSR in MPLS VPN terminology.
- **LSP** - Label Switch Path, a series of LSRs that forward labeled packets to their destinations (unidirectional)
- **Ingress PE router** - Is the edge-LSR an IP packet arrives at from a CE router before being labeled and forwarded to the egress PE router.
- **Egress PE Router** - Is the edge-LSR where the destination route is connected. Receives labeled packets, forwards IP packets.
- **Virtual Routing and Forwarding(VRF)** - It is a technology used in MPLS that allows creation of different routing tables to different customers. It helps in isolation of one customer network from other customer network. Every customers have a different FIB, RIB, LIB, LFIB.
- **Route Distinguisher(RD)** - It is used with VRF and RD uniquely identifies a route. Two or more customers can use same private network at their end, so service provider can differ them with the help of RD value which is attached to the customer route. It is a 64-bit value attached to client's non-unique 32-bit address in order to produce a unique 96-bit VPNv4 address.VPN routes are forwarded over MPLS VPN network using MP-BGP which has a requirement that transported routes must be unique.
- **Route-Targets(RT)** - It is A 64-bit extended BGP community attached to a VPNv4 route to indicate its VPN membership.

- Export RTs are attached to a route when it is converted into a VPNv4 route. It is used to identify the VPN membership of routes .
- Import RTs are used to select VPNv4 routes for insertion into matching VRF tables .

MPLS is a very important part of Next Generation Networks along with IPv6 and Border Gateway Protocol. MPLS has various benefits which are explained below :

- **Less Overhead on ISP Core Routers** - MPLS decreases the overhead of forwarding on core routers. Core routers need not to have full routing tables of internet or customer based routing tables.

- **It can support non-IP protocols forwarding** - With MPLS, Internet Service providers can forward IP and non-IP protocols like ATM, Frame Relay easily. Therefore there is no need to use specialized hardware to run non-IP protocols.

- **Provides BGP enhancement** - MPLS enhances the BGP protocol with Multiprotocol-MP-BGP, and provides various functions like Layer 2 and Layer 3 VPN. Border Gateway protocol is the only protocol that takes the VPN routes from one Provider Edge to other Provider Edge. Interior Gateway Routing protocols are used in the core of MPLS, while BGP takes the Customer VPN routes and internet routing table routes from one provider edge to another provider edge. BGP is only used on the Provider Edge devices and in most of the cases mesh is created between all the Provider Edge devices.

- **Virtual Private Networks** - The biggest benefit of using MPLS for service providers is Virtual Private Networks. MPLS provides an option to the service providers to implement Layer 2 and Layer 3 Virtual Private Networks at a rapid pace. Also with Virtual Routing and Forwarding Instance(VRF) is used with MPLS, therefore different customers are assigned to different VRFs and that helps creating different routing tables for all the customers. Therefore there is no need to use access lists, distribute lists etc or any other filtering. All the customers can use same set of private addresses and there is no need of filtering any of them at the provider edge.

- **Quality of Service** - MPLS provides better options to service provider with quality of service than any other protocols like Frame Relay or ATM. QoS is very important part of service provider networks as there are multiple types of traffic that enters and exit from service provider networks. Service providers mainly categorized their customers on the basis of services for what they pay for. For Example, customers are categorized in Gold, Silver and Bronze categories, with customers in the gold category are most preferred and given more benefits and quality of service is applied for them so that there traffic runs smoothly over the internet service provider network. Different types of traffic like Data, Voice, Video etc travels from one customer edge to another customer edge device and that traffic travels over the provider network and provider can apply quality of service over it, so that traffic like voip be given much preference when some bursty type data traffic is also present in the queue with it. MPLS has more QoS options when compare to other protocols present in its category.

- **AToM(Any Transport over MPLS)** - AToM is part of MPLS with which we can implement Layer 2 VPN. We can make it travel any transport over Multi Protocol Label Switching. It can be Ethernet over MPLS, Frame Relay over MPLS, ATM over MPLS, PPP over MPLS etc. It is also known as VPLS(Virtual Private Wire Service).

- **Traffic Engineering** - It is also one of the most important benefits that makes MPLS better than its competitors. With traffic engineering, load on service provider core network links is properly utilized and traffic load can be shifted from the link which is primarily used to the other link if the load on the link passes some suppress threshold limit.

- **Label Switching** - MPLS uses label switching, this means that the decision making is not performed on the basis of Routing or Forwarding Information Base(FIB), but it is made on the basis of Label Forwarding Information Base. There is no need to have a lookup in FIB table and traffic is easily and forwarded at rapid pace using Label switching protocols. Labels are exchanged at every router and in the whole core network from PE to PE , a label switched path is created to switch packets from one customer office to other customer office.

- **Data Center Interconnections** - Data Centers can be connected using MPLS. MPLS L2 VPN technologies like Virtual Private LAN Service(VPLS) and Ethernet VPN(EVPN) are the most widely used technologies used for Data Center Interconnections.

With MPLS, we can create two types of VPNs :

Layer 2 VPN : With Layer 2 VPN, two remote customer sites can be connected with each other and behave like they are connected using a Layer 2 Switch. Routing Neighbor ship is performed between both the customer-edge routers. Various types of MPLS Layer 2(VPLS) VPN are - Any Transport over MPLS(AToM), Virtual Private LAN Service, Ethernet VPN(EVPN)

Layer 3 VPN : MPLS also created Layer 3 peer-to-peer VPNs by creating neighborship between Customer and Provider Routers. Routing information is shared between customer and provider routers and different customer's routing information is differentiated with the help of Virtual Routing and Forwarding Instance(VRF). A figure below shows MPLS Layer 3 VPN :

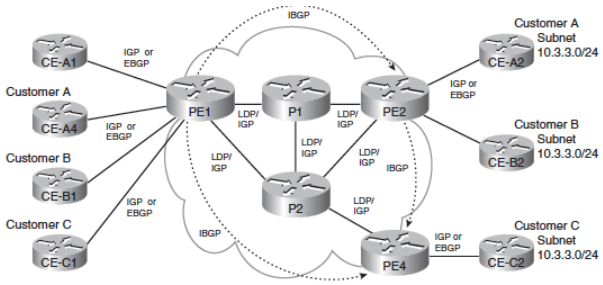

Figure 1.5 - Basic Model of MPLS Layer 3 VPN

1.4) Frame Relay - Frame Relay is a packet-switching technology works at Layer 2 of OSI Model. It is used between LANs over a WAN. The logical path which is created between two routers is known as Virtual Circuit. These VCs can be permanent(PVCs) or switched(SVCs). Frame Relay uses Layer 2 address known as DLCI(Data Link Connection Identifier) which is used to identify the Virtual Circuit. DLCIs are locally significant to a link and can change when passes from frame relay cloud. Frame Relay header is shown below :

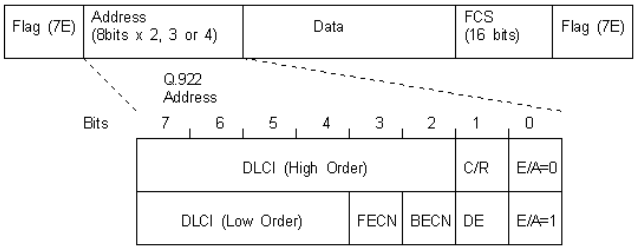

Figure 1.6 - Frame Relay Header Format

LMI - LMI(Local Management Interface) messages are used to manage the communication between DCE devices and DTE devices, DCE device can be a frame relay switch while DTE device can be a Router. A DTE sends LMI enquiry message to the DCE and the DCI responds with LMI status messages to inform the DTE about DLCIs and status of each VCs. There are three types of LMIs :

- CISCO
- ANSI
- q933a

Frame Relay PVC Status - Various Frame Relay PVC status are :

- **Active** - Both end of PVCs are up and communicating.
- **Inactive** - If this message is displayed, it means that local router has received the status about the DLCIs from the frame-relay switch that the remote side is down or has any configuration issue.
- **Deleted** - It means that there is a problem in the local configuration. Frame relay switch has no mapping and replies with the "deleted message".
- **Static** - It indicates that LMI was turned off.

Frame Relay has two types of encapsulations :

- **Cisco** - Only works on Cisco devices.
- **IETF** - Can works on Multi-Vendor environments.

FECN, BECN and DE

- FECN(Forward Explicit Congestion Notification) and BECN(Backward Explicit Congestion Notification) are set in the LAPF header. They are used to signal congestion on a specific PVC.
- Whenever some congestion is noticed on a PVC, FECN bit got set which is used to indicate congestion in its direction.

- Router that got the FECN bit sets the BECN bit on the traffic which is returning to the source, indicates the congestion and it will notify the source to slow down the traffic rate at which source was sending the traffic.
- Discard Eligibility(DE) bit indicates about when the traffic is in violation of the conformed rate and can be discarded during congestion. Frames which are marked with DE bits are dropped before simple frames which are not marked.

Address Resolution

Frame Relay networks are multi-access networks, which means that more than two or more than two devices can be connected in the network pretty similar to Local Area Networks. But we cannot send broadcasts over Frame Relay networks. Therefore frame relay networks are often called NBMA(Non-Broadcast Multi-Access) networks.

Address Resolution is done with Layer 3 to Layer 2 to identify to which remote router does the frame is destined for. Exceptions are Point-to-Point Frame Relay and PPP over Frame Relay.

- **Broadcast Replication** - Frame relay does not have the capability to send single frame to multiple PVCs. There are times when routing protocols need functioning of broadcasts. We can perform a function like broadcast using pseudo-broadcast, what frame relay can do with pseudo-broadcast is that it can create duplicate copies of the frame and send one on each PVC. Therefore Frame Relay can do broadcasts like functioning, but only if it is explicitly configured to do so.

- **Static Mapping** - We can also statically map Layer 3 IP addresses with Layer 2 DLCI addresses. We manually configure them. It also requires broadcast to be enabled manually if there is need of broadcast capabilities.

- **Inverse ARP(InARP)** - It is used to dynamically resolve a Remote Layer 3 IP with the Local layer 2 address which is DLCI in frame relay. It is enabled by default whenever an IP address is configured and also we have enabled Frame Relay on the interface. It has broadcast enabled by default. The InARP status query request can be disabled per DLCI or for all DLCIs or on an interface. If some P2P interface is connected with an interface where InARP is disabled, the InARP disabled interface can still reply, provided an IP address is configured on that interface.

Frame Relay Interfaces

There are mainly two types of characteristics of interfaces in Frame Relay :

- **Physical Interfaces** - They are treated just like Multipoint interfaces. It means that interface can terminate mutliple PVCs.

- **Point-to-Point Sub-interfaces** - These ports can only terminate a single PVC. These ports does not have a requirement of layer 3 to layer 2 address resolution, as there is only single PVC. This also does not send any InARP status query messages, but they will give response to an InARP status query request.
- **Multipoint Sub-Interfaces** - These are multipoint interfaces and can terminate multiple PVCs. They have a requirement of Layer 3 to Layer 2 resolution via manual mapping or through Inverse ARP, as there are multiple PVCs involved. Example topology showing Frame Relay Network is below :

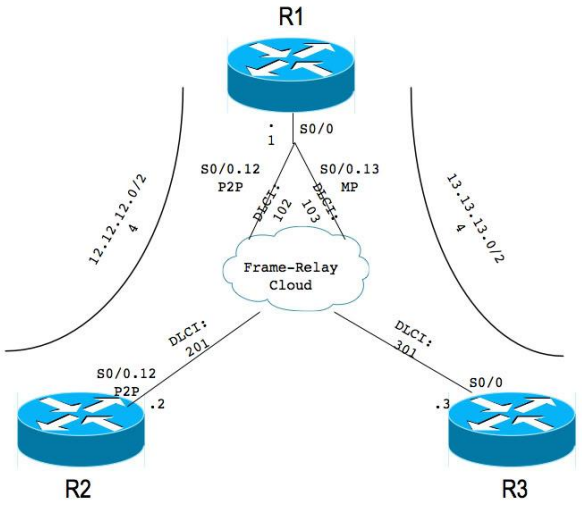

Figure 1.7 - Frame Relay Topology

II. LITERATURE SURVEY

- Multiprotocol Label Switching Architecture[1] by E. Rosen of Cisco Systems, A. Viswanathan of Force10 Networks, and R. Callon of Juniper Networks in Internet Engineering Task Force (IETF) RFC - 3031 specifies the architecture of Multiprotocol Label Switching(MPLS). It is the first standard document of Multiprotocol Label Switching by IETF MPLS Working Group.

- Mustapha B. Ibrahim , Shahad H. Zwayen evaluated the Performance of MPLS and Frame-Relay based on video conferencing for the load.[2] Their research had shown that MPLS gives much better performance than Frame Relay network. MPLS works best in almost every condition that is tested. MPLS works best when traffic engineering and quality of service is needed.

- S.Venkata Raju1, P.Premchand2, A.Govardhan3 evaluated the Routing Performance in Wide Area Networks using mpls ,shows best performance of mpls in terms of throughput and end to end delay. It also describes that MPLS offers enhanced routing capabilities by supporting more than just destination-based forwarding. Some of the new cost-reduction and revenue-generating services that can be deployed with MPLS include traffic engineering, CoSbased forwarding, and VPNs. By separating the control component from the forwarding component, MPLS provides the flexibility to evolve control functionality without changing the forwarding mechanism, thus uniquely positioning MPLS to support the deployment of enhanced forwarding capabilities that will be needed for the Internet to continue its explosive growth.

- Simulation Analysis of latency and packet loss on virtual private network through multivirtual routing and forwarding [4] by Rissal Efendi in Internation Journal of Computer Application(0975 - 8887) Volume 60 - No 19 decribes that by using Multi-VRF run in a Layer 3 MPLS VPN network it will be more secure because it has independent routing table. Encryption and encapsulation process in VPN do not increase the latency of data transmission. Besides that, the transmitted packet is also not lost significantly.

- MPLS: The Magic Behind the Myths[7] by Grenville Armitage, Bell Labs Research, Silicon Valley, Lucent Technologies gives a conclusion that MPLS can leverage ATM's existing cell switching capabilities and new high speed packet forwarding techniques. The real selling point is its ability to support Constraint-routed LSPs from edge to edge using either CR-LDP or M-RSVP. This enables sophisticated load balancing, Qos and MPLS based VPNs to be developed by service providers and large enterprise sites, however such LSPs enable careful engineering of critical cross-core traffic patterns and significant work need to be done before complete solutions exists.

- Using Multiprotocol Label Switching (MPLS) to Improve IP Network Traffic Engineering [8] by Frank Gonzales, Chia-Hwa Chang, Liang-Wu Chen and Chih-Kuang Lin of Colorado University describes the use of Multi Protocol Label Switching technology. This paper describes the increased scalability, manageability, and Quality of Service(Qos) functions related to IP based networks to improve traffic engineering. According to this paper, MPLS network layer scalability and integration of L2 switching and L3 routing has provided the solution for the Internet traffic problem. For service and cost perspective, MPLS allows ISPs to deliver new services which were not possible with traditional IP routing.

- Frame Relay in Public IP Networks [9] by M. Irfan Ali in IEEE Communications Magazine in 1992 describes Frame Relay and its infrastructure and how to use this with Public networks and the evolution of Frame Relay.

- Analysis of traffic engineering parameters while using multi-protocol label switching (MPLS) and traditional IP networks[10] by Faiz Ahmed , Dr. Irfan Zafar in Asian Transactions on Engineering(ATE ISSN: 2221-4267) Volume 01 Issue 03 describes the the effective implementation of resources in the MPLS networks. The simulation results shows that the performances of traffic engineering parameters (i.e packet delay, throughput, loss rate, Jitter etc) in MPLS networks is very stable and much better as compared to traditional IP networks. The results further validate on the basis of better performance to higher-priority flows with higher throughput and lower transmission delay. The network resources are optimized at their optimum performance with the help of traffic engineering. Additionally, the end to end Quality of Service (QoS) is also being ensured.

- Comparing Private Line, Frame Relay, ATM, Ethernet, IP VPNs[11] by AT&T Research Labs

describes Network-based IP VPNs and Ethernet WANs are two of the most popular WAN connectivity alternatives for many of today's leading enterprises. Enterprises should select service providers that offer robust solutions based on an MPLS/IP backbone network that have the flexibility to deliver either type of service, including hybrid solutions utilizing both services. Both network-based IP VPN services and Ethernet WAN services offer enterprises a range of technology and business benefits but perform best when deployed in environments that closely match their capabilities. Network-based IP VPN provides a flexible platform to unify communications across an enterprise's distributed locations, and Ethernet WANs are best at supporting high-throughput applications within a more limited footprint and are often used to connect multiple LANs in a single metro area or interconnect metro WANs.

III. PROBLEM DEFINITION

A company like Amazon has requirements for their critical networks like the need of full mesh connectivity , security and zero downtime, while a simple enterprise company can have different requirements which can be like low cost connectivity.

From ISP point-of-view, security and scalability can be the big issues with which they need to deal, while a customer requires great performance and security.

Cost factor is also a big factor when a customer selects a WAN technology for his enterprise connectivity, while in an ISP, cost factor is with which WAN implementation does they get least profit in return.

IV. OBJECTIVE

- Comparative analysis of various WAN technologies MPLS,FRAME RELAY,DMVPN) will be done.
- Various parameters like security, performance, scalability, cost will be used in comparative analysis.
- Selecting the best WAN technologies based on Enterprise Network .
- Performance will be evaluate by using Graphic Network Simulator(GNS3), Wireshark Packet Analyzer and Cisco 2821, 1841 series routers .

V. RESULTS AND DISCUSSIONS

5.1 Performance Analysis

5.1.1 DMVPN Performance Analysis

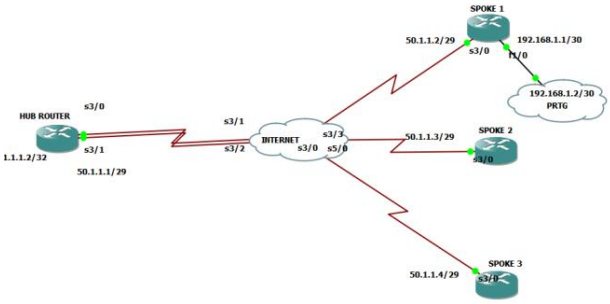

Figure 5.1 - DMVPN Topology in the thesis work

In the DMVPN topology shown in Figure 1.2, we have created a Hub and Spoke Topology with one Hub and Three Spokes, all spokes can send data packets to each other with hub not acting as a transit point, therefore data transfer can happen directly and not using Hub. We have used T1 Links(1.544 Mbps) to connect each site to internet. Hub to internet has two connections resulting in redundant links. A graph below taken from PRTG Monitoring tool shows the minimum, maximum and convergence time (in case of link failure and shifting the traffic to other redundant link).

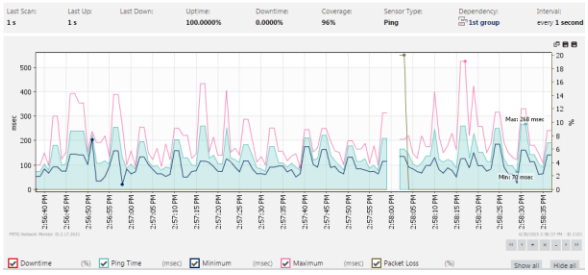

Figure 5.2- Minimum, Maximum and Convergence Time in DMVPN

Above graph shows that it takes maximum 268 msec to complete the ping packet request-reply from PRTG to Hub, Minimum Time is 70 msec, and convergence time is around 3 seconds. We can have a much better performance with faster convergence protocols used or a much better internet connection. But as we are testing on a T1 standard

link, therefore the default result is shown is the graph for a T1 link.

5.1.2) *Multiprotocol Label Switching* -

Topology used for MPLS performance check :

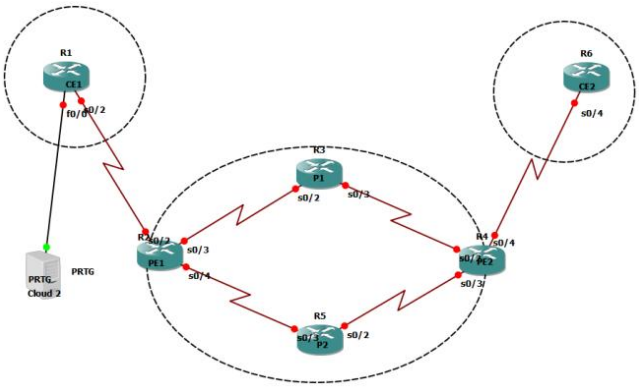

Figure 5.3 - MPLS topology used in thesis

Above topology is used in MPLS Performance check. It has two CEs and two PEs. What we have done is while sending continuous traffic from CE1 to CE2, we broke the primary link from PE-PE to check the convergence time that comes with default parameters. Resulted graph is shown below :

Figure 5.4 - MPLS convergence shown in graph

As shown above, it takes around 3-4 seconds to converge traffic from primary to secondary link. Also it takes minimum 83ms and maximum 289ms for a ping packet to complete over the MPLS network. To converge faster then we can use Faster Convergence protocols like Tuning SPF timers, Fast Reroute etc.

5.1.3) Frame Relay -

Topology used for Frame Relay Topology is shown below :

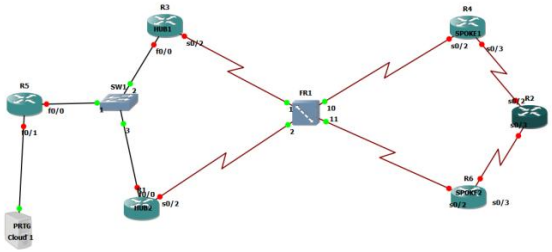

Figure 5.5 - Frame Relay Topology

In the above Hub and Spoke topology, we have multiple Hubs and multiple spokes with Hub 1 acting as primary Hub while Hub 2 is our backup Hub router, when Hub link WAN link goes down the convergence time taken is shown in the following graph :

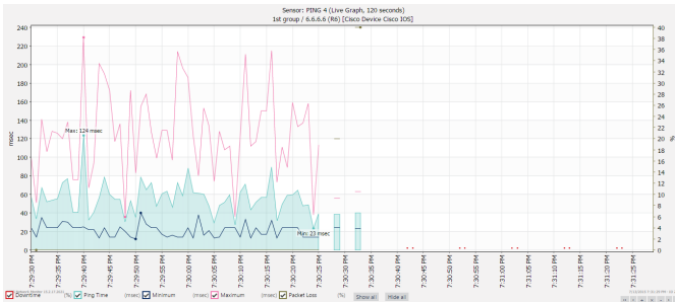

Figure 5.6 - Convergence Time in case of FR

Another screenshot shows why Frame Relay does that slow convergence :

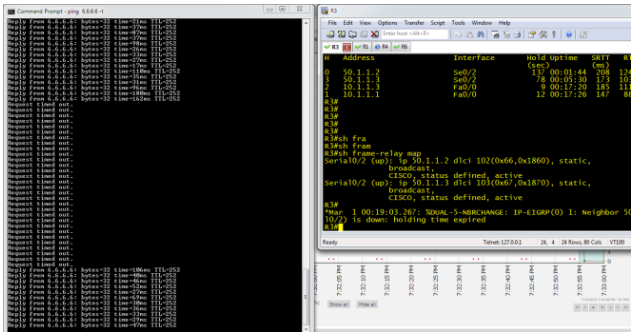

Figure 5.7 - Frame Relay convergence problem

Above screenshots shows that Frame Relay takes a long time for convergence, as its DLCI stayed up even after long time, also IGPs act slow in Frame Relay network than other networks. EIGRP hold time was 180 seconds as compared with 15 seconds for other networks. Total convergence time was over around 55-60 seconds with

over 30 packets got dropped, minimum time is 23 ms and maximum time is 124 ms for a ping packet to complete.

WAN	Minimum Time	Maximum Time	Convergence Time
DMVPN	70ms	268ms	2.5-3 seconds
MPLS	83ms	289ms	3-4 seconds
FRAME RELAY	23ms	124ms	55-60 seconds

Table 5.1 - Performance Analysis of WAN Protocols

5.2) Security Analysis of WAN technologies

DMVPN and MPLS both uses IPSec to secure the IP traffic from one site to other site. DMVPN can be created over Internet, so if data traffic from one site to other site needs to be secure transmission that IPSec is the best solution, also when using MPLS then its much better if we don't rely of Service Provider for security and use IPSec from CE - CE. I have used IPSec for security both for MPLS and DMVPN as it is the best security solution which provides end-to-end-security with Encryption, Hashing and Authentication. For encryption, i have used Advance Encryption Standard(AES), Secure Hash Algorithm - 1(SHA-1) is used for hashing and Pre-Share Authentication is used by me in the DMVPN and MPLS. Results that i got are shown below :

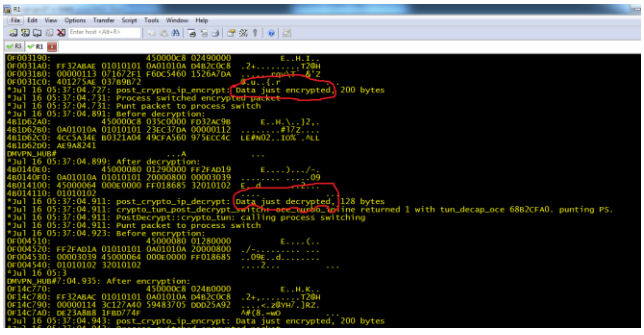

Figure 5.8 - Data from Spoke to Hub in encrypted fashion

As shown above, data sent from spoke 1 to hub is sent in encrypted fashion by using IPSec between Hub and Spokes. Also Wireshark captures of IPSec ESP Packet is shown below :

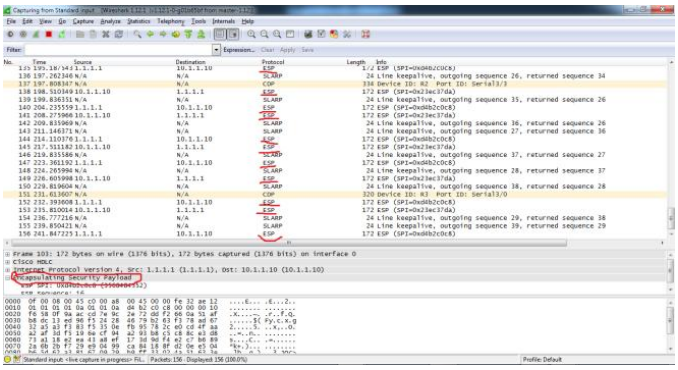

Figure 5.9 - Data encrypted under ESP

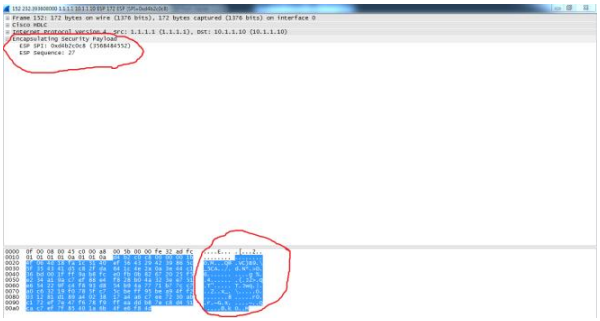

Figure 5.10 - Data encapsulated under ESP

Encapsulating Security Payload or ESP provides Data Integrity, Encryption features with IPSec. MPLS and DMVPN both uses IPSec.

Frame Relay on the other hand, creates a Layer 2 VPN connection and therefore is safe from Layer 3 Attacks like Denial-Of-Service, LMI is the protocol running between Frame-Relay Switches and Routers at Customer End, which cannot be attacked very easily, only thing that can harm is if someone intentionally sends a LMI burst traffic attack, which can be prevented by dropping the excess traffic.

5.3 Scalability Analysis of DMVPN, MPLS and Frame Relay

MPLS provides a better scalability as it is controlled by Service Provider and QoS, Traffic Engineering Features are done by Service provides, service provider just needed to add VRF and neighborship with client. While on DMVPN, which is mainly made on Internet has lesser control over QoS etc features. If a enterprise is large and uses VoIP in their network, then DMVPN can never give the same performance as MPLS as the traffic increases.

Configuration is not needed on Hub whenever Spoke site is needed to be added. Spoke automatically gets peered with the Hub in dynamic way. Therefore as far as configuration is concerned, DMVPN needs lesser configuration. Frame Relay is not used for enterprises having large number of offices requiring large bandwidth, also Frame Relay is mainly used for Hub and Spoke Topologies which are much cheaper than any to any topologies that MPLS L3 or DMVPN dynamically provides, to scale a Frame Relay Network to provide any to any mesh network, it requires more PVCs to be created and n(n-1) links, which can be difficult to manage in Frame Relay Networks if the organization has large number of offices.

VI. CONCLUSION & FUTURE SCOPE

MPLS, DMVPN and Frame Relay are the three most dominating WAN technologies in the industry. Frame Relay is kind of traditional these days. But MPLS is pioneer in the field of Next Generation networks, DMVPN is the easiest and cheapest solution of the all. On the basis of results, DMVPN and MPLS are having a good competition, but it also does not provide ISP with features as MPLS has. MPLS provide total control to Service Provider and it eliminated the need of BGP in the core of ISP networks, also it can provide both L2 and L3 VPN service to customers. Most DMVPN connections are made over internet and they depends on internet speed for performance, also when Quality of Service needed to be used, then MPLS is much better than DMVPN. Therefore as far as performance is concerned, MPLS is a winner with a slight margin as it is much more stable than DMVPN. As far as security is concerned, DMVPN and MPLS can secure the VPN path by implementing IPSec and Frame Relay does not get Layer 3 Attacks as it is Layer 2 and can drops excess burst traffic that comes to it, in case of burst traffic attacks. MPLS is better in scalability in comparison with DMVPN and Frame Relay and DMVPN needs least configuration while adding new customer sites.

With the internet getting stronger, WAN is also getting stronger day by day. Apart from Internet, companies connecting their offices at one location with branches of their offices at other location needs WAN technologies. MPLS is expanding with its new type Ethernet VPN which is started to be used for Data Centers Interconnection. Started in 2014, it's an ultra-fast multipoint to multipoint solution. MPLS is the major part in Next-Generation networks. Dynamic-Multipoint VPN is also getting popular with want to connect their twp or more offices with each other as it provides them the cheapest solution if they are creating it over Internet. Even though DMVPN can also be created over MPLS networks, but it can be much costly then the Internet based. Frame Relay is in his last days as it demands a separate infrastructure in Service Provider, while MPLS and DMVPN can run on routers. MPLS and DMVPN are the WAN solutions that will be used in the upcoming times in large.

VII. REFERENCES

[1] Multiprotocol Label Switching Architecture by E. Rosen of Cisco Systems, A. Viswanathan of Force10 Networks, and R. Callon of Juniper Networks in Internet Engineering Task Force (IETF) RFC - 3031

[2] Evaluating the performance of MPLS and Frame-Relay by Shahad H. Zwayen and Mustapha B. Ibrahim of Al-Nahrain University, Iraq in December, 2014

[3] Evaluation the Routing Performance in Wide Area Networks using mpls by S.Venkata Raju1, P.Premchand2, A.Govardhan3 in 2013.

[4] Simulation Analysis of latency and packet loss on virtual private network through multivirtual routing and forwarding by Rissal Efendi in 2012.

[5] Cisco Documentation for DMVPN, MPLS and Frame Relay

[6] Cisco Configuration Guides for DMVPN, MPLS and Frame Relay

[7] MPLS: The Magic Behind the Myths by Grenville Armitage, Bell Labs Research, Silicon Valley, Lucent Technologies.

[8] Using Multiprotocol Label Switching (MPLS) to Improve IP Network Traffic Engineering by Frank Gonzales, Chia-Hwa Chang, Liang-Wu Chen and Chih-Kuang Lin of Colorado University

[9] Frame Relay in Public IP Networks by M. Irfan Ali in IEEE Cummunications Magazine

[10] Analysis of traffic engineering parameters while using multi-protocol label switching (MPLS) and traditional IP networks by Faiz Ahmed , Dr. Irfan Zafar in 2011

[11] Comparing Private Line, Frame Relay, ATM, Ethernet, IP VPNs by AT&T Research Labs