RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of MPLS Signaling Protocols

Damanjit Kaur [1], Er.Dinesh Kumar[2]
Department of Computer Science and Engineering
GZS PTU Campus, Bathinda
Punjab-India

ABSTRACT

MPLS is the pioneer in Service Provider Networks. Every service provider use MPLS in its core network for fast label switching. This paper explains MPLS and its signaling protocols i.e. LDP, CR-LDP, RSVP, RSVP-TE. This paper explains every signaling protocol that is used in Multiprotocol Label Switching environment. This paper explains differences between MPLS signaling protocols on the basis of performance and security.

Keywords: - MPLS, LDP, RSVP, CR-LDP, TE, LABEL, LSP

I. INTRODUCTION

Multiprotocol Label Switching(MPLS) is a packet-forwarding technology used in high performance telecommunication networks. It is a popular networking technology that uses labels attached to packets to forward them through the network. Routers forward the traffic by looking at the label and not the destination address, so the packets are forwarded by label switching technique instead of IP Switching. The fact that the MPLS Labels are used to forward the packets and no longer the destination IP address has led to the popularity of MPLS. Before MPLS, Frame Relay and ATM were the most popular WAN protocols. They provide Layer 2 VPN service towards Layer 3 customer routers. They are still used today, but customers are shifted to MPLS because of its benefits like "the use of one unified network infrastructure", "Border Gateway Protocol(BGP)-free core", "better IP over ATM integration", "Peer-to-Peer model for MPLS VPN", "Optimal traffic flow", "Traffic engineering" etc.

MPLS uses labels to forward ip packets in the service provider network. One MPLS label is of 32 bits with the certain structure shown below.

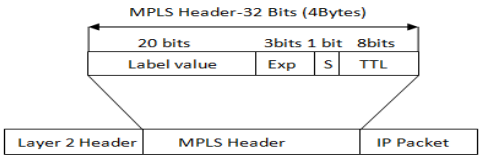

Figure 1 - MPLS Label Format

First 20 bits are the label value. This value can be between 0 and 2^{20}-1, or 1,048,575. First 16 values are reserved and have special meaning. Bits 20 to 22 are three experimental bits used for Quality of Service(QoS) purposes. Bit 23 is the Bottom of Stack(BoS) bit. It is 0, unless the label is bottom label of the stack. Bits 24 to 31 are eight bits used for Time to Live(TTL), just like in IP header.

A. *MPLS Signaling Protocols* -

MPLS signaling protocols are used for label switching purposes. A Label Switch Path(LSP) must be set up with labels assigned at each hop before forwarding of traffic can take place. Various types of MPLS Signaling protocols are:

B. *Label Distribution Protocol(LDP)*

LDP is a label distribution protocols that behaves like a routing protocol. Router creates peer relationship with connected MPLS Router and shares labels with the peer router. LDP is an open standard protocol that exchanges labels and stores them in the Label Information Base(LIB). The label information in the LIB is then used in the data plane to provide MPLS functionality, as follows:

- A label is added to the IP forwarding table(FIB) to map an IP prefix to a next-hop label.
- A locally generated label is added to the Label Forwarding Information Base(LFIB) and mapped to a next-hop label.

C. *Constraint-Based routed LDP*

CR-LDP is a set of extensions to LDP specifically designed to facilitate constraint-based routing of LSPs. It uses TCP sessions between LSR peers and sends label distribution messages along the sessions. CR-LDP

standards attempt to enable the LDP protocol to work over an explicit route, transporting various traffic parameters for resource reservation as well as the options for CR-LSP robustness feature.

D. Resource Reservation Protocol (RSVP)

RSVP was originally designed as a means for a host to determine if there is enough bandwidth available for a particular flow. It is used for establishing LSPs in MPLS networks.

E. RSVP-TE

The original RSVP standard was extended to carry an MPLS label and TE information. RSPV is used with MPLS TE to signal a LSP for a TE tunnel whether the path is built dynamically or defined explicitly. RSVP uses downstream on demand label distribution, meaning a label is only advertised upstream once a label from the downstream LSR is received. RSVP-TE provides support for :

- Explicit path configuration
- Path numbering
- Route Recording

A basic mpls figure showing label distribution is shown below :

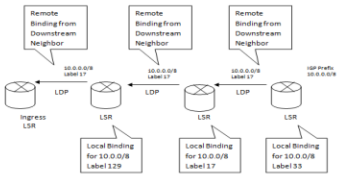

Figure 2: MPLS Label forwarding mechanism

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.

LDP Specification[2] by L. Anderson of Nortel Networks, P. Doolan of Ennovate Networks, N. Feldman of IBM Corporation, A. Fredette of PhotonEx Corporation and B. Thomas of Cisco Systems in IETF RFC - 3036 describes Label Distribution protocol, by which LSRs distribute labels to support MPLS forwarding along normally routed paths. This document is the first standard document for Label Distribution Protocol(LDP) by IETF MPLS Working Group.

Fault Tolerance for the Label Distribution Protocol (LDP)[3] by A. Farrel, Ed. of Movaz Networks in IETF RFC 3479 identifies issues in the LDP specification in RFC 3036, "LDP Specification", that make it difficult to implement an FT LSR using the current LDP protocols, and defines enhancements to the LDP specification to ease such FT LSR implementations.

Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)[4] by L. Martini, Ed. , E. Rosen by Cisco Systems, N. El-Aawar of Level 3 Communications, T. Smith of Network Appliance Inc. and G. Heron of Tellabs in IETF RFC 4447 describes Layer 2 services (such as Frame Relay, Asynchronous Transfer Mode, and Ethernet) can be "emulated" over an MPLS backbone by encapsulating the Layer 2 Protocol Data Units (PDU) and transmittingthem over "pseudowires". It is also possible to use pseudowires to provide low-rate Time Division Multiplexed and a Synchronous Optical NETworking circuit emulation over an MPLS-enabled network. This document specifies a protocol for establishing and maintaining thepseudowires, using extensions to Label Distribution Protocol (LDP).

Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling[5] by M. Lasserre, Ed. , V. Kompella, Ed. of Alcatel Lucent in IETF RFC 4762 describes a Virtual Private LAN Service (VPLS) solution using pseudowires, a service previously implemented over other tunneling technologies and known as Transparent LAN Services (TLS). A VPLS creates an emulated LAN segment for a given set of users; i.e., it creates a Layer 2 broadcast domain that is fully capable of learning and forwarding on Ethernet MAC addresses and that is closed to a given set of users. Multiple VPLS services can be supported from a single Provider Edge (PE) node. This document describes the control plane functions of signaling pseudowire labels using Label Distribution Protocol (LDP), extending RFC 4447. It is agnostic to discovery protocols. The data plane functions of forwarding are also described, focusing in particular on the learning of MAC addresses.

Constraint-Based LSP Setup using LDP[7]by Jamoussi of Nortel Networks, L. Anderson, Utfors AB, R. Callon of Juniper Networks, R. Dantu of Netrake Corporation, L. Wu of Cisco Systems, P. Doolan of OTB Consulting

Corporation, T. Worster, N. Feldman of IBM Corporation, A. Fredette of ANF Consulting, M. Girish of Atoga Systems, E. Gray, Sandburst, J. Heinanen of Song Networks, T. Kilty of Newbridge Networks and A. Malis of Vivace Networks in IETF RFC 3212 specifies mechanisms and TLVs (Type/Length/Value) for support of CR-LSPs (constraint-based routed Label Switched Path) using LDP (Label Distribution Protocol). This specification proposes an end-to-end setup mechanism of a CR-LSP initiated by the ingress LSR (Label Switching Router). We also specify mechanisms to provide means for reservation of resources using LDP.

LSP Modification Using CR-LDP[8]Z by J. Ash of AT&T, Y. Lee of Ceterus Networks, P. Ashwood-Smith, B. Jamoussi, D. Fedyk, D. Skalecki of Nortel Networks, L. Li of SS8 Networks in IETF RFC 3214 presents an approach to modify the bandwidth and possibly other parameters of an established CR-LSP (Constraint-based Routed Label Switched Paths) using CR-LDP (Constraint-based Routed Label Distribution Protocol) without service interruption. After a CR-LSP is set up, its bandwidth reservation may need to be changed by the network operator, due to the new requirements for the traffic carried on that CR-LSP. The LSP modification feature can be supported by CR-LDP by use of the modify value for the action indicator flag in the LSPID TLV. This feature has application in dynamic network resources management where traffic of different priorities and service classes is involved.

Resource ReSerVation Protocol (RSVP)[9] by R. Braden, Ed. and S. Berson of ISI Networks, L. Zhang of UCLA, S. Herzog of IBM Research, and S. Jamin of University of Michigan in IETF RFC 2205 describes version 1 of RSVP, a resource reservation setup protocol designed for an integrated services Internet. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows, with good scaling and robustness properties.

RSVP Operation Over IP Tunnels[10] by A. Terzis of UCLA, J. Krawczyk of ArrowPoint Communications, J. Wroclawski of MIT LCS, and L. Zhang of UCLA in IETF RFC 2746 describes an approach for providing RSVP protocol services over IP tunnels. It briefly describe the problem, the characteristics of possible solutions, and the design goals. It, then present the details of an implementation which meets our design goals.

Support for Resource Reservation Protocol Traffic Engineering (RSVP-TE) in Layer 3 Virtual Private Networks (L3VPNs)[12] by K. Kumaki, Ed. and P.Jiang of KDDI Corporation, T. Murai of Furukawa Network Solution Corporation, D. Cheng of Huawei Technologies, S. Matsushima of Softbank Telecom in IETF RFC 6882 describes how to support RSVP-TE between customer sites when a single PE supports multiple VPNs and labels are not used to identify VPNs between PEs.

S. Veni, Dr.G.M.Kadhar Nawaz and P.Praba, "Performance Analysis of Network Traffic Behavior in Conventional Network over MPLS[14]", Proc of ICCCCT 2010 IEEE International Conference, Nagercoil, Tamil Nadu, India did a performance analysis on network traffic forwarding behavior inside MPLS backbone network.

III. PROBLEM DEFINITATION

MPLS is the technology that creates the backbone network of almost all the major ISPs in the world. It can transport various payloads like Layer 2 in the form of Ethernet, Frame Relay, ATM, PPP, HDLC etc and Layer 3 payloads like IPv4 and IPv6. It switches traffic between interfaces by looking at labels instead of destination IP lookup, so it does forwarding based on locally significant label values. Labels are distributed between two routers using various Label distribution protocols like TDP, LDP, BGP Signaling, CR-LDP, RSVP, RSVP-TE. MPLS can also be of various types like. Main distribution protocols are LDP, RSVP and CR-LDP. Selecting the best label distribution protocol for MPLS networks is very important as MPLS is as label distribution is the soul of MPLS just like routing protocols for IP. Selection of the wrong protocol for MPLS can harm the performance and also provider various other degradation in the service provider networks.

IV. OBJECTIVES

Objective of this paper is to do a comparative and behavior analyses of all the MPLS signaling protocols and find the best one according to the specific requirements and design. Various case studies will be done to achieve this:

1.) Which of the label distribution protocol works best in a basic Layer 3 MPLS?
2.) Which of the label distribution protocol works best in an environment where traffic engineering is necessary?
3.) Which of the label distribution protocol works best in various Layer 2 MPLS/VPLS designs?

4.) Which of the label distribution protocol has the fastest convergence?

5.) How label distribution protocol works with QoS, and which one of them works best in terms of working with QoS?

V. RESULTS

A. *Performance Analysis -*

For performance analysis, convergence time is used check, how much time MPLS layer 3 VPN takes when primary link in MPLS backbone network goes down, Topology used is shown below.

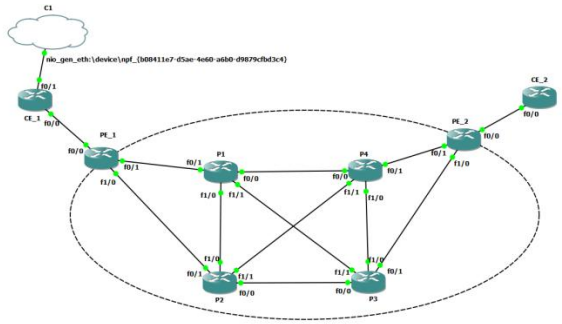

Figure 3: MPLS L3 VPN topology used in Thesis

Clearly from the topology shown above, it is shown that CE_1 is a customer of Internet Service Provider ABC, Customer A has two sites at different locations that are connected with the help of MPLS Layer 3 based VPN. Customer A, when transfers data, voice or video traffic from Customer A _Site_1 to Customer A_Site_ 2, has two paths in the core network of ISP_ABC via P1 and P2. Traffic mainly moves towards P1 which is acting as a primary path and P2 is in use only when P1 goes down. When P1 goes down, convergence time taken with default timers by MPLS L3 VPN is shown in the graph below:

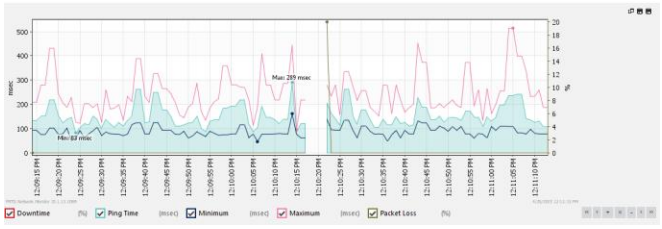

Figure 4: MPLS L3VPN Convergence Time Graph taken from PRTG

Now as we see the graph in Figure 4.2, it shows that there is a delay of around five seconds when traffic from primary link shifts to backup link in case of primary link failure in the MPLS Backbone network. Five seconds is a large amount of time when we talk about network convergence in todays's world where Voice and Video based traffic is a kind of necessity with Video Conferencing solutions, Voice Mails, voice messaging solutions etc.

We can use various methods to fasten the convergence time with Bidirectional Forwarding Detection or by decreasing the Interior Gateway Protocol timers. IGPs used in Service provider network can be either Open Shortest Path First(OSPF) or Intermediate System to Intermediate System(IS-IS), as only Link State routing protocols are preferred in Internet Service Provider(ISP). Both these protocols use Dijkstra Shortest Path First Algorithm(SPF). We can shorten the timers between SPF calculations or other IGP timers to reduce the convergence time. How this will help is whenever a primary link goes down, SPF calculations can be done for backup link in much faster time than by using default timers. After changing the default hello timer and dead timer interval in OSPF which is used as IGP inside the ISP network for internal routing, the results that i got is shown below in a graph taken with the help of PRTF Traffic Analyzer :

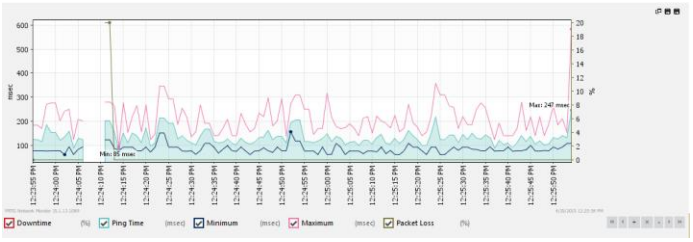

Figure 5: MPLS Layer 3 Convergence Graph with OSPF Timers Tuned.

In the above graph, what the result is showing is that there is not much of a difference that can be made by tuning Hello or Dead Timers of IGP that can be used inside an ISP internal network. Now let's try to change the SPF calculation timers inside an ISP network. We will reduce the timers of SPF calculations that can be done in the case of some link failure so that backup path SPF calculation can be done in much fast manner. One PE is connected with other PE using an IGP protocol, so it will definitely make a difference in our MPLS network. Graph below shows the convergence time between Primary Link failure and traffic shifting from primary link towards backup link.

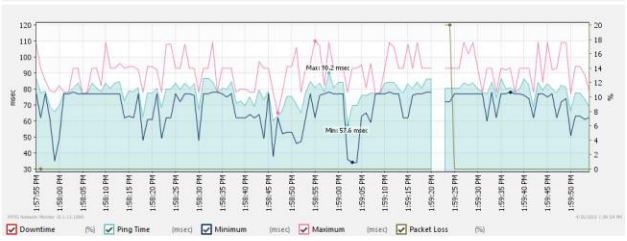

Figure 6: MPLS Layer 3 VPN convergence graph with OSPF SPF Calculation Timers tuned

As we can see, convergence time is reduced from 5-5.5 seconds to 2-2.5 seconds which is much better than the normal results.

The other two types of Label Distribution Protocols act in totally different manner than the LDP. Resource Reservation Protocol(RSVP) and CR-LDP(Constraint-Based Router LDP) are used to support Traffic Engineering and the Label Switch Paths(LSPs) that are made using these two protocols are known as Traffic Engineered LSPs.

CR-LDP is a extension to LDP and uses TCP sessions between LSR peers just like LDP. This allows a reliable distribution of messages between LSR peers. Basic flow setup in CR-LDP is shown below:

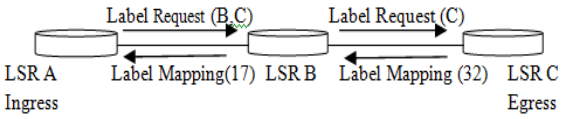

Figure 7: Basic CR-LDP LSP flow

- The ingress LSR, LSR A, needs to set up a new LSP between to LSR C. The traffic parameters which are required for the Session for the network enables LSR A to determine that the route from LSR A to LSR C which forms the new LSP should go through LSR B. In this method LSR A creates a LABEL_REQUEST message with an explicit route of (B,C) and in this request message it will also request traffic parameters for the new route. LSR A reserves the resources which it needs for the new LSP, and then it forwards the LABEL_REQUEST to LSR B on the TCP session.

- LSR B, when receive the LABEL_REQUEST message, determines that it is not the Egress router, and it then forwards the request along the route which was specified in the message. It reserves the resources which were requested for the new LSP, then modifies the explicit route in the LABEL_REQUEST message, and then passes the message to LSR C. LSR B can also reduce the reservation it makes for the new LSP if the appropriate parameters were marked as negotiable in the LABEL_REQUEST

- LSR C then checks that it is the egress for this new LSP. It performs the final negotiation on the resources and created the reservation for the LSP. It allocates a label to the new LSP and distributes the label to LSR B in the LABEL_MAPPING message, which also contains the final traffic parameters reserved for the LSP.

- After the above process LSR B receives the LABEL_MAPPING and matches it to the original request using the LSP ID contained in both LABEL_REQUEST and LABEL_MAPPING message.

- LSR A when receives the LABEL_MAPPING , does not have to allocate a label and it just forward it to an upstream LSR because it is the ingress LSR for the new LSP.

B. Reservation Protocol(RSVP)

RSVP exchanges the messages to reserve resources across a network for IP flows. It is used for LSP tunnels so that it can be used to distribute MPLS labels. It uses UDP to communicate between LSR Peers. There is no need to maintain the TCP session, but it must be able to handle the loss of control messages. Basic flow for LSP setup using RSVP is shown below :

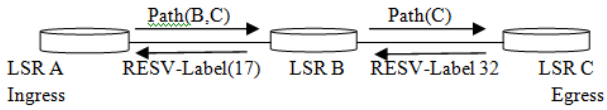

Figure 8: RSVP LSP Setup Flow

- LSR A, which is the ingress LSR, determines that it needs to setup a new LSP to LSR C. The traffic parameters required for the session enables the LSR A to determine that the route for the new LSP should go through LSR B. This process is not like the hop-by-hop route towards LSR C. LSR A builds a Path message with an explicit route of (B,C) and the details of the route requested for the new route. LSR A now sends the IP datagram to LSR B.

- LSR B receives the Path request, which then determines that LSR B is not the egress router for the LSP. It then modifies the explicit route and passes the Path message to the LSR C.

- When message is received at LSR C, LSR C then determines that it is the egress router for the LSP, determines from the requested traffic parameters about the bandwidth it needs to reserve and allocates the resources as required. A label is selected for the new LSP and then the label is distributed to LSR B in a Resv message. It also includes the actual or original details of the required reservation for the LSP.

- LSR B receives the reservation message and matches it with the actual reservation request message using the LSP ID, which is contained in both the PATH and RESV message. It then determines the total resources that are needed in the RESV message, allocates the label for the LSP, creates the forwarding table and passes the new label to LSR A in the RESV message.
- The processing at LSR A is similar, the single difference is that it does not have to allocate a new label and forward this to an upstream LSR because it is the ingress point for the new LSP.

Graph created with RSVP used in the MPLS as a signaling protocol is defined below :

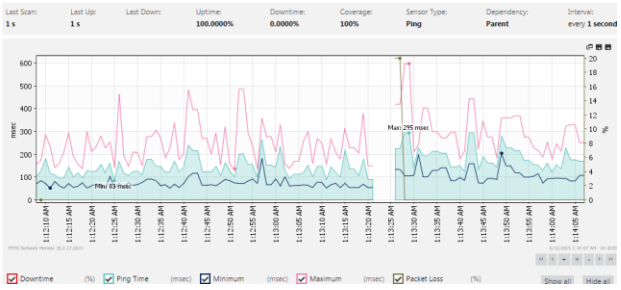

Figure 9: Default Max and Minimum time and convergence time in topology using RSVP

RSVP Reservation message is shown below taken from R2 and R7 :

```
R2#sh ip rsvp reservation  detail

RSVP Reservation. Destination is 2.2.2.2, Source is 7.7.7.7,
  Protocol is 0  , Destination port is 1, Source port is 23
  Next Hop is 2.2.2.2, Interface is
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 0100040D.
  Created: 00:59:34 UTC Fri Mar 1 2002
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Label is 1
  Status: Proxied
  Policy: Accepted. Policy source(s): MPLS/TE

RSVP Reservation. Destination is 7.7.7.7, Source is 2.2.2.2,
  Protocol is 0  , Destination port is 1, Source port is 9
  Next Hop is 23.1.1.3, Interface is FastEthernet0/1
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 02000408.
  Created: 01:00:17 UTC Fri Mar 1 2002
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Label is 27
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
R2#
```

```
R2#sh ip rsvp reservation
To              From            Pro DPort Sport Next Hop      I/F      Fi Serv BPS
2.2.2.2         7.7.7.7         0   1     22    2.2.2.2                SE LOAD 0
7.7.7.7         2.2.2.2         0   1     8     24.1.1.4       Fa1/0    SE LOAD 0
```

```
R7#SH IP RSVp REServation  detail

RSVP Reservation. Destination is 2.2.2.2, Source is 7.7.7.7,
  Protocol is 0  , Destination port is 1, Source port is 23
  Next Hop is 57.1.1.5, Interface is FastEthernet1/0
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 0100040E.
  Created: 01:00:14 UTC Fri Mar 1 2002
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Label is 29
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE

RSVP Reservation. Destination is 7.7.7.7, Source is 2.2.2.2,
  Protocol is 0  , Destination port is 1, Source port is 9
  Next Hop is 7.7.7.7, Interface is
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 03000409.
  Created: 01:00:57 UTC Fri Mar 1 2002
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Label is 1
  Status: Proxied
  Policy: Accepted. Policy source(s): MPLS/TE
```

```
R7#SH IP RSVp REServation
To              From            Pro DPort Sport Next Hop      I/F      Fi Serv BPS
2.2.2.2         7.7.7.7         0   1     23    57.1.1.5       Fa1/0    SE LOAD 0
7.7.7.7         2.2.2.2         0   1     9     7.7.7.7                 SE LOAD 0
```

Figure 10: Output showing Path Reservation between PE devices

Also the graphs were taken using Layer 2 MPLS VPN using LDP and RSVP, which are shown below :

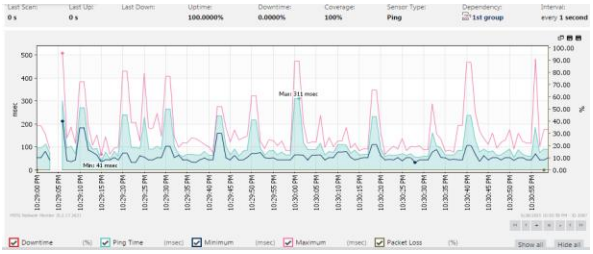

Figure 10: Max, Min and Convergence time in L2 MPLS VPN using LDP in the core.

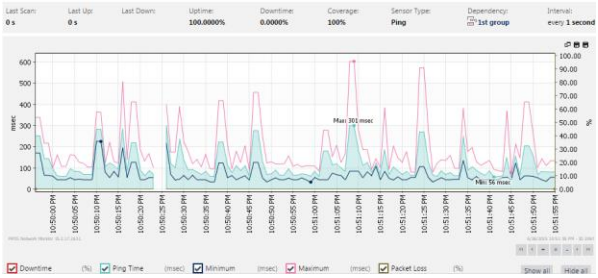

Figure 11: Max, Min, and Convergence Time in MPLS L2 VPN with RSVP used in the core

By looking at the above two graphs of MPLS L2 VPNs, its clear that there are not much differences in the maximum, minimum and convergence times when default timers or SPF calculations are tuned. But L2 VPN provides a slightly better performance that MPLS Layer 3 VPNs.

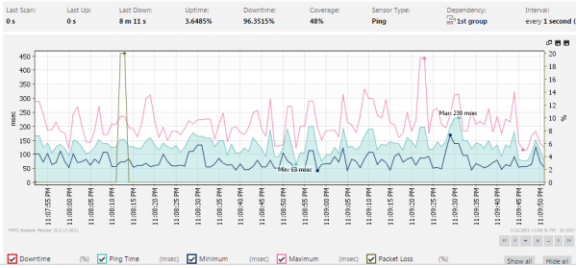

Figure 12: Max,Min and Convergence time in MPLS L2 VPN with RSPV ,SPF timers tuned.

Signaling Protocol	Maximum Time	Minimum Time	Convergence Time	ConvergenceTime with SPF Tuning
LDP(L3VPN)	289msec	83msec	4.5 - 5 sec	2 - 2.5
RSVP(L3VPN)	295msec	83msec	4 - 4.5 sec	2 - 3
LDP(L2VPN)	311msec	41msec	2.5 - 3 sec	Sub-Second
RSVP(L2VPN)	301msec	56msec	2-3 sec	Sub-Second

Table:1 Table showing performance analysis of MPLS protocols.

	LDP Support	CR-LDP Support	RSVP Support
Transport	TCP ,UDP	TCP	Raw IP
Security	Yes	Yes	Yes
High Availability	Yes	No	Yes
Traffic Control	No	Yes	Yes

Table: 2 Table showing difference between MPLS protocols.

C. Security Analysis of MPLS Layer VPNs

Security in MPLS can be achieved by using various methods. Security is important in MPLS networks. All the traffic like Voice, Data and Video traffic that transits from ISP for customer networks needed to be secure, as an insecure ISP network means Customer data will be insecure. MPLS networks can be made secure by performing authentication feature between Label Distribution Protocol(LDP) means MPLS neighborship can be made only if the passwords on the both end of the neighbors are matched. Best thing that can be done for securing MPLS is that we can use IPSec for securing our communication between MPLS networks from our customer site also. IPSec can be used in various scenarios which can be -

1.) Provider Edge to Provider Edge(PE-PE)
2.) Customer Edge to Customer Edge(CE-CE)
3.) Provider to Provider (P-P)

Best practice is to use CE-CE IPSec implementation, where traffic sourced from CE gets encrypted and decryption is done in CE site on the other end. We have used the MPLS Layer 3 design shown in Figure 1.1 for our MPLS Network Security Implementation. We have used IPSec for traffic between 1.1.1.1 which is on CE1 and 8.8.8.8 on CE2 and after creating a secure tunnel between CE1 and CE2; we are able to access R8 via R1 as shown in the figure below:

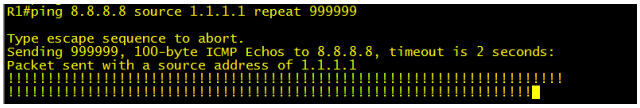

Figure 13: R1 checking reachability with R8 by issuing ping command sourced from 1.1.1.1

After issuing ping command on R1, issued the **debug crypto engine packet** command on R8 to check incoming traffic created with the ping command on R1 to see if the incoming traffic from R1 is coming in encrypted form or not.

To get into more detail,I have also used Wireshark Packet analyzer to sniff data that is going over Service provider network. Below is the capture taken from Wireshark:

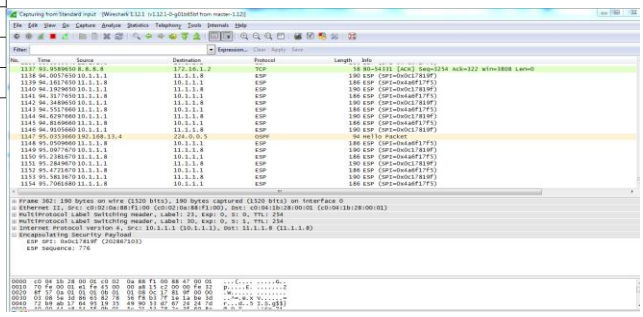

Figure14: Wireshark capture showing traffic from 1.1.1.1 to 8.8.8.8 using ESP.

Above capture from Wireshark shows that Source and Destination IP addresses are hidden because we are using Tunnel Mode in IPSec. With Tunnel Mode, original IP address gets hidden and Tunnel's Source and Destination IP addresses are used which is a add-on to the network security.For more details,Ihave also extracted a packet using Wireshark from1.1.1.1
to 8.8.8.8

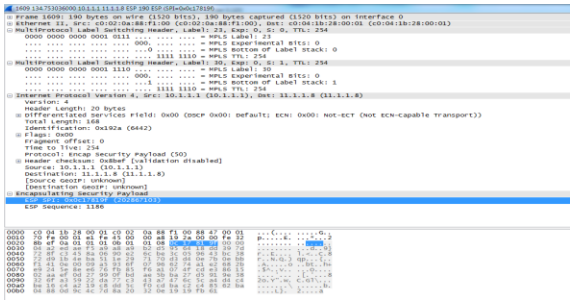

Figure 15: Specific ESP packet captured in Wireshark encrypting MPLS traffic

Above Figure shows that traffic generated from CE1 to CE2 when entered Service Provider MPLS backbone also encrypts MPLS traffic with IPSec. ESP shows encrypted data under the payload section. A graph showing Encrypted and Decrypted traffic between 1.1.1.1 and 8.8.8.8 is shown below:

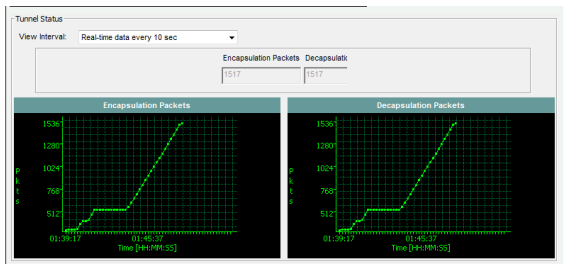

Figure 16: Graph showing encrypted and decrypted packets using IPSec.

Above graph created using Cisco Configuration Professional is showing that 1517 packets have been encrypted using IPSec and same numbers of packets have been decrypted.

We have used IPSec with LDP, but with RSVP, we can only use RSVP Authentication, which provides data integrity with Hashing algorithms like MD5 or SHA-1, We have used SHA-1 in our topology and capture the packets using wireshark packet sniffer:

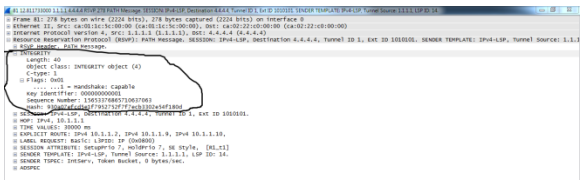

Figure 17: RSVP packet captured from Wireshark with SHA-1 hashing used.

VI. CONCLUSION& FUTURE SCOPE

LDP used as a default label distribution protocol .It is enabled automatically when we enable MPLS.For traffic engineering ,RSVP and CR-LDP are used as they reserves the share of bandwidth for some particular type of traffic.Authentication can be used for secure sharing between neighbor devices.CE-CE communication can be secured with the help of IPsec.LDP uses both TCP and UDP while CR-LDP uses TCP and RSVP uses Raw IP.LSP can be protected in LDP and CR-LDP by using IPsec between PE-PE, while RSVP uses SHA-1 based neighbor authentication for secure sharing.

- LDP is the best solution when only data traffic is used between source CE and destination CE, while RSVP is the best traffic engineering solution.
- RSVP and LDP has a refresh interval for LSP while CR-LDP doesn't have.

Multiprotocol Label Switching (MPLS) is the backbone of the internet .Almost all service providers use MPLS in their core network. PM Narendra Modi's DIGITAL INDIA mission has three basic components and those are Fibre optic cable, MPLS. So improving the performance of MPLS protocols will lead to the overall improvement of performance of internet.

ACKNOWLEDGMENT

This paper has been made possible through the regular hard effort and helps from guide and my family. I would like to thank Associate Prof. Er. Dinesh Kumar, for his guidance and help.

REFRENCES

[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] LDP Specification by L. Anderson of Nortel Networks, P. Doolan of Ennovate Networks, N. Feldman of IBM Corporation, A. Fredette of PhotonEx Corporation and B. Thomas of Cisco Systems in IETF RFC - 3036

[3] Fault Tolerance for the Label Distribution Protocol (LDP) by A. Farrel, Ed. of Movaz Networks in IETF RFC 3479

[4] Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) by L. Martini, Ed. , E. Rosen by Cisco Systems, N. El-Aawar of Level 3 Communications, T. Smith of Network Appliance Inc. and G. Heron of Tellabs in IETF RFC 4447

[5] Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling by M. Lasserre, Ed. , V. Kompella, Ed. of Alcatel Lucent in IETF RFC 4762

[6] LDP Specification by L. Anderson, Ed. , Acreo AB, I. Minie, Ed. of Juniper Networks and B. Thomas, Ed of Cisco Systems in IETF RFC 5036

[7] Constraint-Based LSP Setup using LDP by Jamoussi of Nortel Networks, L. Anderson, Utfors AB, R. Callon of Juniper Networks, R. Dantu of Netrake Corporation, L. Wu of Cisco Systems, P. Doolan of OTB Consulting Corporation, T. Worster, N. Feldman of IBM Corporation, A. Fredette of ANF Consulting, M. Girish of Atoga Systems, E. Gray, Sandburst, J. Heinanen of Song Networks, T. Kilty of Newbridge Networks and A. Malis of Vivace Networks in IETF RFC 3212

[8] LSP Modification Using CR-LDP by J. Ash of AT&T, Y. Lee of Ceterus Networks, P. Ashwood-Smith, B. Jamoussi, D. Fedyk, D. Skalecki of Nortel Networks, L. Li of SS8 Networks in IETF RFC 3214

[9] Resource ReSerVation Protocol (RSVP) by R. Braden, Ed. and S. Berson of ISI Networks, L. Zhang of UCLA, S. Herzog of IBM Research, and S. Jamin of University of Michigan in IETF RFC 2205 t

[10] RSVP Operation Over IP Tunnels by A. Terzis of UCLA, J. Krawczyk of ArrowPoint Communications, J. Wroclawski of MIT LCS, and L. Zhang of UCLA in IETF RFC 2746

[11] RSVP Cryptographic Authentication by F. Baker of Cisco Systems, B. Lindell of USC/ISI , and M. Talwar of Microsoft in IETF RFC 2747

[12] Support for Resource Reservation Protocol Traffic Engineering (RSVP-TE) in Layer 3 Virtual Private Networks (L3VPNs) by K. Kumaki, Ed. and P.Jiang of KDDI Corporation, T. Murai of Furukawa Network Solution Corporation, D. Cheng of Huawei Technologies, S. Matsushima of Softbank Telecom in IETF RFC 6882

[13] Fast Reroute Extensions to RSVP-TE for LSP Tunnels by P. Pan, Ed. of Hammerhead Systems, G. Swallow, Ed. of Cisco Systems, and A. Atlas, Ed. of Avici Systems in IETF RFC 4090

[14] S. Veni, Dr.G.M.Kadhar Nawaz and P.Praba, "Performance Analysis of Network Traffic Behavior in Conventional Network over MPLS", Proc of ICCCCT 2010 IEEE International Conference, Nagercoil, Tamil Nadu, India, pp. 222-226, 2010

[15] Understanding MPLS LDP Signaling Protocol - https://www.juniper.net/documentation/en_US/junos12.1x47/topics/concept/mpls-security-ldp-signaling-protocol-understanding.html