International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

QOS Capabilities for Building MPLS VPN

S. Maheshwarn[1], S. Lillypet[2], C. Vennila[3]

[1]M.E Communication System Final Year, Department of Information and Communication Engineering, P. R. Engineering College, Thanjavur-613 403

[2]Research Scholar, Associate Professor, Department of Information and Communication Engineering, P. R. Engineering College, Thanjavur-613 403

[3]Professor, Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy-620 012

Abstract: ***Multi Protocol label Switching (MPLS) is a core networking technology. It is also referred to as a layer 2.5 technology. A Virtual Private Network (VPN) provides private network connections over a publicly accessible shared network like internet, instead of using leased lines. MPLS is an innovative approach in which forwarding decision is taken based on labels. It also provides a flexible and graceful VPN solution based on the use of LSP tunnels to encapsulate VPN data. Multi-protocol Layer Switching (MPLS) VPNs are best solution for medium and large enterprises that currently deploy site-to-site VPN services. MPLS provides sophisticated traffic engineering capabilities. We present background on MPLS VPNs as well as QoS routing.***

Keywords: MPLS, QoS, OSPF, VPN, VRF

1. Introduction

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. A VPN provides varying levels of security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network, either through the use of a dedicated connection from one "end" of the VPN to the other, or through encryption. MPLS is the architecture for fast packet switching and routing by providing the designation, routing, forwarding and switching of traffic flow through the network. The new IP forwarding that can handle this situation is Multi Protocol Label switching (MPLS). This technology can give higher ability such as scale, traffic engineering capability and provides Quality of Services (QoS).

1.1 MPLS (Multiprotocol Label Switching)

In an MPLS network, incoming packets are assigned a "label" by a "label edge router (LER)". Packets are forwarded along a "label switch path (LSP)" where each "label switch router (LSR)" makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and apply a new label which tells the next hop how to forward the packet. Multiprotocol Label Switching (MPLS) has been here in communication industry for many years. As discussed in RFC-3031.MPLS is a way of tunnelling IP data-grams, within and among independent systems. It also treats the encapsulated IP datagram as raw data and does not access it in the tunnel.

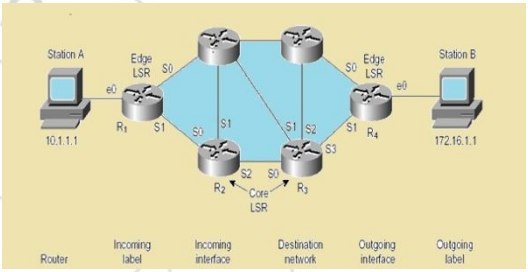

Figure 1: MPLS connection

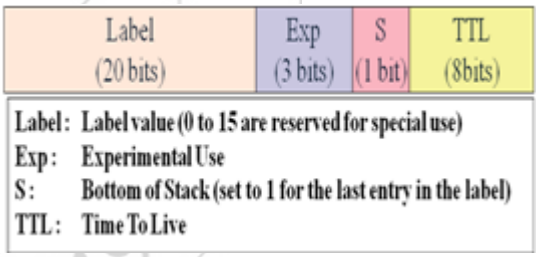

Figure 2: MPLS Label format

MPLS popularity has increased exponentially in the last few years. One of the most compelling drivers for MPLS in service provider networks is its support for Virtual Private Networks (VPNs), in which the provider's customers can connect geographically diverse sites across the provider's network .First thing people confuse is the usage of the words MPLS and VPN.

1.2 VPN (Virtual Private Network)

In a site-to-site VPN, hosts do not have VPN client software; they send and receive normal TCP/IP traffic through a VPN gateway. Nowadays, the network traffic growth rapidly, so the traditional networks like ATM, frame relay, Ethernet are not able to support this situation. So service provider discovers a new technology that solves this problem. The new IP forwarding that can handle this situation is Multi Protocol Label switching (MPLS). This technology can give higher ability such as scale, traffic engineering capability and provides Quality of Services (QoS). MPLS is regarded

as an enhancement to the traditional IP routing. This new technology is suitable for large network that requires optimal performance. Another reason why MPLS technology is important it that, it enables IP packet forwarding that support sophisticated packet classification and high rate data forwarding. For the next generation network, it is become the central element of network to be design with the high performance network with low cost. MPLS is the architecture for fast packet switching and routing by providing the designation, routing, forwarding and switching of traffic flow through the network.

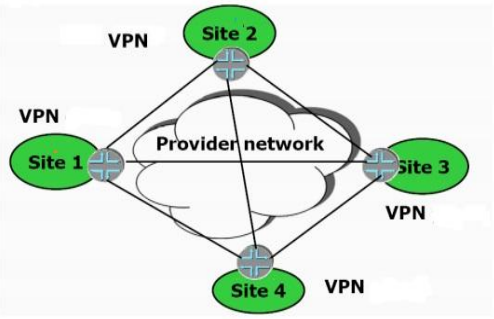

Figure 3: VPN connection

1.3 OSPF (Open Shortest Path First)

It can support up to FOUR equal cost paths and converges quickly. It uses partial updates with only the changes being flooded to the network. OSPF supports VLSM therefore OSPF is classless. It is good for very large networks i.e. those having a diameter of 15 hops or more. It makes good use of bandwidth; OSPF multicasts link-state updates – these are only sent when a topology change occurs. OSPF selects routes based on cost (bandwidth).

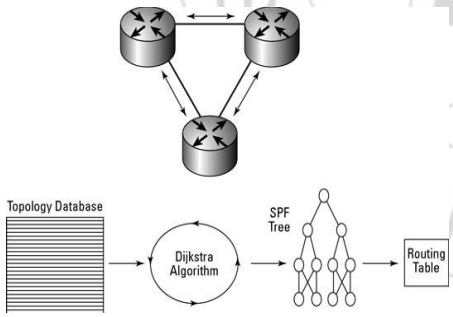

Fig 3: OSPF function

OSPF group's members into 'areas' and breaks the network into small clusters of routers. OSPF limits traffic regionally and can prevent changes in one area affecting another e.g. route flapping. Compare this with a RIP flat network.

2. MPLS VPN Connection

Splitting the different technologies into overlay and network based VPNs can help us to evaluate the current time real time problems such as the overlay arrangement doesn't support scalability of client connections. The problem in this case is because of the requirement policy for every connection from site to many sites, and routing adjacencies over these site to site connections. But in network based solutions sites are connected to locally attached PE routes. So, the network based category is more adoptable than overlay category. In 21st century, we moved toward the deployment of network-based Layer-3 VPN (2547bis) solution that is the main base line for MPLS VPN connection.

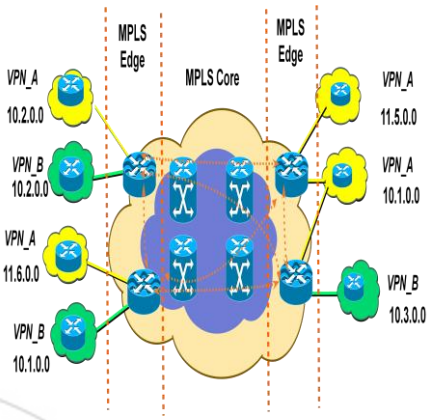

Figure 4: MPLS VPN connection

2.1 Traffic Engineering

Traffic engineering allows a network administrator to make the path deterministic and bypass the normal routed hop-by-hop paths. An administrator may elect to explicitly define the path between stations to ensure QoS or have the traffic follow a specified path to reduce traffic loading across certain hops. The network administrator can reduce congestion by forcing the frame to travel around the overloaded segments. Traffic engineering, then, enables an administrator to define a policy for forwarding frames rather than depending upon dynamic routing protocols. Traffic engineering is similar to source-routing in that an explicit path is defined for the frame to travel. However, unlike source-routing, the hop-by-hop definition is not carried with every frame. Rather, the hops are configured in the LSRs ahead of time along with the appropriate label values.

2.2 LER (Label Edge Router)

Label Edge Routers are working as the gateways of MPLS Domain. Ingress LER, it receives the IP Packet from CE, assigns the appropriate Label. After wrapping label, it sends labelled packet towards the next hop through the Label Switched Path, which is assigned for the specific Forward Equivalence Class. Assigning the Label is known as Label Binding.

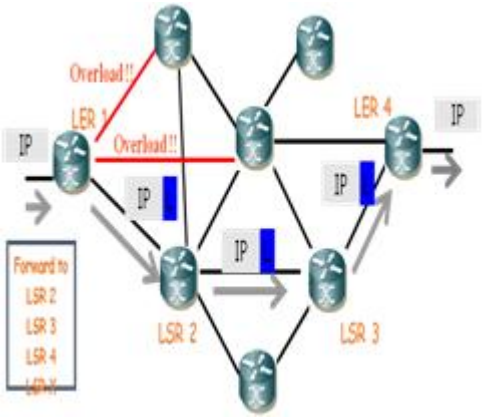

Figure 5: Traffic Engineering

2.3 LSR (Label Switched Router)

Label Switched Routers are basically working as transit switches in MPLS cloud. It receives Labelled IP packets through the appropriate LSP. It analyses the Label bound over the packet, consults the forwarding information table (LIB) and routes the packet through the appropriately mapped out going LSP. When the LSR is routing the packets from incoming LSP to outgoing LSP, it strips out the Incoming Label and assigns a new label to same packet to ensure the security from the intruders. This process is known as Label Swapping or Label Changing. MPLS Network architecture is as shown in the diagram. Lines, shown between CE and LER carry the IP Packets bi-directionally.

2.4 Signalling Mechanism

- Label request—using this mechanism, an LSR requests a label from its downstream neighbor so that it can bind to a specific FEC. This mechanism can be employed down the chain of LSRs up until the egress LER (i.e., the point at which the destined packet exits the MPLS domain).
- Label mapping—In response to a label request, a downstream LSR will send a label to the upstream initiator using the label mapping mechanism.

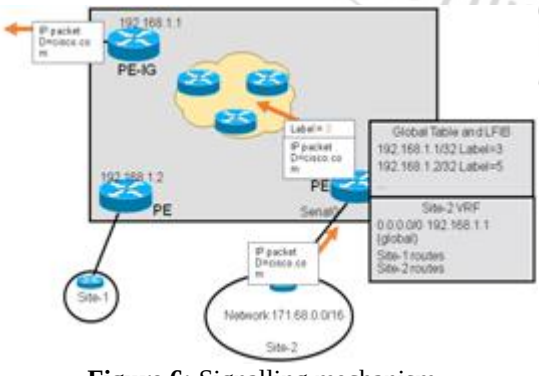

Figure 6: Signalling mechanism

2.5 Communication of Sits

Label Switched Routers are basically working as transit switches in MPLS cloud. It receives Labelled IP packets through the appropriate LSP. It analyses the Label bound over the packet, consults the forwarding information table (LIB) and routes the packet through the appropriately mapped out going LSP. When the LSR is routing the packets from incoming LSP to outgoing LSP, it strips out the Incoming Label and assigns a new label to same packet to ensure the security from the intruders. This process is known as Label Swapping or Label Changing. MPLS Network architecture is as shown in the diagram. Lines, shown between CE and LER carry the IP Packets bi-directionally.

- PE-Provider Edge router
- CE-Customer Edge Router

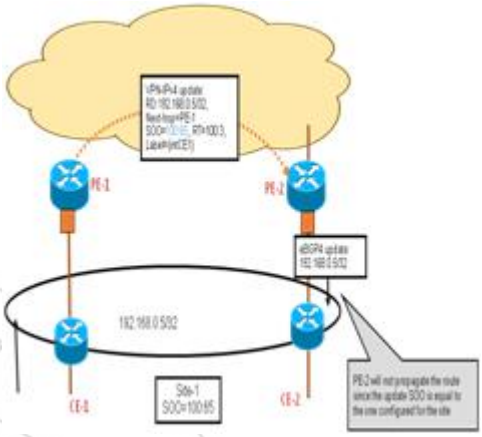

Figure 7: Communication of site

3. Proposed System

MPLS VPN is the technology which is alternative to all other old-fashioned VPN like leased lines, IP tunnels. It is cost effective and provides better flexibility and scalability. Though it is best available solution, it has some drawbacks. Also if we use extra features like QoS, traffic engineering, the throughput of overall architecture will be more. The integration of MPLS VPN with QoS will provide both customer and service provider the new and better option to connect the remote sites. Here we are suggesting few enhancements which will improve overall performance and will provide secure connection.

A. 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 (Internet Protocol Security). IPSEC can be used in conjunction with MPLS to provide high level of encryption.

B. 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. Possible these authentication mechanisms should be deployed to maintain integrity.

C. QoS (Quality of Service)

QoS for web services is becoming more and more vital to service providers. But due to the dynamic and unpredictable characteristics of the web services, it is very difficult duty to offer the desired QoS for web service users. Additionally, different web service applications with dissimilar QoS

necessities will fight for network and system resources such as bandwidth and processing time. However, an enhanced QoS for MPLS VPN will bring competitive advantage for service provider. To provide such a better QoS, it is first necessary to identify all the possible QoS requirements for VPN, which is the objective of this document. This paper discusses possible approaches for supporting VPN with QoS. The QoS requirements for VPN here mainly refer to the quality that the customer will experience. These may include performance, reliability, scalability, capacity, robustness, exception handling, accuracy, integrity, accessibility, availability, interoperability, security, and network-related QoS requirements.

4. Configuring Simulation Model

Within an MPLS domain, a path is set up for a given packet to travel based on an FEC. The LSP is set up prior to data transmission. Lines, shown in the MPLS domain, are the Label Switched Paths that carry labelled IP Packets between the routers. There are two types of Label Switched Path. One is Static LSP and the other is Signalled LSP.

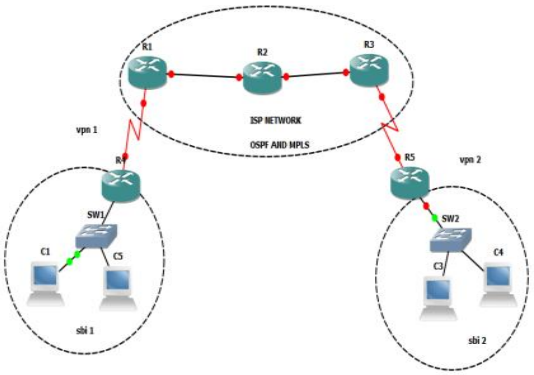

Figure 8: Network simulation model

4.1Configure MPLS VPN

A. Configuring the CE Router

Configuration of the CE router is very simple. The only restriction is that the routing protocol used between the CE and PE routers must currently be RIP version 2, EIGRP, OSPF, or EBGP. Static routes can also be used. The CE router is not necessary to be MPLS enabled. We have OSPF between CE and PE in our simulation.

B. Configuring the PE Router

Configuration of the PE router is much more complicated than that of the CE router. There are7 basic steps involved and they are as follows.

1) Configure the loopback interface to be used as the BGP update source and LDP router ID.
2) Enable CEF (configure) # Ip Cef
3) Configure the label distribution protocol. (Configure) # Mpls label protocol Ldp.
4) Configure the TDP/LDP router-id (optional). (Configure) # Mpls Ldp router-id loopback0
5) Configure MPLS on core interfaces. (Configure) # Mpls Ip
6) Configure the MPLS VPN backbone IGP.
7) We have used OSPF as backbone IGP. We can use any IGP.
8) Configure global BGP parameters.

4.2 Output and result

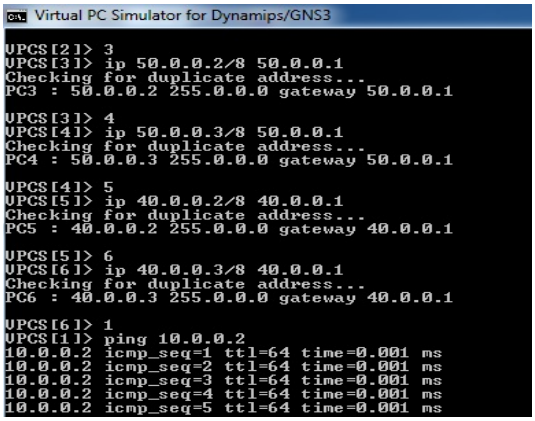

Figure 9: simulation output

The above simulation ping modules are show MPLS VPN communication routing.

5. Conclusion

The internet is said to be expanding and need for support for file, transfers of corporate company's become vital this L3VPN4 process of utilizing layer 3 of the OSI enables the VPN services provided to the corporate to enhance itself and provide the ability to provide better resource management higher quality of service(QoS) and security. This project plays a Key role in next generation networks by delivering high efficient traffic engineering features and high reliable connectivity in secure L3VPN layered network which enable the network to perform well even in heavy traffic environments. Thus the L3VPN network results better resource management Quality of service (QoS) with security.

References

[1] https://en.wikipedia.org/wiki/Virtual_private_network.
[2] Cisco "MPLS VPN Technology" Chris Metz" The Latest in VPNs: Part II" Published by the IEEE Computer Society May 2004.
[3] Yoo-Hwa Kang , and Jong-Hyup "The Implementation of the Premium Services for MPLS IP VPNs".
[4] LeeYanfei Zhao, Zhaohai Deng" A Design of WAN Architecture for Large Enterprise Group Based on MPLS VPN" 2012 International Conference on Computing, Measurement, Control and Sensor Network.
[5] M.Hachimi, M.-A Breton, and M. Bennani, "Efficient QoS Implementation for MPLS VPN," International Conference on Advanced Information Networking and Applications, pp. 259-263,March 2008.
[6] Muhammad Romdzi "Implementation of Quality of Service (QoS) in Multi Protocol Label Switching (MPLS) Networks" 2009 5th International Colloquium on Signal Processing & Its Applications (CSPA).

[7] Tim Wu, "MPLS VPNs: Layer 2 or Layer 3? Understanding the Choice", Riverstone Networks, 2002.
[8] Dr. Hosein F. Badran, "Service Provider Networking Infrastructures with MPLS" in Sixth IEEE Symposium on Computers and Communications (ISCC'01) July 05, 2001.
[9] E. Rosen, Y. Rekhter, "BGP/MPLS VPNs" RFC 2547, March 1999.
[10] K. Hamzeh, G. Singh Pall, W. Verthein, J. Taarud, W.A. Little: Point-to-Point Tunneling Protocol – PPTP, IETF draft: draft-ietf-pppext-pptp-02.txt, 1997. [7] S. Hanks, T. Li, D. Farinacci, P. Traina "Generic Routing Encapsulation over IPv4 networks", RFC1702, 1994.
[11] E. Rosen, Y. Rekhter: "BGP/MPLS VPNs", RFC 2547, 1999. S. Previdi: "Introduction to MPLS-BGP-VPN", Proceedings of MPLS Forum 2000, 2000.
[12] G. Heron, L. Martini: "An Architecture for L2VPNs", IETF draft: draft-ietf-ppvpn-12vpn- 00.txt, 2001.
[13] R. Pulley: "Implementing VPNs Using MPLS", Proceedings of MPLS Forum 2000, 2000.

Author Profile

Mr.S.Maheshwaran received B.E in electronics and communication P.R. Engineering College, Thanjavur in 2013. He is currently doing M. E in Communication Systems from Anna University, Thanjavur, India. He has presented papers in international conferences and published papers in international journals.

Mrs.S.Lillypet M.E, pursuing Ph.D in Anna University Chennai, Tamilnadu, India. She is currently working as Associative Professor in P.R. Engineering College, Thanjavur, India. Her research interest Free Space Optics in wireless communication.

Mrs.Dr.C.Vennila M.E,,Ph.D. she has done Ph.D in National Institute of technology. She is currently working as Professor in Saranathan College of Engineering, Trichy, India. Her research area is VLSI Systems.