ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Implementation of Multi Protocol Label Switching – Virtual Private Network for Corporate Networks

M. Kanmani[1], S.Beulah Hemalatha*[2]

Assistant Professor, Dept. of ECE, Jerusalem College of Engineering, Chennai, Tamil Nadu, India[1]

Assistant Professor, Dept. of ECE, Bharath University, Chennai, Tamil Nadu, India[2]

* Corresponding Author

ABSTRACT: Recently MPLS is used for building up VPNs in IP backbone, called MPLS VPN. To provide people with voice, data and all categories of multimedia services, distinguishing between data flows is a requirement. To address these router performance, Quality of Service and traffic engineering issues, Multi - Protocol Label Switching (MPLS) was proposed for IP based internetworks. To achieve the security that is required for corporate users, Virtual Private Networks (VPNs) can be used to guarantee that traffic is securely tunneled over the Internet. MPLS based VPNs enable connectionless routing within each VPN community. This paper discusses the benefits available in IP VPNs and how the MPLS+BGP model is selected in the network. Then how a branch office connects itself to other offices using MPLS VPN services delivered by a service provider.

I. INTRODUCTION

With the rapid development of the Internet, there arises great interest in the deployment of Virtual Private Networks (VPNs) across IP networks. Multi-Protocol Label Switching (MPLS) is an innovative technique for high performance packet forwarding. There are many uses for this technology, both within a service-provider environment and within the enterprise network, and the most widely deployed usage today is the enabling of VPNs. With the introduction of MPLS-enabled VPNs, it is possible to provide better scale for their networks than with the methods available in the past. MPLS is believed to be a key technology for building up VPNs (i.e. MPLS VPNs) due to a number of reasons as follows:

- MPLS offers fast forwarding capability.
- MPLS connects sites through setting up label switch paths (LSPs) on which traffic engineering can be applied.
- Data can easily be recognized and prioritized to ensure Quality of Service for voice and video applications.
- The labels can include information about the source application of the data and effectively which user or organization the data "belongs to".
- MPLS is capable of scaling into very large networks.

QoS is regarded as a key element of any VPN services. This paper discusses the issues of QoS in MPLS VPNs and how it achieves security equivalent to that of Frame Relay and ATM.

1.1 Background of MPLS VPN

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet [1]. A VPN enables us to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork, while maintaining secure

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

communications [2]. The VPN connection across the Internet logically operates as a wide area network between the sites. There are two different methods to construct VPNs across IP backbone.i.e. Customer Premises Equipment (CPE) and network based. Most current VPN implementations are based on CPE equipment. On the other hand, in network based VPNs, the operation of VPN is outsourced to an Internet Service Provider and is implemented on network as opposed to CPE equipment [3].

Multi-Protocol Label Switching (MPLS) is an innovative technique for high performance packet forwarding. The path created in an MPLS network is called a label switched path. Each MPLS enabled router in the network is considered a label switching router [4]. Finally, the actual forwarding of packets is accomplished using a header value that contains a numeric label value. The forwarding of user data traffic through an MPLS network is accomplished by label values assigned by the MPLS routers themselves. This assignment occurs in an upstream direction. The downstream router informs the upstream router what label value to use when sending traffic along LSP. When the downstream router receives that label value, it swaps the label with the value assigned by its downstream router. [5] This exchange of labels between two routers on a single link results in the label value having local significance only.

1.2 MPLS VPN

MPLS is becoming a widely deployed technology, specifically for providing VPN services. Security is a major concern for companies migrating to MPLS VPNs from existing VPN technologies such as ATM [6].

Principles of MPLS VPN Network

1. MPLS networks are smarter than IP networks.

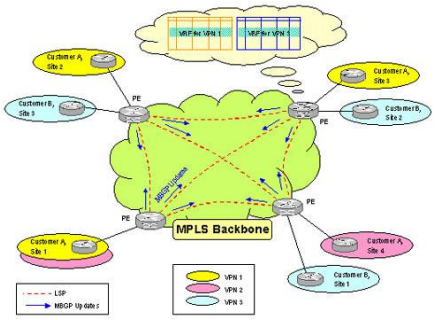
2. When IP traffic from a source network enters an MPLS network, it is classified and assigned a label by a label edge router, converting the IP packet into an MPLS packet.

3. The labeled packet is then forwarded along a label switch path to a label switch router which in turn forwards the packet using instructions on the label.

4. At each hop, the label is removed and a new one is added before the packet is passed on.

5. When the packet reaches the edge of the MPLS network, the label is removed, unencapsulating the packet and reconverting it into an IP packet.

6. It is then forwarded onto the destination network as a normal IP packet.



PE = Provider Edge Router

Fig. 1 MPLS VPN Architecture

II. DATA AND ROUTING SEPARATION BETWEEN VPN

It is a requirement for enterprises that the address apace between the MPLS core and all VPNs on the same shared network be independent, so that each customer can use the same address space without interfering with other customers [9]. That is, every VPN customer and the core itself must be able to use the entire Ipv4 address range completely independently. Similarly, data traffic from each VPN must remain separate, never flowing to another VPN. A related requirement is that routing information for one VPN instance must be independent from any other

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

VPN instance and from the core. This requirement applies as well to distribution and processing of routing information.

2.1 Routing Separation

To achieve routing separation among VPNs, MPLS VPNs apply the following principles:

1. Each VPN is assigned to a Virtual Routing and Forwarding (VRF) instance – Every provider-edge router maintains a separate VRF instance for each connected VPN [7]. Each VRF on the provider-edge router is populated with routes from one VPN, either through statically configured routes or through routing protocols that run between the provider-edge and the customer-edge router. Because every VPN is associated with a separate VRF, there is no interference among the VPNs on the provider-edge router [8].
2.
3. Unique VPN identifiers – To maintain routing separation across the core to the associated provide-edge routers, unique VPN identifiers such as the route distinguisher are added to the multiprotocol Border Gateway Protocol (BGP). VPN routes are exchanged across the core only by multiprotocol BGP. This BGP information is not distributed again to the core network, but only to the associated provider-edge routers, which keep the information in VPN=specific VRFs. Thus, routing across a MPLS network remain separate for each VPN [10].

2.2 Traffic Separation

MPLS-based VPNs adhere to the "true peer VPN" model – that is, they perform traffic separation at Layer 3 through the use of separate IP VPN forwarding tables. MPLS-based VPNs enforce traffic separation between customer by assigning a unique VRF to each customer's VPN [11]. Forwarding within the service provider backbone is based on labels; MPLS sets up label-switched paths (LSPs), which begin and terminate at the provider-edge routers. (Normal routing, in contrast, is performed by customer-edge routers). The provider-edge router determines which forwarding table to use when handling a packet because each incoming interface on a provider-edge router is associated with a particular VPN. Therefore, a packet can enter a VPN only through an interface that is associated with that VPN.

By maintaining separation among addressing plans, routing and traffic, the MPLS VPN core network architecture the same security as comparable ATM or Frame Relay-based L2VPNs. It is not possible to intrude into other VPNs or the core through the MPLS VPN network.

2.3 QoS Routing in MPLS VPNs

MPLS supports explicit paths and alternative paths so that QoS routing can be naturally used in MPLS VPNs. QoS routing might be used in such cases as finding routes for connecting a number of sites into a VPN or setting up paths for sessions within VPNs. QoS routing is also believed to be one of the key components for supporting QoS in MPLS VPNs.

III. MPLS VPN SECURITY MODEL ARCHITECTURE

When comparing MPLS VPN based solutions to traditionally layer 2 based VPN solutions such as Frame Relay and ATM, several key security requirements need to be addressed:

- It is necessary to have addressing and routing separation.
- The internal structure of the backbone network must be hidden from the outside. Just as a Frame-Relay or ATM network core is hidden, so must an MPLS – VPN core.
- The network must have resistance to attacks, both Denial-of-Service (DoS) and intrusion attacks.

3.1 Address and Routing Separation

MPLS-VPNs allows the use of private or public addressing. This is possible by adding a 64 bit route distinguisher (RD) to each IPv4 route. This new route called a "VPN-IPv4 address" ensures that VPN unique addresses are also unique in the MPLS core. The only exception here is the IP addressing of the PE to CE links, they will need to be unique if using dynamic routing protocols.

Routing separation between customers is also a necessity. MPLS provides route separation by having each PE router maintain a separate routing table for each connected VPN. This routing table called a Virtual Routing and

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Forwarding (VRF) instance contains the routes from one VPN that were learned statically or through dynamic routing protocols. These VRFs are separate from each other as well as from global routing table.
To prove that MPLS based VPNs provided both addressing and routing separation examination of the routing table of every CE, PE and P router can be carried out. On the CE routers, the routes that belong solely to the VPN that the CE was a member of and there are no routes to other VPNs or the core are examined. The same steps are repeated on the PE routers by verifying that every VRF routing table contained the same information. On the P routers verification of no VRF routing tables and the only routes that appeared were to other routers in the providers network.

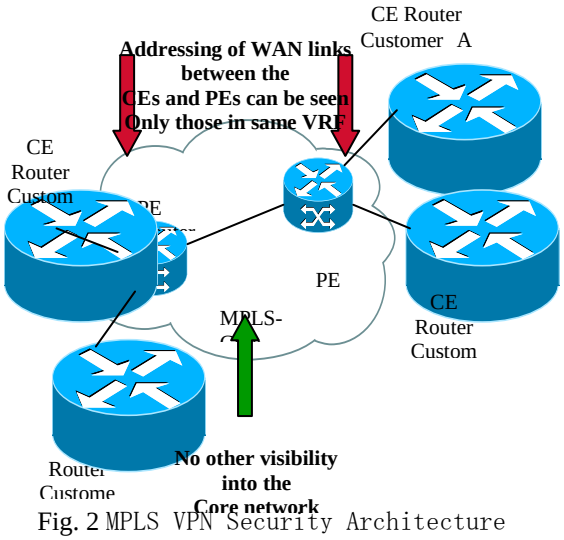


Fig. 2 MPLS VPN Security Architecture

3.2 Resistance to Attacks

Two potential ways to attack MPLS-VPN are first by attempting to attack the PE routers directly, and second by attempting to attack the signaling mechanisms of MPLS. Traffic isolation prevents an attack across VPN boundaries.

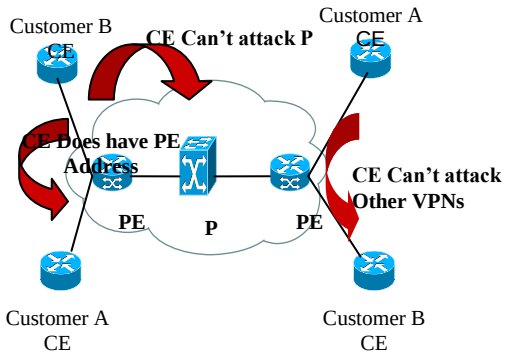


Fig. 3 DoS Diagram

In order to attack the PE routers directly it is necessary to know its address. As discussed in hiding the MPLS Core it is possible to hide the addressing structure of the MPLS core from outside world except when running a dynamic routing protocol.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

In this case the router will know at least the router ID of the PR router in the core. If an attacker does not know the IP address of any router in core the attacker now has to guess addresses and send packets to these addresses. However, due to the address separation of MPLS each incoming packet will be treated as belonging to the address space of the customer. Thus it is highly difficult to reach an internal router even through IP address guessing.

IV. IMPLEMENTATION

The steps involved in implementation of MPLS-VPN are as follows: Connect port 0 of CHENNAI_PE router to CE router and port 1 to port 0 of CORE_ROUTER. Port 1 of CORE_ROUTER is connected to port 1 of BANGALORE_PE (B'LORE_PE) and port 0 of B'LORE_PE is in turn connected to CE router. Assign the IP address of the network as shown in the architecture. Specify the Router_ID of CHENNAI_PE, CORE_ROUTER AND B'LORE_PE as 97.251.224.1, 10.0.0.1 and 97.251.22.1 respectively. After assigning the IP address establish OSPF for all the routers and check whether packets are transmitted from source to destination customer via routers using ping commands.

After configuration, analyze the router traffic using MRTG tool. The performance characteristics of configured MPLS VPN such as its availability, data volume, incoming and outgoing traffic, Data volume, Traffic volume and any breakdown were analyzed using InfoVista tool.

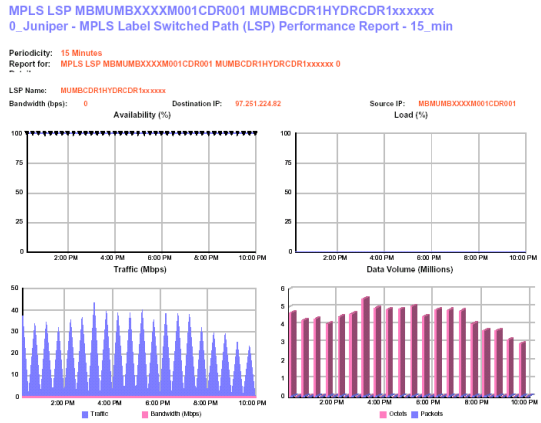


Fig. 4 LSP Performance Report-1 from source to destination

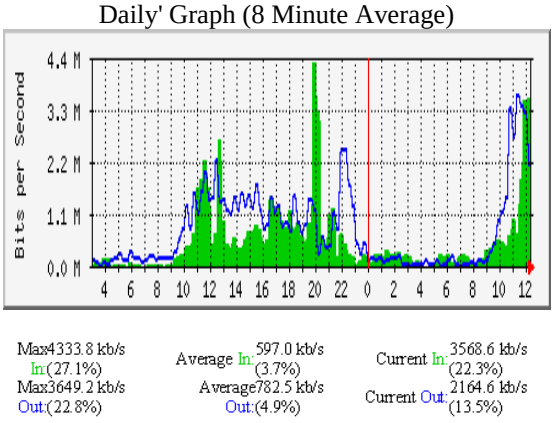


Fig. 5 Analyzing incoming and outgoing traffic of PE router

V. CONCLUSIONS

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

MPLS is likely used in VPNs due to the distinguished merits, e.g., fast forwarding, tunneling etc. MPLS VPN networks provide full address and traffic separation, and hide addressing structure of the core network and the VPNs. It is not possible from the outside to intrude into the core network or VPNs by abusing the MPLS mechanisms. Neither is it possible to intrude into a properly secured MPLS core. There is, in fact, one significant difference between VPNs based on MPLS and those based on Frame Relay or ATM. That is, the control structure of the core is on Layer 3. This initially raised concerns that the architecture could be open to DoS attacks from other VPNs or the Internet. This paper has demonstrated that it is possible to secure an MPLS infrastructure as that of ATM or Frame Relay services. It is also possible to offer Internet connectivity to MPLS-based VPNs in a secure manner.

REFERENCES

1. "Murali Kodialam and T.V. Lakshman", Minimum Interference Routing with Applications to MPLS Traffic Engineering", in Proc. IEEE INFOCOM 2000, pp. 884 – 893.
2. Sengottuvel P., Satishkumar S., Dinakaran D., "Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling", Procedia Engineering, ISSN : 1877-7058, 64() (2013) pp.1069-1078.
3. "Uyless Black", MPLS and Label Switching Networks, Pearson Education Inc., Second Edition.
4. Muruganantham S., Srivastha P.K., Khanaa, "Object based middleware for grid computing", Journal of Computer Science, ISSN : 1552-6607, 6(3) (2010) pp.336-340.
5. "Douglas E. Comer", Internetworking with TCP/IP, Vol. 1, Prentice Hall of India, Fourth Edition.
6. Anbazhagan R., Satheesh B., Gopalakrishnan K., 'Mathematical modeling and simulation of modern cars in the role of stability analysis", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4633-4641.
7. "George Sackett", Cisco Router Handbook, Tata McGraw Hill, Second Edition.
8. Rajendran S., Muthupalani R.S., Ramanathan A., "Lack of RING finger domain (RFD) mutations of the c-Cbl gene in oral squamous cell carcinomas in Chennai, India", Asian Pacific Journal of Cancer Prevention, ISSN : 1513-7368, 14(2) (2013) pp.1073-1075.
9. "Carlton R. Davis", IPSec Securing VPNs,Tata McGraw Hill, Edition 2001.
10. Langeswaran K., Revathy R., Kumar S.G., Vijayaprakash S., Balasubramanian M.P., "Kaempferol ameliorates aflatoxin B1 (AFB1) induced hepatocellular carcinoma through modifying metabolizing enzymes, membrane bound ATPases and mitochondrial TCA cycle enzymes", Asian Pacific Journal of Tropical Biomedicine, ISSN : 2221-1691, 2(S3)(2012) pp.S1653-S1659.
11. "Y.Rekhter, T. Li", A Border Gateway Protocol4, RFC 1771, T.J. Watson Research. Center, IBM Corp, Cisco Systems, March 1995.
12. B Karthik, TVUK Kumar, MA Dorairangaswamy, E Logashanmugam, Removal of High Density Salt and Pepper Noise Through Modified Cascaded Filter, Middle East Journal of Scientific Research, 20(10),pp 1222-1228, 2014.
13. Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Applications of fMRI for Brain MappingarXiv preprint arXiv:1301.0001, 2012.
14. Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Respiratory rate, heart rate and continuous measurement of BP using PPGIEEE Communications and Signal Processing (ICCSP), 2014 International Conference on, PP 999-10022014.
15. Kamatchi, S; Sundhararajan, M; , Optimal Spectral Analysis for detection of sinusitis using Near-Infrared Spectroscopy (NIRS) .
16. Shriram, Revati; Sundhararajan, M; Daimiwal, Nivedita; , Human Brain Mapping based on COLD Signal Hemodynamic Response and Electrical NeuroimagingarXiv preprint arXiv:1307.4171, 2013
17. [17]Daimiwal, Nivedita; Sundhararajan, M; Shriram, Revati; , Comparative analysis of LDR and OPT 101 detectors in reflectance type PPG sensorIEEE Communications and Signal Processing (ICCSP), 2014 International Conference on, PP 1078-1081,2014