Establishing Private Network Over Public Infrastructure Using Multi Protocol Label Switching Technology over Ipv6

D.Sathishkumar[1], V.Elavarasi[2], S. Chitra[3], D.Vaidehi[4],
1PG scholar,E.G.S.Pillay engineering college ,Nagapattinam
2Asst Professor,E.G.SPillay engineering college ,Nagapattinam
3Asst Professor,E.G.SPillay engineering college ,Nagapattinam
4Sub Divisional Engineer,RGMTTC,Chennai

Abstract---Traditional IP based networks, Frame Relay and ATM networks have many disadvantages in the management operation of large networks such as cost, security, scalability and flexibility. To solve this, an MPLS-based VPN networking is introduced that can work with existing deployed backbones and allow organizations to interconnect the dispersed sites and remote workers through secure links by using public internet. In this paper we tried to provide a better understanding of services provider large networks management operation; through focusing on the MPLS VPN technology. To get familiar with the MPLS VPN networks behaviour , we chose the interaction between routing protocols as a case study to evaluate the MPLS VPN networks performance. This work mainly focus on studying the effect of the interior gateway routing protocols in the MPLS VPN networks. We chose famous protocols for investigation (OSPF) and we proposed two different scenarios and simulated them by using GNS3,VPCS,,WIRESHARK, then a deep analyses of the network performance was provided.

Keywords--VPN,MPLSVPN,OSPFv3,RIPng ,LDP,LSR, LER

I. INTRODUCTION

Multiprotocol Label Switching (MPLS) has been around for several years. It is a popular networking technology that uses labels attached to packets to forward them through the network. The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching. The label switching technique is not new. Frame Relay and ATM use it to move frames or cells throughout a network. In Frame Relay, the frame can be any length, whereas in ATM, a fixed length cell consists of a header of 5 bytes and a payload of 48 bytes.

The header of the ATM cell and the Frame Relay frame refer to the virtual circuit that the cell or frame resides on. The similarity between Frame Relay and ATM is that at each hop throughout the network, the “label” value in the header is changed. This is different from the forwarding of IP packets. When a router forwards an IP packet, it does not change a value that pertains to the destination of the packet; that is, it does not change the destination IP address of the packet. The fact that the MPLS labels are used to forward the packets and no longer the destination IP address have led to the popularity of MPLS.

MPLS is an improved method for forwarding packets through a network using information contained in labels attached to IP packets. The labels are inserted between the Layer 3 header and the Layer 2 header in the case of frame based Layer 2 technologies, and they are contained in the virtual path identifier (VPI) and virtual channel identifier (VCI) fields in the case of cell-based technologies such as ATM.

MPLS combines Layer 2 switching technologies with Layer 3 routing technologies. The primary objective of MPLS is to create a flexible networking fabric that provides increased performance and stability. This includes traffic engineering and virtual private networks (VPN) capabilities, which offer quality of service (QoS) with multiple classes of service (CoS). In Figure 1, MPLS network incoming packets are assigned a label by an Edge Label-Switched Router. Packets are forwarded along a *Label-Switched Path (LSP)* where each *Label-Switched Router (LSR)* makes forwarding decisions based solely on the label's contents.

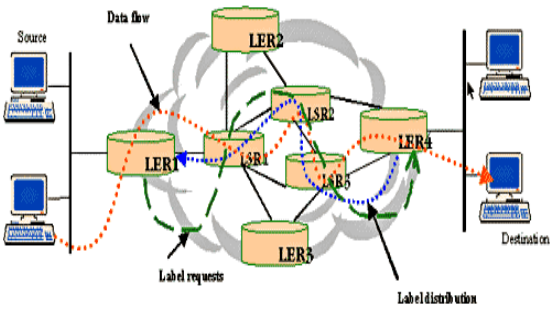


Fig1.MPLSnetwork.

MPLS-based VPNs use a combination of connectionless VPNs between the customers and service providers (thus minimizing the provisioning complexity and cost) with connection-oriented VPNs in the network core (reducing the overhead on the P devices). Furthermore, several additional mechanisms have been implemented to allow the customers to use overlapping address spaces. In a typical MPLS-VPN network, the customer edge (CE) routers and provider edge (PE) routers exchange the customer routes using any suitable IP

ISSN: 2278 – 909X

routing protocol. These routes are inserted into VRFs on the PE routers, which guarantees the perfect isolation between customers.

In this work we tried to investigate the effect of the interior routing protocols in the performance of the MPLS VPN networks. The Interior Gateway Protocols (IGPs) allow routers to exchange information within an autonomous system (AS). Examples of these protocols are Open Short Path First (OSPFv3), Routing Information Protocol. After deep study of the most popular routing protocols, we decide to choose the OSPF routing protocols as a case study to analyze the effect of the BGP in the MPLS VPN networks since they used frequently in the large scale enterprise networks.

II.RELATED WORK.

During the preparing of this paper and to reach the state of art for the effect of the IGPs in the MPLS VPN many related scientific papers where studied.

Ref [1], the authors Tried to provide a better understanding of services provider large networks management operation; through focusing on the MPLS VPN technology. presented an efficient QoS configuration scheme for MPLS based VPNs services. From their study they proved the efficiency of the QoS scheme proposed for MPLS VPN.

Ref[2], the paper We have examined characteristics of proposed models for the IPv6 support on MPLS networks, and selected the ”6PE technology” as an initial support of IPv6 in MPLS networks. mainly comprehensively presented an overview of MPLS,BGP and, both layer 2 and layer 3 VPNs. In particular, IP VPNs issues such as speed, scalability and security are discussed in details. then , the paper proposed a new design scheme for MPLS/BGPVPNs by merging the features of layer-3 (such as scalability and intelligence) with the features of layer-2 (such as efficiency and simplicity).

Ref[3], the authors presented a detailed descriptions of MPLS VPN networks and suggested a MPLS VPN network for a VoIP services design, then they provided a performance analyses of the proposed design according to the interior gateway protocols (RIP, OSPF).

Ref [4], the paper mainly focused in the interactions between BGP and OSPF in a large scale networks. This analyzes the performance of VoIP traffic in (BGP) - (MPLS) IP (VPN) between two interior routing protocols namely Enhanced Interior Gateway Protocol (EIGRP) and Open Shortest Path First (OSPF).

III. SIMULATION SCENARIOS

To get a clear and better understanding of the behaviour of MPLS VPN network according to the chosen interior gateway protocol (OSPF or RIP) used in it, we proposed two different network scenarios and implemented them in GNS3 simulation tool.

First design: Medium service provider MPLS VPN network backbone with interior gateway protocol and exterior gateway protocol (BGP). Figure.2 shows the simulated scenario have a for medium MPLS VPN network having a 2 branches company need to be connected with each other via service provider MPLS VPN cloud network. Each site contains three routers and the MPLS VPN network has four routers.

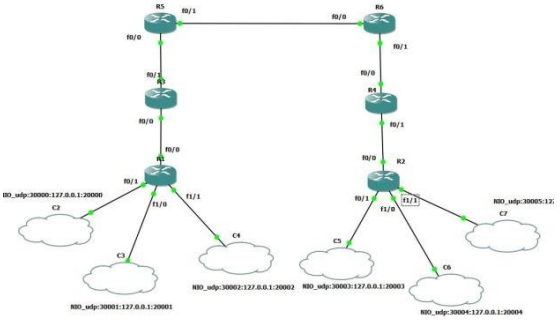


Fig. 2 Medium Service Provider Network

This scenario was made by using two autonomous systems:1.Service provider autonomous system named AS-1 contains of:

a) Two provider edge (PE) routers for receiving and transmitting data from the customer sites router through the MPLS VPN backbone.

b)Three provider (P) routers which handling the traffic and routing through the service provider network.

2.Customer autonomous system called AS-1 contains an enterprise network named S Microsystems Company and each site have:

a) Customer edge router: to transmit and receive data for service provider network.

b)Two Customer routers. To make a communication between each company site *Virtual Private Network* through MPLS cloud is used and named *VPN red* as shown in Figure 3:

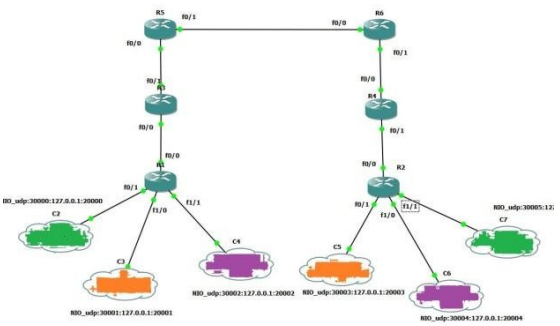


Figure 3: Medium Service Provider Network *VPN*

ISSN: 2278 – 909X

Second Design: Large service provider MPLS VPN network backbone with interior gateway protocol and exterior gateway(BGP), as shown in Figure4. This scenario consists of four autonomous systems: 1. Service provider autonomous system named AS-1 includes:
1.Four provider edge (PE) routers. 2. Four provider (P) routers.
2. First customer autonomous system named AS-2 contains aenterprise network belongs to company1which have two sites need to be connected via MPLS VPN, each site has:
1. Customer Edge router (CE). 2. Two customer clouds.
3. Second customer autonomous system named AS-3 contains an enterprise network belongs to company 2 which have two sites need to be connected via MPLS VPN, each site has:
1. Customer Edge router (CE). 2. Two customer clouds.

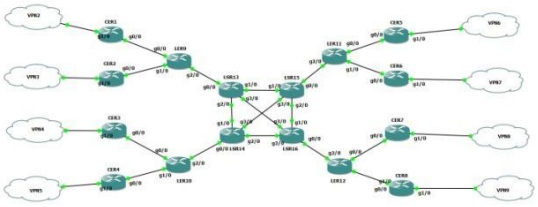


Fig.4.Large Service Provider Network

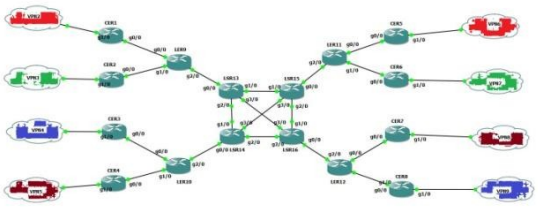


Fig.5.Large Service Provider Network VPN

Links between any route are GIGA Bit ETHERNET (1000Mbps) link. Each scenario was implemented for two times according to the IGP used, one time by using OSPF and other time by using.

IV. CONFIGURATIONS

A. MPLS routers configuration:

Each router has to be capable to enable MPLS as shown in Figure6. in addition, the providers edge (PE) routers must be configured with exterior gateway routing protocols (BGP) between all PEs, i.e. all PEs are BGP neighbours as shown in Figure 6 ,and IGP (OSPF or RIP) to communicate with other provider (P) router. Provider routers need to be configured with the same IGP used for PEs routers:

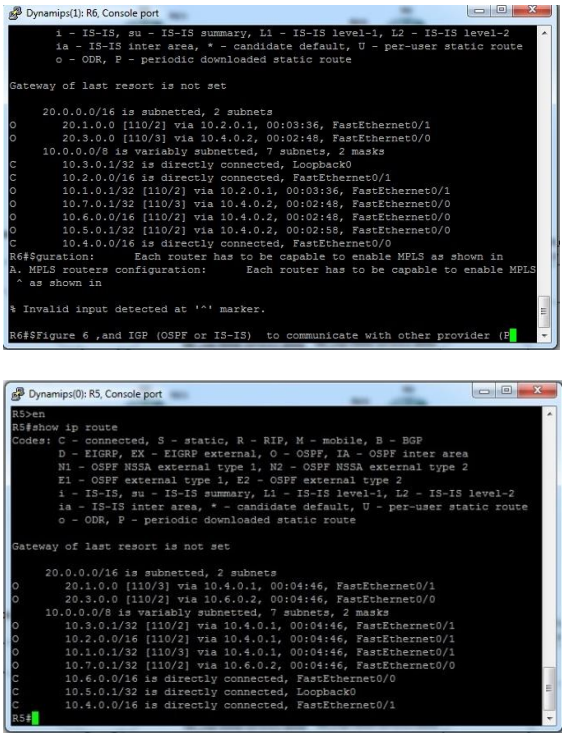


Fig.6.MPLS and BGP configuration

B. VPN Configuration:

VPNs in both scenarios have the same configurations settings ,the first scenario have just one VPN named red VPN and the second scenario have two VPN's named green VPN and blue VPN. Figure7 shows the initial configuration:

Fig.7 VPN Configuration.

Test Parameters:
To get a fair judgment about which IGP protocol is the best to be used in MPLS VPN networks, and to illustrate the effect of the IGP in MPLS VPN networks, many factors have been examined and these factors classified as: 1.Parameters related to the protocol itself:(convergence time).2.Parameters related to the VPN:(delay ,load and throughput).

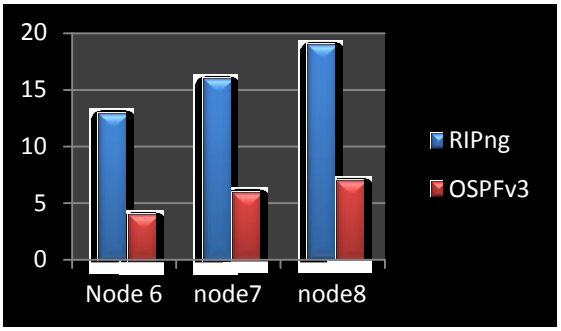
ISSN: 2278 – 909X

V. RESULTS AND DISCUSSION

The objective of this paper is to help making a right decision when choosing the interior gateway protocols for MPLS VPN backbone networks, after running GNS3 simulator for few hours in each scenario, the following results were achieved: Each scenario has been simulated for two times one by using OSPF and the other by using RIP. First we test the parameters related with VPN network:

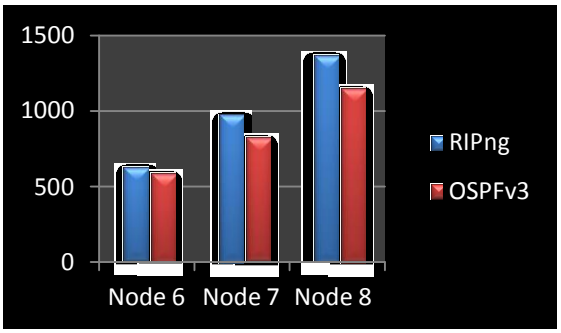
1.Packet Loss Between RIPng & OSPFv3

Nodes	Packet Loss	
	RIPng	OSPFv3
6	13	3
7	17	5
8	21	8

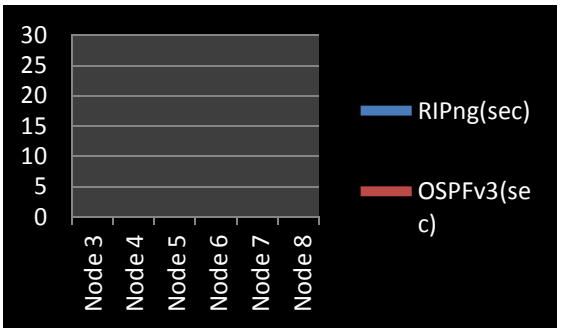


2.Latency Between RIPng & OSPFv3

Nodes	Latency(sec)	
	RIPng	OSPFv3
6	15	9
7	19	11
8	21	13



Node	Convergence time(sec)	
	RIPng	OSPFv3
3	14	6
4	16	7
5	17	9
6	19	12
7	20	13
8	24	15



VI. CONCLUSION

This work is an initial foot step in the very long road towards the interesting service provider networks management world. To study the effect of interior gateways routing protocols a detailed discussion in deferent routing concept were introduced, the specifications of the two routing protocols chosen in this work were presented. Based on the simulation results, it can be concluded that MPLS VPN provides best solution when implementing the service providers networks compared to traditional IP networks. Furthermore, with respect to the two case studies s the following results were achieved : Results from the two protocols (OSPFv3,RIPng) scenarios shows that both protocols acts well .In large networks OSPFv3 get better results than RIPng with respect to the delay, because OSPFV3 packets are directly encapsulated in link layer frames, While OSPF packets encapsulated in IP datagram. From the simulation results It is clear that the OSPFV3 have much faster convergence time than RIPng. Both protocols support multiple instances, traffic engineering and multi-topology. OSPFV3 provide the ability to design large networks by building a single large Level 1 (L1) area without any hierarchies in OSPFV3 , something that would be difficult with RIPng.

ISSN: 2278 – 909X

3.Convergence Time Between RIPng & OSPFv3

Convergence time is the time, which a group of routers reach the state of convergence. Optimally the routing protocols must have fast convergence time.

REFERENCES

[1] Sarah Mustafa Eljack, Suhail Badawi Abdelkarim School of Electronics Sudan University of Science & Technology Khartoum, Sudan "Effect of the Interior Gateway Routing Protocols in the Multiprotocol Label Switching Networks"

[2] Satoshi & Nobuo Ogashiwa Uda School of Information Science, Japan Advanced Institute of Science and Technology1-1 Asahidai, Tatsunokuchi, Ishikawa 923-1292, Japan zin@jaist.ac.jp "IPv6 support on MPLS networks Experiences with 6PE approach"

[3] Rozita Yunos, Siti Arpah Ahmad , Noorhayati Mohamed Noor, Raihana Md Saidi Faculty of Computer and Mathematical Sciences UiTM Malaysia "Analysis of Routing Protocols of VoIP VPN over MPLS Network"

[4] J. D. Clercq, G. Gastaud, T. Nguyen, D. Ooms, S. Prevost, and F. L. Faucheur. Connecting IPv6 Islands across IPv4 Clouds with BGP. IETF Internet Draft (Work in Progress), January 2002. (draft-ietf-ngtrans-bgp-tunnel-04).

[5] B. Jamoussi, Ed., L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, M. Girish, E. Gray, J. Heinanen, T. Kilty, and A. Malis. RFC 3212: Constraint-Based LSP Setup using LDP. IETF, January 200

ISSN: 2278 – 909X