Twin Labeled Virtual Private Network Above Multi-Protocol Label Switching Network for VoIP

LAKSHMINARAYANAN.V[1], NAVEENPRASAD.C[2], MANASHAA MADHAVAN[3] SUGANYA.A[4]
[1,2&4]Dr.Mahalingam College of Engineering and Technology, Pollachi, TamilNadu, India.
[3]Swinburne University of Technology, School of Science, Computing and Engineering Technologies, Australia

Abstract—*Multi-protocol label switching network (MPLS)is implemented in Virtual Private Network (VPN) to effectively fulfill the demands of Voice Over Internet Protocol (VoIP) services in a secure and effective way. The proposed idea is to differentiate the clients with in a network by adding them to a virtual private network by enabling different techniques like virtual routing and forwarding system. The need of high security within the network along with better transmission speed for sharing data and information is achieved by enabling Multi-protocol label switching within the network of a big organization. Going Forward, the configurations of the network are controlled by assigning an IP address to route itself within the network using a unique identity by enabling Open Shortest Path First (OSPF) protocol. The initial proof of the proposed network is built using a simulator commonly known as theGNS3. In which we use the Border gateway protocol (BGP) to create MPLS–VPN network between customer end and edge router in the server end. This established a premeditated network that proves to enhance the virtual routing in an efficient way which is clearly demonstrated by the simulation outputs*

Index Terms—*MPLS, VPN, OSPF, IP, BGP, Router, GNS3.*

INTRODUCTION

The Virtual Private Networks commonly known as VPN is a method of interconnecting several independent sites to a client with help of a Service Provider (SP) that acts as the backbone of the network that is placed over a devoted communication link. In the SP network, each client site is interlinked with the network in a linear fashion. This helps the network by increasing the effectiveness of communication and networking linkage protocol [5-6]. A network with the SP service can extend a VPN service within the network. In addition to this it also helps to effectively reduce the installation cost compared to the dedicated private Wireless Area Network (WAN's). The proposed network consists of individual customers through various distinct links that sources information from the spine or SP. The clients can expand the network by outsourcing and managing and planning the multipart tasks in a physically dispersed network.

Unfortunately, the current solutions that are available in relation to the VPN network are all not used to exchange or use the available information within the network to tie one apparatus of any vendor and/or a single SP effectively. This gap identified from the past pieces of literature acted as a catalyst over the strong desire to investigate the operation of the VPN network by incorporating the idea of using IP-based client identification technique to enhance the public Internet standards, this also, helped us in establishing the connection to exchange of data/information across multiple SPs. IP address-mapping and dual encapsulation are used in several IP-based solutions that exist all around the world in the recent past. This involves management of complex configurations across the network and monitoring of the superfluous information that are processed in the arrival and departure of clients that enter the SP's networks to access information.

The latest Internet innovation that has shocked the cohort of researchers is the Multi-Protocol Label Switching (MPLS) within the network that advances information within the network by utilizing distinct labels assigned to every data packet. The Intermediate MPLS nodes don't have to take a have a glimpse at the content of data in every bundle. Especially, the destination IP addresses assigned to the packets of

https://doi.org/10.37896/pd91.4/91435

information are not examined, this grants MPLS to offer a capable epitome device that can be used for private information sharing across the SP spine. In this way MPLS can give an uncommon base for the technological improvements that are established as standards in VPN networks [7-9].

Using dedicated rented network lines for connecting the remote nodes in a WANs is to provide every line an end-to-end connection in between two client sites connected to the spine of the server [1-4]. These kinds of networks are expensive to be incorporated, solely if the impacts between sites need to bolster certain level of redundancy. It is clear that the is no possibility that allows a framework to share under-used data transfer capacity or bandwidth across the network. In order to increase the transmission capacity of the existing sites considering the specific end goal to experience short-term peaks in request.

Thus, the proposed idea contributes to enhance the utilization of L3VPN in line with the MPLS acting as a backbone for the network which provides abundant resource that are managed by QOS.

MULTI PROTOCOL LABEL SWITCHING

In general, when two circuits are consistently exchanging information or data, then it is termed to be known as switching. Information can be an analog or a digital signal that embedded valid information within it. In the past decade, there is a drastic change in the concept way of using analog and digital signals in data transmission which led to the modern era of networking that uses digital signals for communicating within the network. This led to the process of designing digital switches that are used to associate the digitalized information within the network. The Circuit Switches and Packet Switches are some of the switching techniques that are used to enhance the implementation of different model that are used in Multi-Protocol Label Switching.

a) Circuit Switches

Circuit switch are fundamentally controlling the exchange of information in the voice paths. The wide range of computerized data set is isolated into a balanced set of 64 kbps. Circuit switch make use of these 64 kbps in order to handle the voice exchange happing in the network. Voice tests of a specific discussion should to attain the end point sequentially through the 64 kbps. The digital path is maintained by the advanced way by keeping up greatest admissible delay of 125µs. In order to dodge through the damage of the intelligence. Keeping in mind the destination is to satisfy the overhead scenarios, exchanged way should to be a never-ending item till the end of the communication. No other user can additionally interrupt in the network path. Furthermore, the switched paths can be organized by sort of services and class of services [12].

b) Packet Switches

Rather than partitioning the computerized digital spectrum, whole message is isolated into small packets, which are addressed and numbered. Parcel switch sends the addressed and numbered packets one by one to the destination, in various courses, by utilizing the whole range of accessible data from the week ago. Receiver needs to hold up until every packet are received. At that point packets are sorted out consecutively and after that transformed as message. Since the bundles are steered through various courses, this directing gets to be association misfortune [13].

https://doi.org/10.37896/pd91.4/91435

Some the restrictions of the packet switching network are condensed below:

- Formation and preparing of the routing table is dreary.
- In circuit switch the class of services is not connected right now.
- In existing IP networks, the type of services in manual board is not accessible.
- Due to random routing of packets, packet loss may happen.
- The packets of information within the network are not reaching the destination sequentially.
- Processing delay happens at the receiving end and also security problem.

c) Label switches

As per limitations said in the packet switches it can be overwhelmed by means of following techniques in the present IP network.

- Connectionless IP routing is transformed into a connection oriented routing by overlapping the network layer function along with the data link layer function.
- According to the class and kind of services like classifications and priorities in circuit switches IP address is converted over as labels that Routes codes in circuit switch.
- The Labels are only used for Intermediate Routers that are used for auxiliary routing of distinct IP bundles that uses suitable labels.

The proposed network system casts-off the above mentioned limitation of the switches by using the Multi-Protocol Label switching. Therefore, the MPLS is the implementation of the circuit switch model within the packet switch area. This frame the use case of several data link structures like ATM system, Frame Relay PPP/Ethernet, etc.

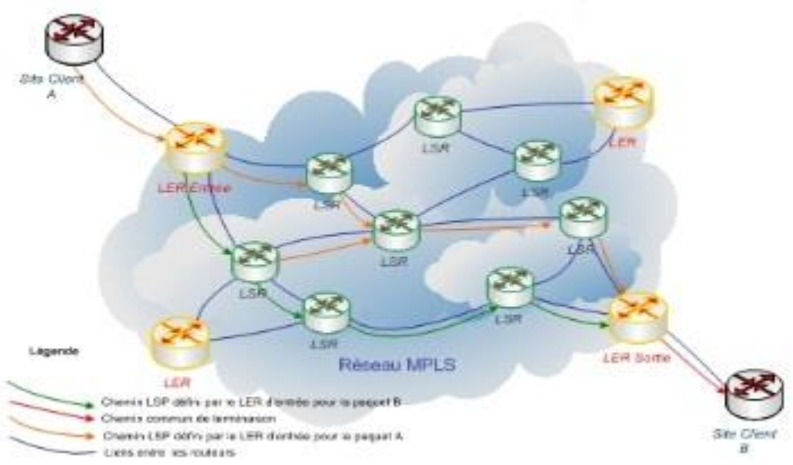
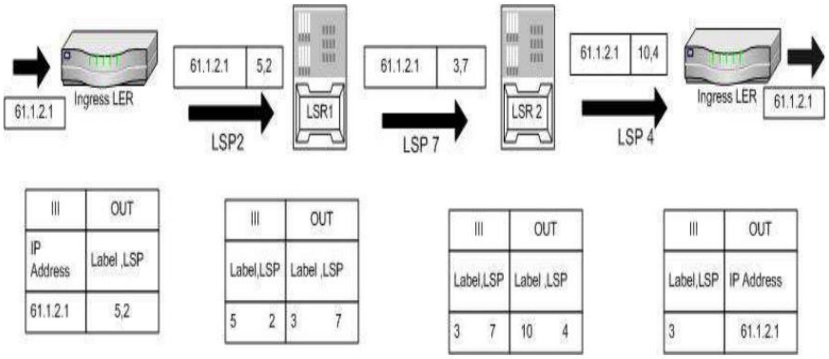

Site Client
A
LER Entrée
LSR
LSR
LSR
LER
LSR
LSR
LSR
LSR
LSR
LER
Réseau MPLS
LER Sortie
Site Client
B
Legende
Chemin LSP défini par le LER d'entrée pour le paquet B
Chemin commun de terminaison
Chemin LSP défini par le LER d'entrée pour le paquet A
Liens entre les routeurs

Fig1.MPLSArchitecture

d) MPLS IP Network Components

The components of the MPLS IP network consist of the customer edge that works within the IP level and a source edge that acts as the entry point of the MPLS Domain which is also called as the “Label Edge Router”. In addition to this there exists the routers in the service provides end which are used as transit switches in between LER’s commonly known as the “Label Switching Routers”. Also, the packets are transferred between the two routers through the labeled switching path.



III	OUT
IP Address	Label ,LSP
61.1.2.1	5,2

III	OUT
Label,LSP	Label ,LSP
5 2	3 7

III	OUT
Label,LSP	Label ,LSP
3 7	10 4

III	OUT
Label,LSP	IP Address
3	61.1.2.1

Fig2.Labelswitching

A. Types of protocols that are used in MPLS Networks

- **Open Short Path First (OSPF)** is a kind of a routing protocol, that multicasts the conversion in routing table from the end of the host towards all other congregations’ nodes within the margin of network and computes the shortest path based on intermediate hubs, bandwidth and several factors [10].

- **Border Gateway Protocol** is another type of routing protocol, which provides routing within the routing domain of the independent systems using loop-free routing within the network. An autonomous system consists of a set of routers which are operated by the same administrations that controls the services that are connected to the system. Henceforth, the MPLS Domain progresses to end up in an autonomous system setup. The VPN networks and the MPLS networks often tend to use the BGP in general [11].

B. LAYER 3 VPNs (L3VPN)

For numerous enterprise and service provider customers the L3VPNn provides IP and MPLS-based network virtualization solutions. The Layer3VPNs uses a peer-to-peer model that incorporates the BGP that provides the VPN-related information. This extremely ascendable, model permits initiative customers to farm out the information regarding the routing to the service providers by ensuing that the significant cost of investments and reduction in operational complication for originalities. These providers can also facilitate and offer the much attributed value-added services like traffic engineering and Quality of Service.

Consenting network convergence that comprehends voice, video and data. Easy Virtual Network (EVN) is newly supplanted in the IP-based VPN network. This uses the advanced Virtual Routing Forwarding instance (VRF)-Lite. The new routing instance streamlines the third layer of the virtualization of the network. This permits customers to effortlessly provide traffic parting and path segregation in the shared network substructure. This negotiates the process of installing MPLS in the enterprise network.

https://doi.org/10.37896/pd91.4/91435

VIRTUAL ROUTING FORWARDING -AWARE SERVICES

VRF is a technology comprised in IP network routers that consents multiple occurrences of a routing table to exist in a router and work concurrently. This increases functionality of the network by assenting network paths to be separated/segmented without using several devices. Due to this traffic is routinely segregated. It also boosts the security and can eradicate the need for encryption and authentication. Internet service providers will always take the benefit of VRF to create or generate distinct VPNs for the client; consequently, due the technology it is denoted as VPN Routing Forwarding.

Multiprotocol Label Switching (MPLS) for achieved shared services by enabling the service providers to deal with the network benefits of MPLS VPNs to their endorsers. Administration Providers can likewise impact this innovation to give deliberately alluring IP administrations, making supplementary income streams. It keeps on amplifying its generally conveyed IOS MPLS VPN answer for include both conventional and propelled administrations: Management, Security, Redundancy, Multicast VPNs, VPN Select, system administration IP address interpretation and Initiative clients can rehearse this adaptable, open administration model to offload and outsource antiquated IP administrations.

STEPS TO BUILD MPLS VPN TOPOLOGY

The following are the steps to build MPLS-VPN network:

1. Network topology is constructed considering the corresponding IP address in GNS3.
2. Preliminary configuration for all routers in GNS3.
3. OSPF enabling with in service provider routers.
4. MPLS enabling between service provider routers.
5. VPN is figure between customer routers and edge routers.
6. VoIP is completed in network and VPN is verified by ping command.

1) Network topology is built with corresponding IP address inGNS3:

GNS3 is one of the widely used open source software that is used to simulate complex network structured that are being placed as close as possible to the real world networking conditions and tested by performing networking operations. Also the above mentioned setup is achieve3d without having dedicated network hardware such as routers and switches within the network. The network is built in GNS3 simulator by incorporating necessary interfaces.

Cisco 3700 routers are used for customer Routers and Cisco 7200 routers are used for service provider routers due to its MPLS enabling process. The MPLS can be enabled only for the routers of series above 3700 routers. The routers are enabled with two interfaces of fast Ethernet.

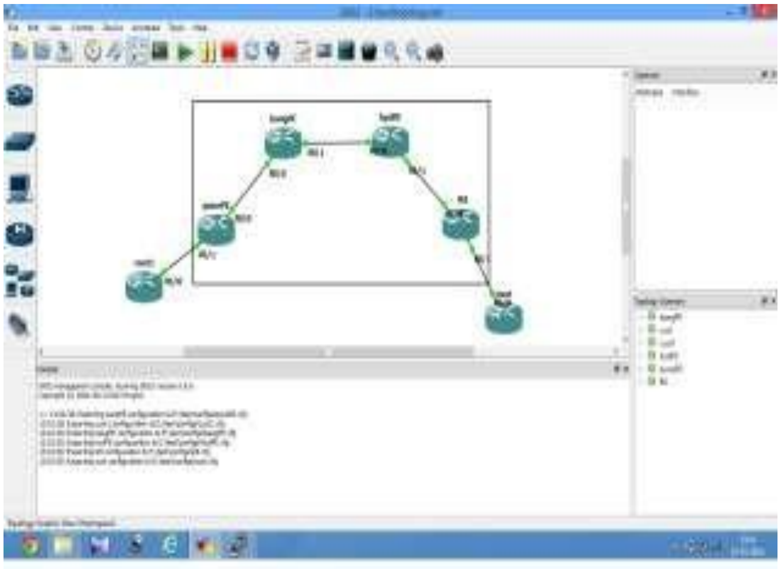


Fig3.NetworktopologybuiltinGNS3

2) Preliminary configuration for all routers in made in GNS 3:

It is configuring the routers with its loop back address and its IP address for all interfaces. The preliminary can be verified with the command “ship int brief”.

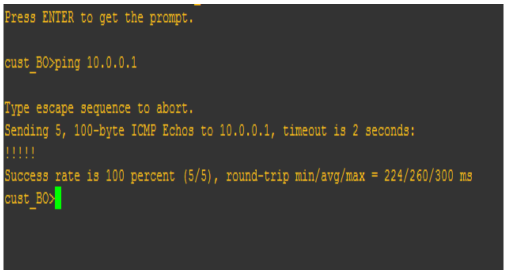
RESULTS AND DISCUSSION

1) Enabling OSPF between service provider routers:

The Open Short Path first (OSPF) is the most preferred routing protocol, that is used to create multiple instances of the alteration in table that is considered as the reference for the routing all other hosts within the border of network. This helps us compute the shortest path based on intermediate nodes, bandwidth of transmission. OSPF chooses routes based on the bandwidth of the transmission signal and the OSPF group’s associates itself to the defined ‘areas’ and breakdowns the network into minor bunches of routers. OSPF limits its data streaming of traffic regionally and it can also help us avoid variations in one domain disturbing another node within the domain e.g. route flapping. Finally, it compares the output of this with a RIP flat network to evaluate the efficiency and effectiveness of the network.

2) Enabling VPN on MPLS network:

The above image illustrated the VPN that is built between all the customers and edge



```
Press ENTER to get the prompt.

cust_BO>ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 224/260/300 ms
cust_BO>
```

Fig:4 Connectivity between customer branch office to host office

3) VOIP is done in network and VPN is built through BGP protocol:

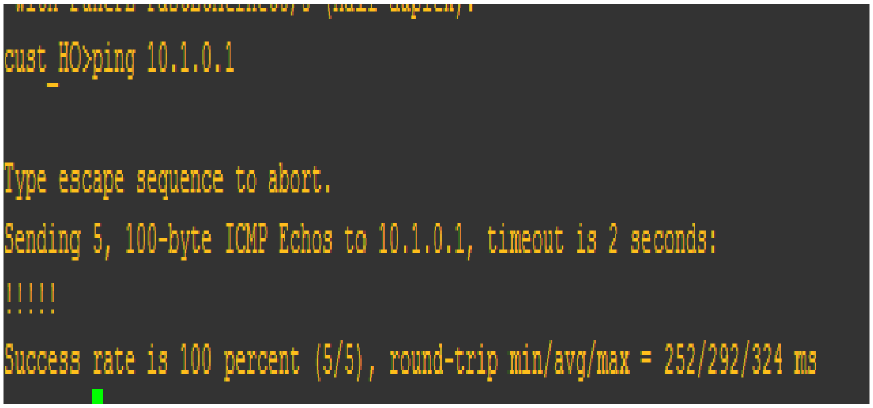
The connectivity between the two routers of each customer can be verified by ping command. If connectivity gets succeed, then the path of a single private network was made successfully

TABLE1.IPFORALLROUTERS

ROUTERS	**F0/0**	**F0/1**
CUST_HO	192.18.16.33	
PUNE PE	192.18.16.2	192.18.16.32
BANG_PE	192.18.16.7	192.18.16.3
HYD_PE	192.18.16.12	192.18.16.8
CHEN_PE	192.18.16.10	192.18.16.13
CUST_BO	192.18.16.9	

CONCLUSION

Due to vast growth in internet, the issues like data and file transfer in huge amount (Kilobytes to Megabytes) is a major criterion. This layer3vpn technique helps to achieve the process of utilizing, thelayer3of OSI, which enables the VPN to enhance itself and to provide better QOS with high security. Virtual routing and forwarding table helps to find the difficulties in recognizing the IP addresses of the users using the same IP in the same autonomous system.



```
with [illegible] FastEthernet0/0 (half duplex).
cust_HO>ping 10.1.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 252/292/324 ms
```

Fig: 5 connectivity between customer host office to branch office

This research project of dual tagging the VRF and MPLS in layer3 focuses on playing a key role on the next generation of networking research. This is achieved by delivering high efficient traffic engineering and high reliable connectivity of secure L3VPN layered network, which will help the network to perform in a good manner in a heavy traffic environment. These ideas can also be useful in deploying the concepts using IPV6 addressing and by enabling different routing protocols in future work.

REFERENCES

[1].Francesco Palmieri,(2003),'VPN Scalability over High Performance Backbone Evaluating MPLS VPN against Traditional Approaches,' Proceedings ofthe8thIEEE International Symposium on Computers and Communication,vol.2,pp.975-981.

[2].Hiroshi Yamada(2006),'End-to-End Performance Design Framework of MPLS Virtual Private Network Service across Autonomous System Boundaries', IEEE International

[3].Lanjun ,Lin bi ying (2011)Research for Service Deployment Based on MPLS L3 VPN Technology, IEEEInternationaltransaction.*,M.BELLAFKIH*

[4].Li-Der Chout ,Mao Yuan Hong(2006) 'Design and Implementation of Two-Level VPN Service Provisioning Systems over MPLS Networks', IEEE International Symposium

[5].Mahesh Kr. Porwal, AnjulataYadav,S. V. Charhate(2008) 'Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS',IEEE International journal.

[6].Md.ArifurRahman, A.H.Kabir, K.A.M.Lutfullahl, Z.Hassan (2007) 'Performance Analysis of MPLS Protocols over conventional Network', IEEE International Symposium.

[7].Muhammad Romdzi Ahamed Rahimi Habibah Hashim(2009) i,Habibah Hashim(2009) Habibah Hashim(2009) 'Implementation of Quality of Service (QoS) in Multi- Protocol Label Switching (MPLS) Networks', IEEE International

[8].Shu-meiLI, Hai-yingLIANG(2011)'A Model of Path Fault Recovery of MPLS VPN and Simulation', IEEE International

[9].TranCongHung, PhD, LeQuocCuong,Ph.D,Tran ThiThuy(2010)'A Study on any Transport over MPLS(AToM)'Functioning.

[10]. Moy, J., 1998. Open shortest path first (ospf) version 2. IETF: The Internet Engineering Taskforce RFC, 2328.

[11]. Rekhter, Y., Li, T. and Hares, S., 2005. *A border gateway protocol 4 (BGP-4)*(No. RFC 4271).

[12]. Gudla, V.R., Das, S., Shastri, A., Parulkar, G., McKeown, N., Kazovsky, L. and Yamashita, S., 2010, March. Experimental demonstration of OpenFlow control of packet and circuit switches. In Optical Fiber Communication Conference (p. OTuG2). Optical Society of America.

[13]. Nagle, J., 1985. On packet switches with infinite storage.