Creation of Virtual Private Network Over MPLS Network for Voice over Ip

Dr. A. Sumithra & Balasubramanian Devaraj
Department of Information Technology
Velammal College of Engineering and Technology Madurai, India
asm@vcet.ac.in; dipla.1990@gmail.com

ABSTRACT:
This paper treats a MPLS-VPN implementation in a network, which was initially configured for fulfilling the demands for mainly voip services.The MPLS network has the important advantage of highest degree of security with better transmission speed which was seeked by many organization all over the world.The network was built in simulator software called GNS3.Intially preliminary configuration are done in all routers with their corresponding ip address with enabling sop protocol in service provider routers to find the shortest path to find the destination routers. Then label distributive protocol (LDP) is enabled with in service provider routers in which routers capable of Multiprotocol Label Switching (MPLS) exchange label mapping information. The Border Gateway Protocol (BGP) is enabled between edge routers and customers to build a virtual private network to enhance voice over ip using MPLS-VPN network. The simulation for this network is verified by using GNS 3 simulator.

Key words-
Multi Protocol Label Switching; Virtual Private Network; Label Disributive Protocol

I. INTRODUCTION

Historically, private WANs were provisioned using dedicated leased line connections, each line providing a point-to-point connection between two customer sites. [1-4]Such networks are expensive to put in place, especially if the connections between sites need to support some level of redundancy. There is also no scope in such a system to share under-utilized bandwidth across several customers or conversely, to increase the bandwidth available between particular sites dynamically in order to meet short-term peaks in demand.

Virtual Private Networks (VPNs) are a method of interconnecting multiple sites belonging to a customer using a Service Provider (SP) backbone network in place of dedicated leased lines [5-6]. Each customer site is directly connected to the SP backbone. The SP can offer a VPN service more economically than if dedicated private WANs are built by each individual customer because the SP can share the same backbone network resources (bandwidth, redundant links) between many customers. The customer also gains by outsourcing the complex task of planning, provisioning and managing a geographically distributed network to the SP.

Unfortunately, existing VPN solutions are not all interoperable and may be tied to one equipment vendor and/or a single SP. This has created strong interest in IP-based VPNs running over the public Internet using standards-based interoperable implementations that work across multiple SPs. Many of these IP-based solutions require IP address-mapping or double encapsulation using two IP headers. This can require complex configuration management and requires additional processing at the entry to and exit from the SP's networks. The new Internet technology, Multi-Protocol Label Switching (MPLS) forwards data using labels that are attached to each data packet. Intermediate MPLS nodes do not need to look at the content of the data in each packet. In particular the destination IP addresses in the packets are not examined, which enables MPLS to offer an efficient encapsulation mechanism for private data traffic

traversing the SP backbone. MPLS can, therefore, provide an excellent base technology for standards-based VPNs. [7-10]
This project put forwards the utilization of L3vpn along with mpls backbone the provide high amount of resource management QOS and security.

II. MULTI PROTOCOL LABEL WITCHING-AN OVERVIEW

Switching is the process by which, two circuits are interconnected for exchanging information. Information is in the form of either analog or digital. In electro mechanical era, information was in the form of analog. Presently, information is in the form of digital. In order to interconnect the circuits, supporting the digitized information, suitable digital switches are designed. Digital Switches are classified as

(1)Circuit switch
(2) Packet switch

Apart from the above models of switching, Multi-Protocol Label Switching model is configured in Packet Switch Area.

a)*Circuit switches*

Circuit switch mainly supports the switching the voice paths. Digital spectrum is divided into equal parts (64 kbps). Circuit switch uses these 64 kbps path for voice switching. Voice samples of a particular conversation should reach the destination sequentially through the 64 kbps digital path by maintaining maximum permissible delay of 125 us, to avoid the loss of intelligence. In order to satisfy the above conditions, switched path should be permanent until the end of the conversation. . Hence, the routing becomes connection oriented. No other user also can intrude in that path. Also the switched paths can be categorized according to the type of services and class of services.

Instead of dividing the digital spectrum, entire message is divided into packets, addressed and numbered. Packet switch sends the addressed and numbered packets one by one to the destination, in different routes, by using the entire spectrum available in last week.. Receiver has to wait until all the packets are received. Then packets are arranged sequentially and then converted as message. Since the packets are routed through different routes, this routing becomes connection loss.

Hence, the limitations of the packet network are summarized as follows:

- Creation and processing of routing table is tedious.
- Class of services (Priorities) as in circuit switch is not implemented presently.
- Type of services (category) as in manual board is not available in the present IP network.
- Loss of packet, because of the random routing of packets.
- Delayed processing at receiving end, since packets are not reaching the destination sequentially.
- Security problem.

C)*Label switches*

Above limitations can be overcome by using following techniques in the present IP network.

- Connectionless IP routing is converted into connection oriented routing by overlaying Network Layer function with Data link layer Function.
- IP address is converted as Labels (Rout codes in circuit switch), according to the class and type of services like categories and Priorities in circuit switches.
- Intermediate Routers uses the Labels only (Rout Codes in Circuit Switch) for further routing of destined IP packet with appropriate Label.

The above techniques are used in Multi-Protocol Label switching. Hence, MPLs is the implementation of circuit switch model in the Packet switch area. MPLS frame uses the various Data Link frames like ATM, Frame Relay PPP/Ethernet etc. Since MPLS uses label switching and supports the multiple

protocols, it is called Multi-Protocol Label Switching.

d) Components of MPLS IP Network

- Customer Edge, which works at IP level.
- Provider Edge is the entry point of MPLS Domain. It is called "Label Edge Router"
- Provider Routers are working as transit switches in between LERs. These are known as "Label Switching Routers".
- Label switched path is the data path between two routers, through which packets are traveling.

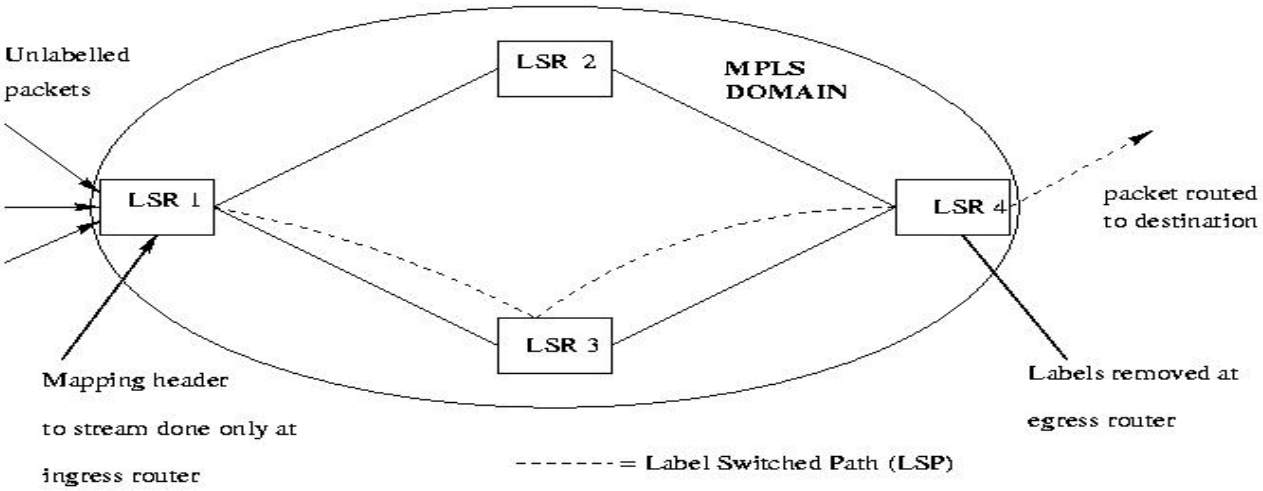


Fig.1 MPLS Architecture

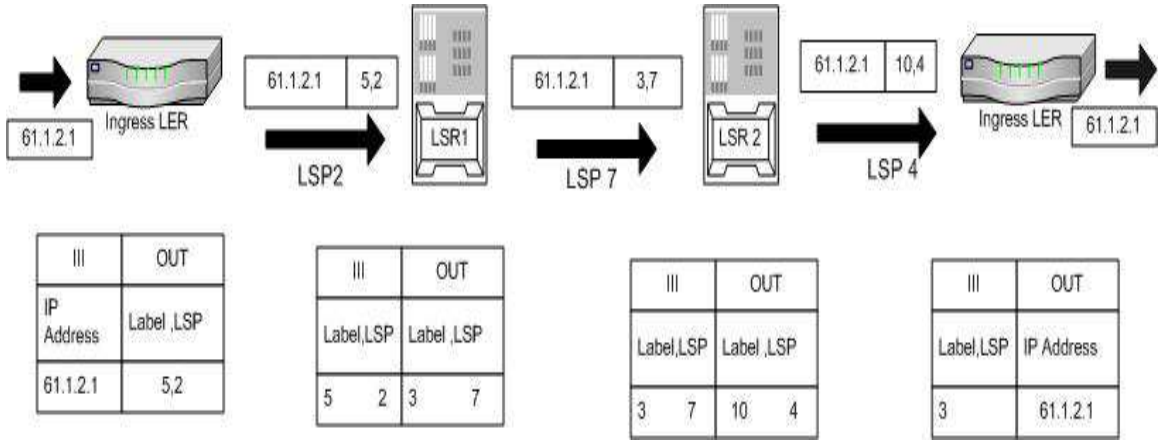


Fig:2 Label switching

LER receives destined IP packet 61.2.1.1 from the Customer Edge and selects the correct label (5) from its LIB. It binds the selected label (5) according to the FEC over the IP packet and sends it through the preprogrammed LSP (2) towards the LSR 1. On receipt of labeled IP Packet, LSR1 analyses label only and it will ignore the IP address. It will consult its LIB for further routing. As the result it removes the incoming label (5), winds the newly assigned label (3) over the IP Packet and sends it towards the LSR2 over the assigned LSP (7). LSR2 consults its LIB and transmits the IP Packet after swapping the incoming Label (3) with outgoing

Label (10) towards the egress LER over the pre assigned LSP (4). Egress LER stripes the label (10), goes through the destined IP address (61.1.2.1) and hands over it to the correct CE.

e)Label

A label in MPLS is used as the routing code like STD code in circuit switch. It identifies the path a packet should traverse in the MPLS domain. Label is encapsulated in a Data Link Layer 2 header.

So, new layer is formed in between Network Layer and Data Link Layer in OSI Layer concept. The name of the new layer is MPLS SHIM Layer. Function of this layer is to bind the MPLS Label over the IP packet received from the customer edge. Label contains the information about next hop address. Value of the label is having local significance. So same label number can be reused in some other area.

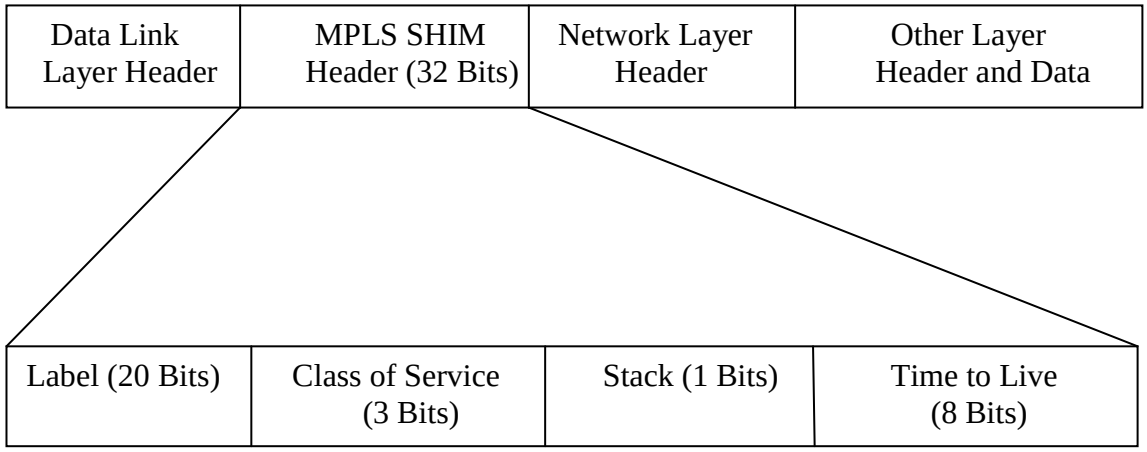


Fig 3: Mpls label format

f) Different types of protocols used in MPLS Networks

- **Open Short Path first (OSPF)** is the routing protocol, thatmulticasts the change in routing table of a host to all other hosts with in the boundary of Network and computes the shortest path based o of intermediate hubs,bandwidth and many factors
- **Label Distribution Protocol** between peers. This protocol is one among the Interior Gateway Protocols (IGP)
- **Border Gateway Protocol** is also one among the routing protocol, which provides loop-free inter domain routing between autonomous systems. An autonomous system is a set of routers that operate under the same administration. Here MPLS Domain becomes autonomous system. BGP is often run among the VPN networks and MPLS Network.

III STEPS TO BUILD MPLS VPN TOPOLOGY

The following are the steps to build mpls-vpn network:

1. Network topology is built with corresponding ip address in gns 3
2. Preliminary configuration for all routers in made in gns 3
3. Ospf enabling with in service provider routers
4. Mpls enabling between service provider routers
5. Vpn is build between customer routers and edge routers
6. Voip is done in network and vpn is verified by ping command

1) Network topology is built with corresponding ip address in gns 3:

GNS3 is an open source software that simulate complex networks while being as close as possible to the way real networks perform. All of this without having dedicated network hardware such as routers and switches. The network was built in gns 3 simulator with 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. Thumps can be enabled only for the routers of series above 3700 routers. Throwers is enabled with two interfaces of fast Ethernet.

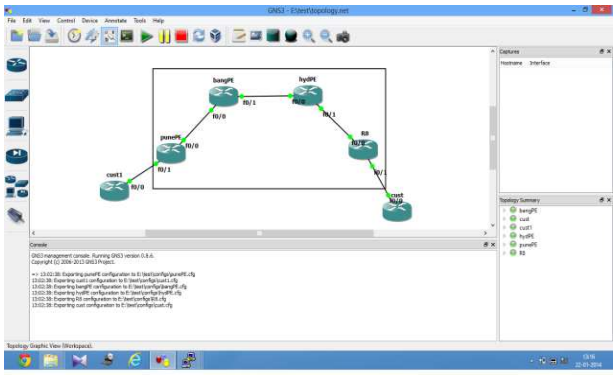


Fig: 4 Network topology built in Gns 3

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 "show pint brief".

TABLE I

IP ADDRESS FOR ALL ROUTERS

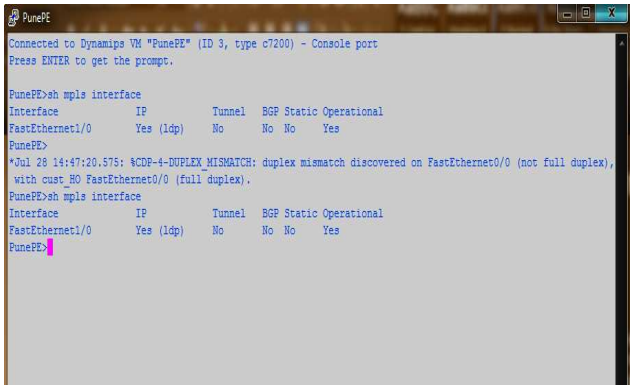
ROUTERS	F0/0	F0/1
CUST_HO	172.16.16.70	
PUNE PE	172.16.16.5	172.16.16.69
BANG_PE	172.16.16.9	172.16.16.6
HYD_PE	172.16.16.25	172.16.16.10
CHEN_PE	172.16.16.14	172.16.16.26
CUST_BO	172.16.16.13	

3) Enabling ospf between sevice provider routers:

The Open Short Path first (OSPF**)** is the routing protocol, thatmulticasts the change in routing table of a host to all other hosts with in the boundary of Network and computes the shortest path based o of intermediate hubs,bandwidth and many factors
OSPF selects routes based on cost (bandwidth).
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.

4) Enabling label distributive protocol between service provider routers:

Enabling LDP is a protocol in which encryption and decryption is done in edge routers in order to enable mpls network. Labels usually correspond to IP destination networks
Label Distribution Protocol between peers. This protocol is one among the Interior Gateway Protocols (IGP)



5) Enabling Vpn on MPLS network:

Here, vpn is build between all the customers and edge router which it is connected to the particular customer. More number of vpn can be built over mpls network using Bgp protocol

Border gateway protocol (bgp) is a protocol for exchanging routing information

between gateway hosts(each with its own routers) in a network of autonomous system. Bgp can be used as gateway for transmission of information between the customer.

The reason why bgp protocol is most popular is because at present BGP-4 is only available exterior gateway protocol deployed between autonomous systems.

Fig: 5 Mpls enabled in router interface

BGP Routing Process:

1. A pool of routes that a router receives from its peers
2. An input Policy Engine that can filter the routes or manipulate their attributes
3. A decision process that decides which routes the router itself will use
4. A pool of routes that the router itself uses
5. An Output Policy Engine that can filter the routes or manipulate their attributes.
6. A pool of routes that the router advertises to other peers

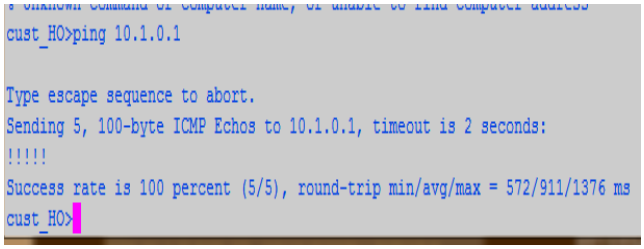


Fig: 6 Connectivity between from host office to customer branch office

6. 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.

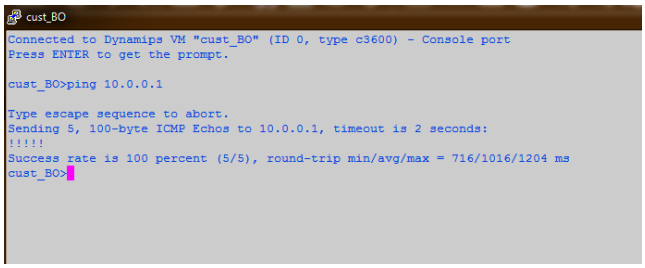


Fig: 7 Connectivity between customer branch office to host office

IV. CONCLUSION

As internet is said to be expanding and need for support for file, transfers of corporate companies become vital this l3vpnv4 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 an 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. The following project has the facility to be employed in IPv6 addressing also which is to be deployed in the fourth coming years which will enable higher degree of addressing and auto-configuration mechanism.

REFERENCES

[1]. Francesco Palmieri, (2003), 'VPN Scalability over High Performance Backbone Evaluating MPLS VPN against Traditional Approaches,' Proceedings of the 8th IEEE 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, IEEE International transaction.*, 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 RomdziAhamedRahimi,HabibahHashim(2009) 'Implementation of Quality of Service (QoS) in Multi-Protocol Label Switching (MPLS) Networks', IEEE International .

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

[9]. Tran Cong Hung, PhD, Le QuocCuong, Ph.D, Tran ThiThuy (2010) 'A Study on Any Transport over MPLS (AToM)'Functionin