International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

IMPLEMENTING MPLS BASED WIDE AREA NETWORK AND QUALITY ANALYSIS BASED ON MPLS VPN AND MPLS RSVP SIGNAL

N.Saranya (M.E)[#1], S.Karthika[*2] , Aishwarya Rout[*3] , Koushiki Priya[*4]

Assistant Professor[#1], Final Year U.G Students[*2,3,4,]*
Department of ECE, SRM Institute of Science and Technology, Chennai
tvmsuriya@gmail.com , routaish0412@gmail.com , koushikipriya@gmail.com

***Abstract*— MPLS(Multi Protocol Label Switching) is an emerging technology which has started attracting all the service provider networks with its exceptional and admirable features. Virtual Private Network is one of its most popular feature which carries traffic securely and privately from customer's one end to another through the service provider's network. It is virtual since there is no real physical connection between the sites. A VPN enables network-enabled devices to transmit data across the shared or public network infrastructure securely and privately. In this project, MPLS based VPN is implemented in a corporate environment. Two different organizations are connected with the central site through MPLS based ISP's network. Concerning the security requirements, it hides the customer's network from ISP's network.**

***Keywords*— Multiprotocol label switching(MPLS), Internet telephony , Quality of service, Virtual private network Delays, Switches , Packet loss , Internet service provider**

I. INTRODUCTION

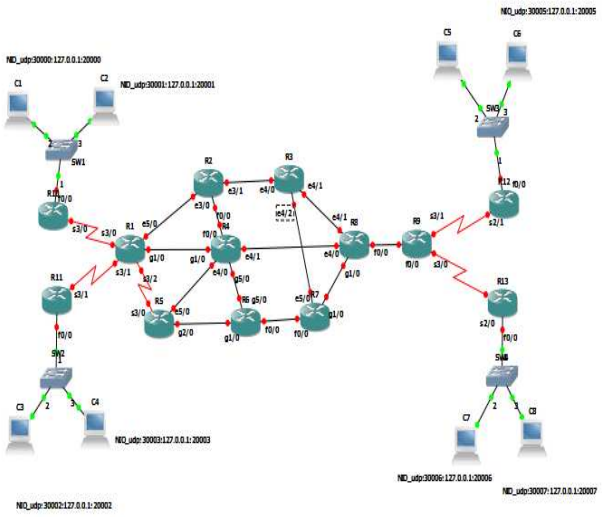
An understanding of the basics behind MPLS is required for understanding MPLS based VPNs. MPLS evolved for a number of reasons. The first was that it provided a more scalable method of allowing IP traffic to travel over an ATM network. Second, MPLS enhances routing functionality. On a traditional service provider IP Network, traffic is routed via an interior routing protocol such as OSPF Finally, MPLS allows service providers to offer customers enhanced services. MPLS is based upon routers, or switches, performing label switching to provide a Label Switched Path (LSP) through a network. MPLS VPNs are network based, meaning that they are not the CPE-based VPNs that are more prevalent. Despite international differences, it is clear that the use of VPN technology will continue to grow, and an increasing amount of providers. Multi Protocol Label Switching is fast forwarding and reliable technology which makes every transmission efficient as compare to the simple IP based network [1]. MPLS technology helps to minimize the delay for voice which is considered as delay sensitive traffic. In this paper it is explained by performing experiments on real environment that MPLS based network provide better Quality of Services (QoS) as compared to conventional networks for voice and other traffics, in term of packet loss and end to end delay. We explained the MPLS based network that helps VOIP application to transmit from source to
destination with minimum delay and zero packet lose by enabling QoS (Quality of services) for different types of TCP and UDP traffics. Moreover, MPLS technology is explained in detail along with QoS for IPv4 and MPLS. By the end results are discussed by transmitting traffic over designed network without quality of services and then with quality of services, these experiments show the incredible results. In old systems, QoS may also be maintained using IPv4 however; we cannot reduce the propagation delay on IPv4 networks due to large processing delay on each hop. Therefore, in this paper, we are going to implement MPLS based networks to reduce propagation delay, to avoid packet loss in order to improve Mean Opinion Score (MOS) for VOIP networks. In todays networking voice over Internet protocol is most famous, required and cost-effective services for all users. This VOIP is also known as internet telephony. This VOIP is a real time traffic which is transmitted by RTP (Real Time Protocol). VOIP has two things data and control signaling. The controlling of VOIP is done by using RTCP (Real Time Control Protocol). All real rime transmissions are connectionless communications which is handled by UDP (User Datagram Protocol). Voice over IP is transmitted by using RTP/UDP/Protocol. Similarly TCP/IP is connection-Oriented communication; it gives acknowledgement even every packet received at destination. TCP/IP is more reliable but we cannot use it for voice because VOIP is delay sensitive traffic, so we transmit it by using UDP [2]. As it is explain above that VOIP is real time traffic so this is delay sensitive traffic. But while transmission of voice or data there will be end to end delay. End to end delay is basically the overall time taken to transmit traffic from source to destination. There are some factors which affect the end to end delay while transmission.

II. EXISTING SYSTEM

Implementation of high speed networks in internetworking environment is very essential in the present century, at present IPv4 networks provides communication in internet work environment. In IPv4 network, routing is being done at layer 3

network layer based destination network ID. The problems are more delay, less security, less quality of services. Latency is the time taken by the packet to travel from source to destination. Latency is high in existing system. Security is defined as delivering information without any modification to the user. Security is less in existing system. Processing delay is the time it takes routers to process the packet header, processing delay is more in existing system Propagation delay is the amount of time it takes for the head of the signal to travel from the sender to the receiver. Propagation delay is also more in existing system Scalability: No. of routers increases eventually No. of networks also increases.

III. PROPOSED SYSTEM



IPv4 network with MPLS protocol networking proposed to overcome all the limitation of IPv4 network. This network shares the information through VPN and it provides the corporate domains to access, transfer, receive, data with high efficiency, security, resource management. It also proposed that MPLS employed with OSPFv2 protocol provides standard Traffic engineering along with BGPv4 protocol provides inter AS high reliable connectivity in an secured L3VPN layered Network this schema can achieve reliable explicit routing which Deploys maximally-disjoint pre-calculated alternate paths with improved secured packet transmission in networks supported even in heavy traffic environments.

IV. HARDWARE AND SOFTWARE DESCRIPTION

Hardware components which we use are router, switch and host. A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node. A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination A network switch (also called switching hub, bridging hub, officially MAC bridge is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

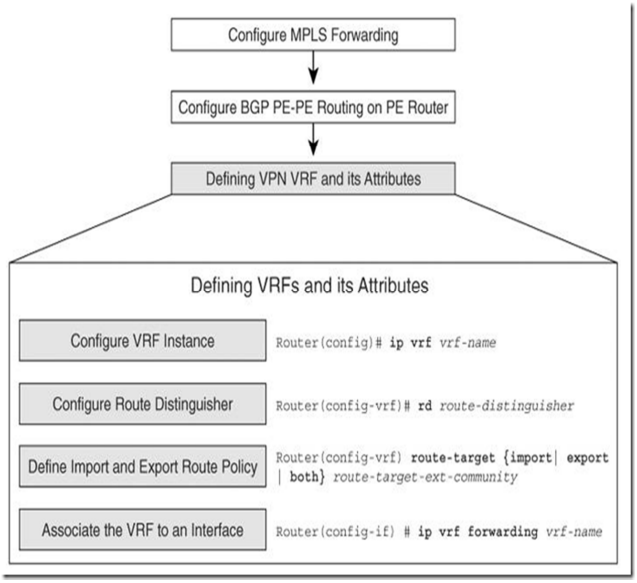
A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network address .Computers participating in networks that use the Internet protocol suite may also be called IP hosts. Specifically, computers participating in the Internet are called *Internet hosts*, sometimes Internet nodes. Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces. The addresses are configured either manually by an administrator, automatically at startup by means of the Dynamic Host Configuration Protocol (DHCP), or by stateless address auto configuration methods.

GNS3 is the software which we use is a Graphical Network Simulator that allows emulation of complex networks. You may be familiar with VM Ware or Virtual PC that are used to emulate various operating systems in a virtual environment. These programs allow you to run operating systems such as Windows XP Professional or Ubuntu Linux in a virtual environment on your computer. GNS3 allows the same type of emulation using Cisco Internetwork Operating Systems. It allows you to run a Cisco IOS in a virtual environment on your computer. GNS3 is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. Dynagen runs on top of Dynamips to create a more user friendly, text-based environment. A user may create network topologies using simple Windows ini-type files with Dynagen running on top of Dynamips. GNS3 takes this a step further by providing a graphical environment.

GNS3 allows the emulation of Cisco IOSs on your Windows or Linux based computer. Emulation is possible for a long list of router platforms and PIX firewalls. Using an Ether Switch card in a router, switching platforms may also be emulated to the degree of the card's supported functionality. This means that GNS3 is an invaluable tool for preparing for Cisco certifications such as CCNA and CCNP. There are a number of router simulators on the market, but they are limited to the commands that the developer chooses to include. Almost always there are commands or parameters that are not supported when working on a practice lab. In these simulators you are only seeing a representation of the output of a simulated router. The accuracy of that representation is only as

good as the developer makes it. With GNS3 you are running an actual Cisco IOS, so you will see exactly what the IOS produces and will have access to any command or parameter supported by the IOS. In addition, GNS3 is an open source, free program for you to use. However, due to licensing restrictions, you will have to provide your own Cisco IOSs to use with GNS3. Also, GNS3 will provide around 1,000 packets per second throughput in a virtual environment. A normal router will provide a hundred to a thousand times greater throughput. GNS3 does not take the place of a real router, but is meant to be a tool for learning and testing in a lab environment. Using GNS3 in any other way would be considered improper.

V. IMPLEMENTATION



We configure router with first IP Configuration, OSPF, MPLS, MPLS VPN, MPLS RSVP are the configurations which are used in software. Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model. OSPF is a widely used IGP in large enterprise networks. IS-IS, another LSR-based protocol, is more common in large service provider networks.

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name "multiprotocol". MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL

MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer (layer 2) technology, such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. Multiprotocol label switching belongs to the family of packet-switched networks.

MPLS VPN is a family of methods for using multiprotocol label switching (MPLS) to create virtual private networks (VPNs). MPLS VPN is a flexible method to transport and route several types of network traffic using an MPLS backbone. There are three types of MPLS VPNs deployed in networks today: 1. Point-to-point (Pseudo wire) 2. Layer 2 (VPLS) 3. Layer 3 (VPRN).

Traffic engineering refers to the process of selecting LS paths chosen by data traffic in order to balance the load on various links, routers, and switches in the network. This is most important in networks where multiple parallel or alternate paths are available. The goal of Traffic Engineering is to facilitate efficient and reliable IP network operations while simultaneously optimizing resource utilization and network performance. Prior to MPLS TE, this technique is possible with either IP or ATM depending on the protocol used between a pair of edge routers in a network. Traffic Engineering in MPLS involves the technique of directing traffic that flows within a network. Several routing procedures implement packet forwarding for a secure transmission.

VI. APPLICATION

It is used in banking and it can be applied in long distance communications as it fulfils the limitations of the exposed system that has more latency, more delay and less quality of service .It is used in military network as it has less delay .The proposed system is also useful for network providers .The proposed system is a great way to connect to the cloud. MPLS VPN are carried over a single carrier's network, which offers better reliability and security than the public internet. The combination of cloud services and MPLS VPNS can create what's known as a "virtual private cloud."
MPLS VPNs help provide quality performance for cloud-based applications chiefly because they enable enterprises to prioritize certain types of their traffic ,a concept known as class of service. This takes on added importance when you consider the sorts of applications that may be getting shifted to the cloud, everything from delay-sensitive voice-over-ip-traffic to enterprise applications like enterprise resource

planning or sales force automation. With CoS, enterprise can detect which types of their traffic is given priority ,so they can avoid an employee conducting a massive file transfer causing a hiccup in the CEO's conference call.
MPLS VPN enable each site on the network to connect to every other site via a single connection to the MPLS network. This can significantly reduce the amount of bandwidth customers need ,especially at their main headquarters and cloud provider sites.
Similar to how cloud services enable you to quickly add capacity on as needed basis it's far easier to add capacity to an MPLS VPN than via traditional carrier services. And being able to expand the capacity of your cloud application and services may not do you much good if you can't increase the capacity of the connection to them at the same time .The combinations of cloud services and MPLS VPNs really can make the cloud seem like an extension of your premise-based network and services, creating what's known as a "virtual private cloud."

VII. ADVANTAGES

The advantages of the proposed system is that it leads to simplified network management. It provides the ability to consolidate voice, video and data functions on a single converged network. It provides more bandwidth for a lower price as well as it leads to quality of service enablement. Last but not the least latency is ensured. In MPLS the packets are being added at the MPLS edge routers ,it is possible to set the path that the traffic will have to take through the network .More specifically each class of traffic can be set individual performance characteristics.

QUALITY OF SERVICE : Since MPLS network enables traffic engineering ,it is possible to send –data traffic over a lower priority path and real time delay sensitive voice .This enables network convergence

Network redundancy :An MPLS core network is generally designed and built to overcome individual hardware faults or line disconnection .In such cases ,the data is re-routed through the next optimum path with a fail-over time of 50 ms or lesser. Even the last mile connections can be backed up etc depending upon the options with the service provider.

Protocol independent Forwarding: MPLS networks can carry any type of packets-be it IP, frame relay or ATM using the same infrastructure, This is because ,whatever type of packets comes in ,MPLS labels would be attached to it for transmitting them over the MPLS network and these labels are protocol independent.

SECURITY :Service providers take full responsibility for the security of information that is sent over an MPLS network. Service providers also create IP tunnels throughout the network without the need for any encryption from user end

International MPLS: There are options with service providers to connect individual locations across different countries using MPLS by sharing and inter-connecting their respective MPLS networks.

International MPLS: There are options with service providers to connect individual locations across different countries using MPLS by sharing and inter-connecting their respective MPLS networks.

Lesser Hops-With an MPLS network ,there are lesser number of hops between the various network points resulting in improved response times and application performance.

VIII. CONCLUSION

In order to conclude this project we get to know that the designed proposed system overcomes the limitations of the existing system which includes more latency ,more delay ,less quality of service etc. The proposed system is a scalable ,protocols-independent transport .In this system, data packets are assigned labels which creates end to end circuits. As a result the proposed system has less latency and more quality of service.

IX. REFERRENCES

I. Hussain, "Overview of MPLS Technology and Traffic Engineering Applications", *International Conference on Networking and Communication (INCC)*, pp. 1-9, 2004.
II. Goode, "Voice over Internet Protocol (VoIP)", *Proceedings of the IEEE Conf*, pp. 1495-1517, 2002.
III. K. P. Mahesh, A. Yadav, S. V. Charhate, "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic Distribution in OSPF and MPLS", *Proc of Int. Conf. on Emerging Trends in Engineering and Technology (ICETET)*, pp. 9-14, 2008.
IV. Khan, W. Kiess, "Quality-Of-Service (QOS) for Virtual Networks in Openflow MPLS Transport Networks", *IEEE 2ND International Conference In Cloud Networking (CLOUDNET)*, pp. 8-13, 2014.
V. S. Ahmed, W. Ali, M. Hassan, "Performance Evaluation of IPv4 and IPv6 over MPLS using OPNET", *International Journal of Computer Applications*, no. 3, pp. 0975-8887, 2015.
VI. K. Nichols, *tools.ietf.org*, 1998,.
VII. L. Berger, *tools.ietf.org*, 2010,
VIII. Lee Hyunseok, "An Efficient Recovery Mechanism for MPLS-based Protection LSP", *IEEE International Conference on ATM and High Speed Intelligent Internet Symposium*, pp. 22-25, 2001.
IX. J. Yackoski, "Managing End-to-End Delay for VoIP Calls in Multi-Hop Wireless Mesh Networks", *IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1-6, 2010.
X. Ali, A. Ashraf, "A Comparative Study of Bandwidth Requirements of VoIP Codecs over WiMAX Access Networks", *IEEE International Conference on Next Generation Mobile Applications Services and Technologies (NGMAST)*, pp. 10-15, 2009.
XI. L. Qi, "Super VLAN Technique Applied to Network Reform", *International Conference on Computer Science and Service System (CSSS)*, pp. 785-788, 2012.
XII. N. Rikli, S. Almogari, "Efficient Priority Schemes for the Provision of End-to-End Quality of Service for Multimedia Traffic over MPLS VPN networks", *Journal of Computer and Information Sciences-King Saud University*, no. 25, pp. 89-98, 2013.
XIII. Alkayyal, S. Sotiriadis, "Optimizing Voice over Multi-protocol Label Switching (VoMPLS)", *P2P Parallel Grid Cloud and Internet Computing (3PGCIC)*, pp. 16-21, 2013.