CARRIER SUPPORTING CARRIER(One ISP is supporting other ISP for sending Internet/VPN traffic): WITH CUSTOMER CARRIER PROVIDING MPLS VPN SERVICES TO USER SITES

MRS.SIJI SIVANANDAN[1], B.SHWETA KRISHNAN[2]

[1]Associate Professor, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, India
[2]Second UG Student, Department of Electronics and Communication Engineering, Meenakshi Sundararajan Engineering College, Chennai, India

---

Abstract - *MPLS technology is being widely adopted by service providers worldwide to implement VPNs to connect geographically separated customer sites. VPNs were originally introduced to enable service providers to use common physical infrastructure to implement emulated point-to-point links between customer sites. A customer network implemented with any VPN technology would contain distinct regions under the customer's control called the customer sites connected to each other via the service provider network.*

In traditional router based networks, different sites belonging to the same customer were connected to each other using dedicated point-to-point links. The cost of implementation depended on the number of customer sites to be connected with these dedicated links. A full mesh of connected sites would consequently imply an exponential increase in the cost associated. Frame Relay and ATM were the first technologies widely adopted to implement VPNs. These networks consisted of various devices, belonging to either the customer or the service provider, that were components of the VPN solution.

Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following Overlay model, Peer-to-peer model.

1. INTRODUCTION

Historically, private WANs were provisioned using dedicated leased line connections, each line providing a point-to-point connection between two customer sites. 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. 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

2. CURRENT METHODOLOGY:

A **virtual private network** (**VPN**) is a method of computer networking–typically using the public internet–that allows users to privately share information between remote locations, or between a remote location and a business' home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely.

VPNs are frequently used by remote workers or companies with remote offices to share private data and network resources. VPNs may also allow users to bypass regional internet restrictions such as firewalls, and web filtering, by "tunneling" the network connection to a different region. Technically, the VPN protocol encapsulates network data transfers using a secure cryptographic method between two or more networked devices which are not on the same private network, to keep the data private as it passes through the connecting nodes of a local or wide area network.

3. PROPOSED SYSTEM

The recent evolution of IP networks is seeing IP Applications becoming more complex and requiring higher bandwidth consumption. More recently, IP networks are employing Multi-Protocol Label Switching (MPLS) which offers better switching and enables Virtual Private Network (VPN).However, the service quality is becoming a major issue in MPLS networks due to having to accommodate the higher bandwidth consumption by certain applications such as voice over IP (VoIP), client–server and peer-to-peer applications, java applications and customized applications. This paper will focus on the implementation of Quality of Service (QoS) in MPLS networks using the java network simulation tool called J-SIM. Recently there has been an increasing market demand to provide metropolitan and longer-reach Ethernet connectivity. According to a Yankee Group estimate, in 2001 the market for virtual private network (VPN) services over traditional (ATM and Frame Relay) transports was three times larger than IP VPN services in 2000, although the IP (including Multiprotocol Label Switching [MPLS)) segment is growing much faster and could eclipse traditional services before 2005.This growth, combined with the increasing need to protect existing infrastructure and provide traditional point-to-point connections of different types, has pushed service providers to Look for solutions that allow them to carry Layer 2 and Layer 3 traffic across a common, converged, single infrastructure without changing the existing service models.

The appearance of new uses underlines the need for a greater quality of service (QoS) not only for conveying accurately or increasing a certain traffic, but also conveying it as soon as Possible while holding management account of the resources networks (band-width), which implies a network management even more complex. These are the needs which gave birth to MPLS technology. This technology adapted particularly well to the engineering of traffic because it allows the creation of ways that are explicit and independent of IP road. In this article we tried to deduce principal operation from MPLS protocol in IMS architecture. We propose to associate the mechanisms of management of QoS in the architecture of the Next Generation Networks (NGN) with plan of IP Multi-media Subsystem session (IMS). We will strongly highlight the importance of the MPLS used for the transport of the IP datagram and the traffic. We underline the advantages of MPLS utility in the IMS platforms to provide guarantees of QoS from beginning to end.

4. COMPONENT DETAILS:

GNS3 is a Graphical Network Simulator that allows emulation of complex networks. We may be familiar with VMware or Virtual PC that are used to emulate various operating systems in a virtual environment. These programs allow we to run operating systems such as Windows XP Professional or Ubuntu Linux in a virtual environment on our computer. GNS3 allows the same type of Emulation using Cisco Internetwork Operating Systems. It allows us to run a Cisco IOS in a virtual environment on our 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 in-type files with dynagen running on top of Dynamips. GNS3 takes this a step further by providing a graphical environment.

To allow complete simulations, GNS3 is strongly linked with:

- Dynamips, the core program that allows Cisco IOS emulation.
- Dynagen, a text-based front-end for Dynamips.
- Qemu, a generic and open source machine emulator and virtualizes.

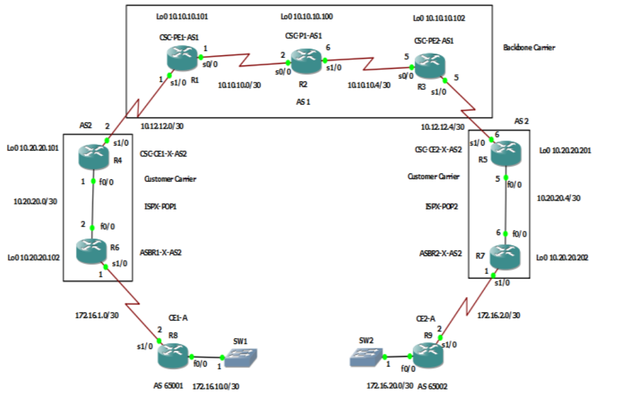
5. DESIGN TOPOLOGY:

The following prerequisites are required to configure MPLS Layer 3 VPN:

To perform these configuration tasks, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group includes the corresponding command task IDs. All command task IDs are listed in individual command references and in the Cisco IOS XR Task ID Reference Guide. If you need assistance with your task group assignment, contact your system administrator. You must be in a user group associated with a task group that includes the proper task IDs for

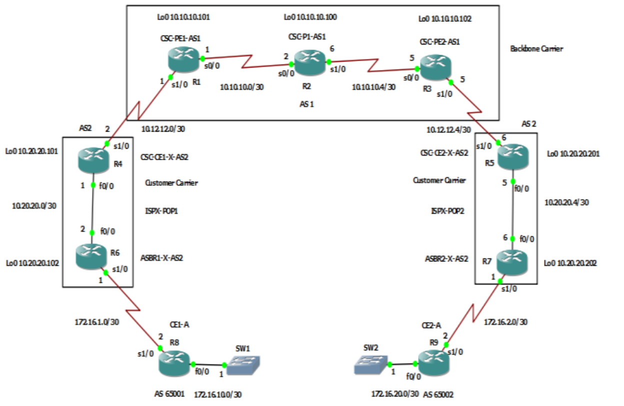
- – BGP commands
- – MPLS commands (generally)
- – MPLS Layer 3 VPN commands
- The following prerequisites are required for configuring MPLS VPN Inter-AS with autonomous system
- boundary routers (ASBRs) exchanging VPN-IPV4 addresses or IPv4 routes and MPLS labels:

Before configuring external Border Gateway Protocol (eBGP) routing between autonomous systemsor subautonomous systems in an MPLS VPN, ensure that all MPLS VPN routing instances and sessions are properly configured.



CARRIER SUPPORTING CARRIER NETWORK

DESIGN TOPOLOGY



6. CONCLUSION:

As internet is said to be expanding and need for support for file, transfers of corporate company's 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.

Future scope

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

ACKOWLEDGEMENT:

I strongly record my deep sense of gratitude and thankfulness with utmost respect to my project guides MR. RAVINDRAN (ASSISTANT GENERAL MANAGER) and MR.SASIKUMAR (JUNIOR TELECOM OFFICER) – BSNL-RGMTTC for giving me this wonderful opportunity to work on the project **"CARRIER SUPPORTING CARRIER(One ISP is supporting other ISP for sending Internet/VPN traffic): WITH CUSTOMER CARRIER PROVIDING MPLS VPN SERVICES TO USER SITES"**

REFERENCES:

[1] Julian Andres , Caicedo-Munoz, "QoS-Classifier for VPN and Non-VPN traffic based on time-related features", Elsevier Computer Networks 144(2018) 271-279.

[2] Vishal H. Shukla, Sanjay B. Deshmukh, "Implementing QOS Policy in MPLS Network", International Journal of Computer Applications, 2015 (0975 – 8887).

[3] Nasser-Eddine Rikli, "Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks", Journal of King Saud University – Computer and Information Sciences (2013) 25, 89–98.

[4] Samiullah mehraban1, "Deploy Multi Protocol Label Switching (MPLS) using Virtual Routing and Forwarding (VRF)", (ICOEI 2018)

[5] Mohammad Hossein Bateni, "Multi-VPN Optimization for Scalable Routing via relaying" , IEEE/ACM transactions on networking, vol. 18, no. 5, october 2010