RESEARCH ARTICLE OPEN ACCESS

INTERNET SERVICE WITH MPLS VPN IN MULTI PROTOCOL LABEL SWITCHING

Karthik P[1], Shalini S [2]
1(Assistant Professor, Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: pkpristuni@gmail.com)
2 (M.C.A., Scholar Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: shalinisaravana96@gmail.com)

Abstract:

In computer networking and telecommunications internet service using mpls vpn in multi protocol label switching (MPLS) is a data carrying mechanism, which emulates some properties of circuit switched network over packet switched network. Branches of Corporate companies have normally distributed their data over the entire nation at least. They may require their own private, secure, faster and economic data network between corporate office and all branch offices. Virtual Private Network (VPN) is the solution for the above problem. In this concept only switched path (Virtual Paths) are assigned between the hosts. A VPN enables to send data between two computers across the shared or public internetwork in a manner that emulates the properties of a point to point private link. MPLS VPN takes the advantage of the inherent characteristics of MPLS to provide secured data networking, typically for business users, in conjunction with other VPN technologies to help increase scalability while keeping costs at a manageable level.

***Keywords* — MULTI PROTOCOL LABEL SWITCHING (MPLS), Virtual Private Network (VPN), Virtual Paths.**

I. INTRODUCTION

The purpose of this research is to demonstrate the configuration used to access the Internet services from a Multiprotocol Label Switching (MPLS)-based VPN using a global routing table. In certain network scenarios, it is required to access the Internet from an MPLS-based VPN in addition to continuing to maintain the VPN connectivity among corporate sites. This configuration focuses on providing Internet access from the VPN routing and forwarding (VRF) that contains the default route to the Internet gateway router (IGW).

II. PROBLEM ANALYSIS

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. There are many types quality of service can be offered in MPLS network and one of them is Differentiated Services or Diffserv which is being used in this work. This paper presents the QoS benefits of Diff-Serv aware MPLS networks when simulating the network using J-Sim. Outputs such as throughput and packet drops will be discussed in this paper also in conclusion, Authors suggest that J-Sim has been used to perform the evaluation of DiffServ-Aware

MPLS network. The QoS scheme selected is Differentiated Services because of its scalability in large networks and its per hop behavior which enables it to be implemented independently. The simulation results show that there are excellent improvements in throughput for EF traffic when Diffserv is used to police traffic.

ISSUES IN SERVICES

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 [MPI.S)) 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. Thus Cisco has an opportunity to deliver its Layer 2 tunneling solutions to address this market requirement. Cisco Any Transport over MPI.S (AtoM) is one such solution that addresses the needs of providers who would like to deploy MPI.S and offer services such as Layer 2 aggregation and virtual leased lines using MPI.S traffic engineering and quality of service (QoS) along with Cisco AtoM. Our paper “A study on any transport over MPI.S” is divided into the following main parts: The first part present “Introduction”. The second part present “AtoM pseudo wire operation”. The third part present “AtoM and QoS support”. The fourth part present “Dilfer and AtoM”. The fifth part present “Configuration Examples for AtoM by NS2”. The sixth part present “Conclusion”.

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. Admittedly, the growth of the flows of access and the convergence of the services known as “triple play”(Internet, voice/videoconference, television video on demand) on An infrastructure IP federator involves a considerable increase of volumes of IP traffic as well as new constraints in terms of QoS and reliability for IP networks. Mechanisms of engineering of Traffic, QoS and security become necessary to support this evolution (in terms of volume and nature) of the transported traffics. Various methods of engineering of traffic for IP

Networks have been specified for several years. Among these methods, we find one based on the use of 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. We conclude our article by a simulation from an MPLS network. In this article puts the light on the basic principles of MPLS protocol, release its interest and the advantages it offers to the developers, to the ordinary users and his combination with the IMS. We illustrated results of simulation on MPLS network relating to the processes of routing. We proposed to associate the mechanisms of management of QoS in the NGN with plan of IMS session. We could underline the advantages of this architecture in MPLS. The solution suggested by guaranteed MPLS of QoS is guaranteed even if several fields are crossed. We contribute by a new way of approaching the modern networks, by highlighting the fact that the traditional technological cleavages used until now to present the networks (in particular cleavages Telecoms vs. LAN or vs. WAN, or layer 2 vs. layer 3 of OSI model

III. PROPOSED METHODOLOGY:

3.2.1 Layer 3 VPNs (L3VPN)

L3vpn provides IP and MPLS-based network virtualization solutions for enterprise and service provider customers.MPLS Layer 3 VPNs use a peer-to-peer model that uses Border Gateway Protocol (BGP) to distribute VPN-related information. This highly scalable, peer-to-peer model allows enterprise subscribers to outsource routing information to service providers, resulting in significant cost savings and a reduction in operational complexity for enterprises. Service providers can then offer value-added services like Quality of Service (QoS) and Traffic Engineering,

3.2.2 Border Gateway Protocol (BGP) VPNs

Layer 3 VPN over Multiprotocol Label Switching (MPLS) is the most widely deployed MPLS application in Service Provider and self-managed Enterprise networks. Implementation of this architecture provides secure control and forwarding planes upon which to build robust VPNs.Virtual Routing Forwarding instances constructed by Multiprotocol-Border Gateway Protocol (MP-BGP) provide adequate routing separation on a shared multi-service edge. The integration between MP-BGP and MPLS technology allows users to maintain separation between traffic from multiple subscriber networks as the traffic is switched through a single shared core.

IOS MPLS Layer 3 VPNs enable Service Providers to offer any-to-any connectivity services that can be implemented over either an MPLS or an IP infrastructure.To meet unique customer requirements, It has also extended MPLS Layer3 VPN support over IP with MPLS VPN over IP. This solution, which supports Layer 3 VPNs for L2TPv3, eliminates the need to implement MPLS in the core.

Service Providers can realize numerous benefits from the MPLS Layer 3 VPN architecture. It enables them to:

- Build scalable, manageable, and secure LAN, MAN, and WAN networks
- Provide precise Service Level Agreements for IP traffic
- Bundle Internet connectivity, Voice over IP, Multicast, and traditional IP services, which are already present in most subscriber networks
- Support remote access technologies (ie: DSL, Dial, IPsec)
- Ease migration from Frame Relay or ATM to Layer 3 VPN services

3.2.3 Simplified Layer 3 Network Virtualization

Deliver traffic separation and path isolation capabilities on a shared network infrastructure with Easy Virtual Network (EVN). An IP-based network virtualization solution, EVN takes advantage of existing Virtual Routing and Forwarding (VRF)-Lite technology to simplify Layer 3 network virtualization, improve support for shared services, and enhance management and troubleshooting.

3.2.4 Inter-AS/Carrier Supporting Carrier

Deployments of Multiprotocol Label Switching (MPLS) have become routine in large-scale global networks, which demand solutions to complex business and network problems. There are two primary components of the IOS MPLS Inter-Domain Solution: Inter-AS and Carrier Supporting Carrier.

Carrier Supporting Carrier (CSC) is a hierarchical VPN model that allows small Service Providers, or customer carriers, to interconnect their IP or MPLS networks over an MPLS backbone. This eliminates the need for customer carriers to build and maintain their own MPLS backbone. Both Inter-AS and CSC can construct scalable networks that help maintain network segmentation based on internal organizational or operational boundaries.

3.2.5 Multicast VPN

This process provides the service providers to provide multiple numbers of unique services and resource utilization and QOS can be enhanced

3.2.6 VRF-Aware Services

IOS Multiprotocol Label Switching (MPLS) for Managed Shared Services enable Service Providers to offer the connectivity benefits of MPLS VPNs to their subscribers. Service Providers can also leverage this technology to provide economically attractive IP services, creating additional revenue streams. It continues to expand its widely deployed IOS MPLS VPN solution to include both traditional and advanced services: IP address translation and management, Security, Redundancy, Multicast VPNs, VPN Select, and network management. Enterprise customers can use this flexible, open service model to offload and outsource traditional IP services to their Service Providers. These services can also be consolidated across self-managed Enterprise MPLS VPN networks for greater operational leverage and economies of scale

3.2.7 Advantage of these services

- Provide a diversified range of services (Layer 2, Layer 3 and Dial up VPNs) to meet the requirements of the entire spectrum of customers from Small and Medium to Large business enterprises and financial institutions.
- Make the service very simple for customers to use even if they lack experience in IP routing.
- Make the service very scalable and flexible to facilitate large-scale deployment.
- Provide a reliable and amenable service.
- Offering SLA to customers.
- Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity and Capable of offering fully managed services to customers

3.3. Software Description

3.3.1 Introduction to GNS3 (Graphical Network Interface)

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.

GNS3 allows the emulation of Cisco ios on our 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, 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 practiceIn these simulators we 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. However, due to licensing restrictions, we will have to provide our own Cisco ios 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. GNS3 was developed primarily by Jeremy Grossmann. Additional developers involved in creating GNS3 are David Ruiz, Romain Lamaison, Aurélien Levesque, and Xavier Alt. Dynamips was developed by Christophe Fillot. Dynagen"s primary developer was Greg Anuzelli.

3.3.2 Introduction to Wire shark (Network Analyzer)

Wire shark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

3.3.3 Features

- Data can be captured "from the wire" from a live network connection or read from a file that recorded already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.

3.4 System Implementation

3.4.1 L3vpn Approach

System Implementation:

The following steps are followed in creating an MPLS based L3Vpn network environment and analyzing its performance

Topology setup module:

Initially the setup is being created and in IOS-enabled GNS3 simulator to yield a high performance we select a c7200 high end edge routers is selected and placed in the virtualization area a total of 6 routers is being selected and placed in an mesh topology

Structure

- Two act as the MPLS back bone supporting routers
- Two act as the provider edge router backed with BGP-MPLS support

L3vpn approach can be implemented considering the following parameter

IP Addressing module:

Basically IP addressing can be done in two ways,

- Static addressing
- Dynamic addressing

Due to inflexibility we leave out static addressing process and consider dynamic addressing which is more reliable and flexible in configuring IP addresses

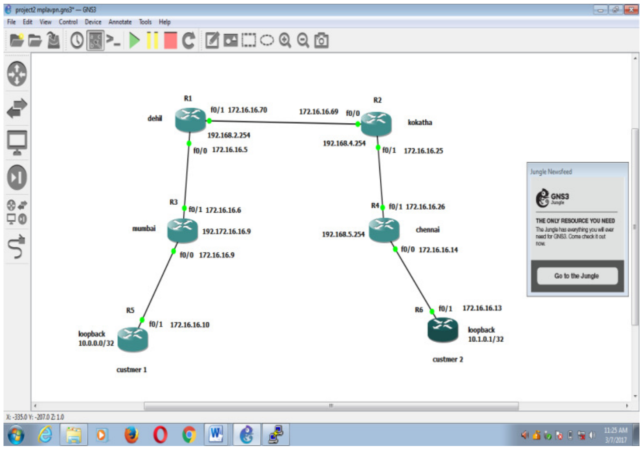
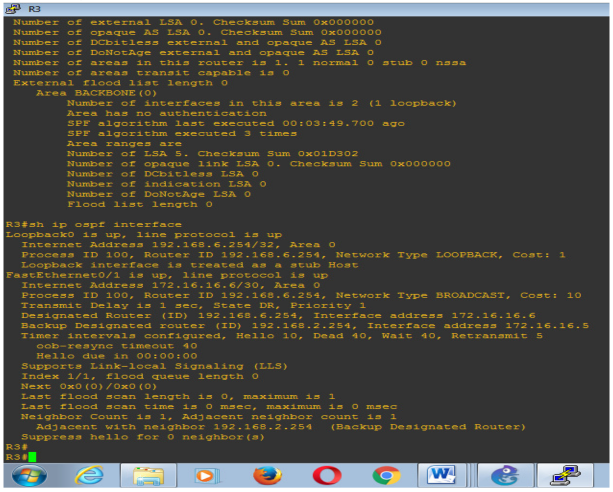


Fig.3.4 schematic network topology

Router connectivity module:

In order to complete high capable data transfer we consider the implementation of Gigabyte Ethernet (GE) cable connectivity throughout the network linking all the routers from (R1-R6)



```
R3
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 00:03:49.700 ago
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x01D302
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

R3#sh ip ospf interface
Loopback0 is up, line protocol is up
  Internet Address 192.168.6.254/32, Area 0
  Process ID 100, Router ID 192.168.6.254, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
FastEthernet0/1 is up, line protocol is up
  Internet Address 172.16.16.6/30, Area 0
  Process ID 100, Router ID 192.168.6.254, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.6.254, Interface address 172.16.16.6
  Backup Designated router (ID) 192.168.2.254, Interface address 172.16.16.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.254  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
R3#
```

Fig.3.5 Router connectivity module

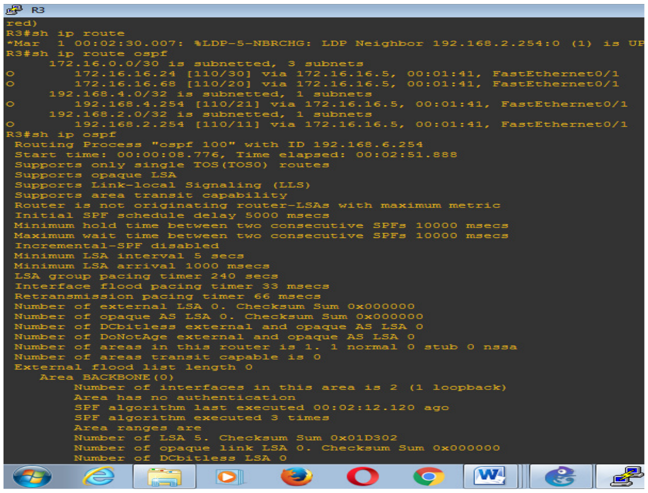
OSPFv2-Dynamic Addressing module

Among the a variety of available dynamic addressing protocols we like better to implement OSPF (open shortest path algorithm) It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm for every router employed in the network

(OSPF) Process of dynamic addressing is done it provide the capability of the routers to construct and maintain IP routing tables of associated resources when customized this enhances the steadfastness to the network

Loop back addressing module

This aspect enables the connectivity sandwiched between the virtual feedback environments The most commonly used IP address on the loopback device is 127.0.0.1 for IPv4, even though any address in the range 127.0.0.0 to 127.255.255.255 is mapped to it

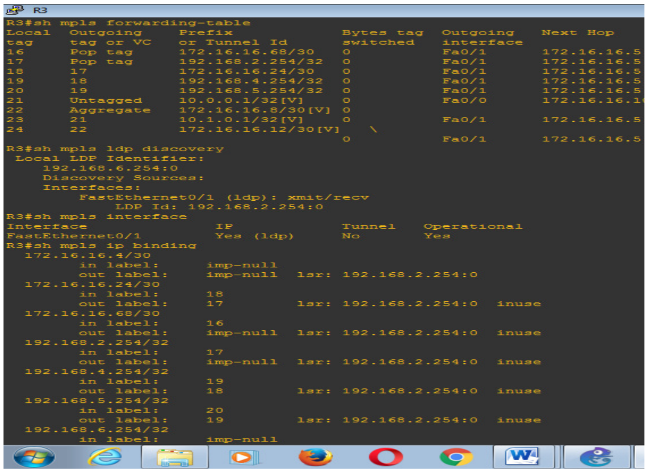


```
R3
red)
R3#sh ip route
*Mar  1 00:02:30.007: %LDP-5-NBRCHG: LDP Neighbor 192.168.2.254:0 (1) is UP
R3#sh ip route ospf
     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.16.24 [110/30] via 172.16.16.5, 00:01:41, FastEthernet0/1
O       172.16.16.68 [110/20] via 172.16.16.5, 00:01:41, FastEthernet0/1
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.254 [110/21] via 172.16.16.5, 00:01:41, FastEthernet0/1
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.254 [110/11] via 172.16.16.5, 00:01:41, FastEthernet0/1
R3#sh ip ospf
 Routing Process "ospf 100" with ID 192.168.6.254
 Start time: 00:00:08.776, Time elapsed: 00:02:51.888
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 00:02:12.120 ago
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x01D302
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
```

Fig.3.6 Loop back addressing module

Configuring- MPLS module

MPLS is a high end utility to the VPN networks it provides better flexibility and Security to the network



```
R3
R3#sh mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     172.16.16.68/30   0          Fa0/1      172.16.16.5
17     Pop tag     192.168.2.254/32  0          Fa0/1      172.16.16.5
18     17          172.16.16.24/30   0          Fa0/1      172.16.16.5
19     18          192.168.4.254/32  0          Fa0/1      172.16.16.5
20     19          192.168.5.254/32  0          Fa0/1      172.16.16.5
21     Untagged    10.0.0.1/32[V]    0          Fa0/0      172.16.16.1
22     Aggregate   172.16.16.8/30[V] 0
23     21          10.1.0.1/32[V]    0          Fa0/1      172.16.16.5
24     22          172.16.16.12/30[V]   \
                                     0          Fa0/1      172.16.16.5
R3#sh mpls ldp discovery
 Local LDP Identifier:
    192.168.6.254:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/1 (ldp): xmit/recv
            LDP Id: 192.168.2.254:0
R3#sh mpls interface
Interface              IP            Tunnel   Operational
FastEthernet0/1        Yes (ldp)     No       Yes
R3#sh mpls ip binding
  172.16.16.4/30
        in label:     imp-null
        out label:    imp-null  lsr: 192.168.2.254:0
  172.16.16.24/30
        in label:     18
        out label:    17        lsr: 192.168.2.254:0  inuse
  172.16.16.68/30
        in label:     16
        out label:    imp-null  lsr: 192.168.2.254:0  inuse
  192.168.2.254/32
        in label:     17
        out label:    imp-null  lsr: 192.168.2.254:0  inuse
  192.168.4.254/32
        in label:     19
        out label:    18        lsr: 192.168.2.254:0  inuse
  192.168.5.254/32
        in label:     20
        out label:    19        lsr: 192.168.2.254:0  inuse
  192.168.6.254/32
        in label:     imp-null
```

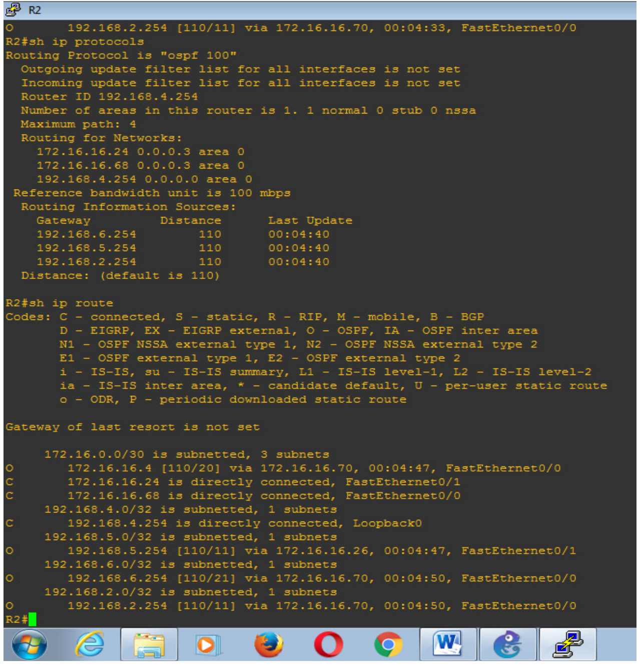
Fig.3.7 Configuring- MPLS module

The process of configuring MPLS to the network is done in two ends

- Provider (P)
- Provider Edge (PE)

Configuring VPN module

The routers P network act as the MPLS core network and that MPLS is programmed In to two dynamic ways one globally and the other uniquely to the specific router this P network routers acts as the MPLS back bone of the entire network they tend to act as the carriers of the packets with swapping of the labels assigned and relatively not interfering with the packet IP address

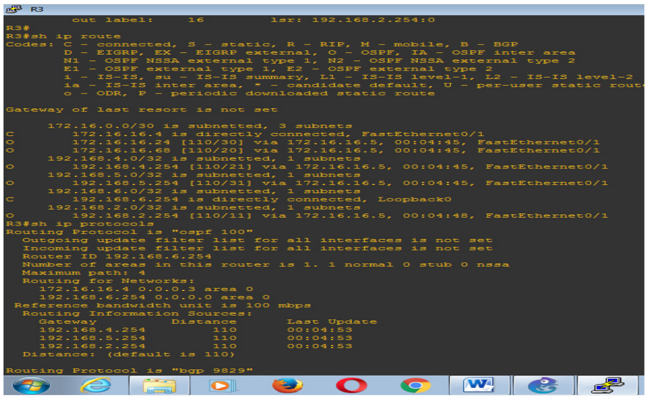


```
R2
O       192.168.2.254 [110/11] via 172.16.16.70, 00:04:33, FastEthernet0/0
R2#sh ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.4.254
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.16.24 0.0.0.3 area 0
    172.16.16.68 0.0.0.3 area 0
    192.168.4.254 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.6.254        110      00:04:40
    192.168.5.254        110      00:04:40
    192.168.2.254        110      00:04:40
  Distance: (default is 110)

R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.16.4 [110/20] via 172.16.16.70, 00:04:47, FastEthernet0/0
C       172.16.16.24 is directly connected, FastEthernet0/1
C       172.16.16.68 is directly connected, FastEthernet0/0
     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.254 is directly connected, Loopback0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.254 [110/11] via 172.16.16.26, 00:04:47, FastEthernet0/1
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.254 [110/21] via 172.16.16.70, 00:04:50, FastEthernet0/0
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.254 [110/11] via 172.16.16.70, 00:04:50, FastEthernet0/0
R2#
```

Fig.3.8 Configuring VPN module

Configuring PE routers module

This is said to be the edge routers of the network. Here also the MPLS configuration is done Dynamically that is both globally and uniquely to separate routers but since the customer edge is in no need of the MPLS support, the router terminal which is connected to the provider edge alone is configured with MPLS and the other end of the terminal connected to the customer edge is not configured with MPLS

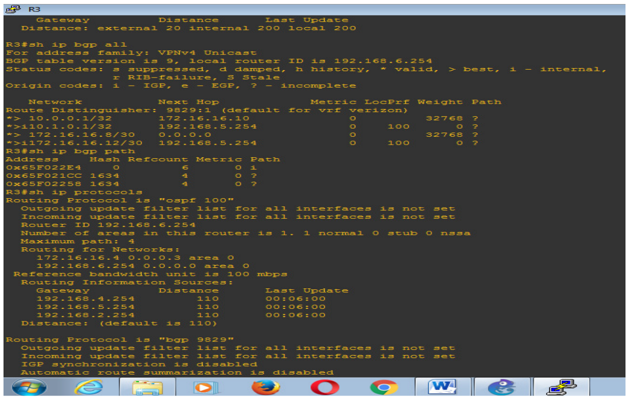


```
        out label:     16          lsr: 192.168.2.254:0
R3#
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.16.4 is directly connected, FastEthernet0/1
O       172.16.16.24 [110/30] via 172.16.16.5, 00:04:45, FastEthernet0/1
O       172.16.16.68 [110/20] via 172.16.16.5, 00:04:45, FastEthernet0/1
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.254 [110/21] via 172.16.16.5, 00:04:45, FastEthernet0/1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.254 [110/31] via 172.16.16.5, 00:04:45, FastEthernet0/1
     192.168.6.0/32 is subnetted, 1 subnets
C       192.168.6.254 is directly connected, Loopback0
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.254 [110/11] via 172.16.16.5, 00:04:48, FastEthernet0/1
R3#sh ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.6.254
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.16.4 0.0.0.3 area 0
    192.168.6.254 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.4.254        110      00:04:53
    192.168.5.254        110      00:04:53
    192.168.2.254        110      00:04:53
  Distance: (default is 110)

Routing Protocol is "bgp 9829"
```

Fig.3.9 Configuring PE routers module

Configuring BGP module

This is the most important configuration done to the network it enables inter connectivity between the As-As another feature of this BGP protocol is that it provides separate creation of VRF's which are very effective in controlling and maintaining route information's of separate VPN's this VRF's are highly effective since they utilize virtual tables they don't consume large resource's compared to other inter As-As protocolsThe configuration is done to the side of the PE terminal which is connected to the Customer edge. This enable the separate VPN's to connect with the internet cloud which is nothing but the collection of inter As-As

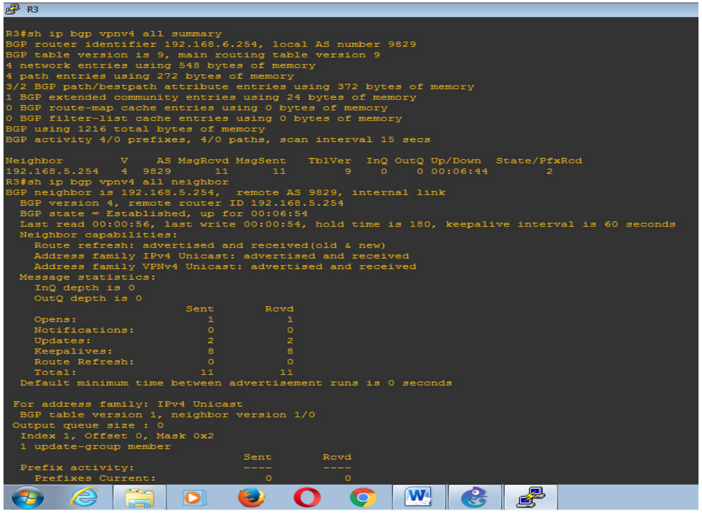


```
    Gateway         Distance      Last Update
  Distance: external 20 internal 200 local 200

R3#sh ip bgp all
For address family: VPNv4 Unicast
BGP table version is 9, local router ID is 192.168.6.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 9829:1 (default for vrf verizon)
*> 10.0.0.1/32      172.16.16.10             0         32768 ?
*>i10.1.0.1/32      192.168.5.254            0    100      0 ?
*> 172.16.16.8/30   0.0.0.0                  0         32768 ?
*>i172.16.16.12/30  192.168.5.254            0    100      0 ?
R3#sh ip bgp path
Address    Hash Refcount Metric Path
0x65F022E4    0        6      0 i
0x65F021CC 1634        4      0 ?
0x65F02258 1634        4      0 ?
R3#sh ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.6.254
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.16.4 0.0.0.3 area 0
    192.168.6.254 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.4.254        110      00:06:00
    192.168.5.254        110      00:06:00
    192.168.2.254        110      00:06:00
  Distance: (default is 110)

Routing Protocol is "bgp 9829"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
```

Fig.3.10 Configuring PE routers module

configuring separate VPN's module

This configuration process enables the creation of an separate VPN"s in the network this process provides the ability to the Provider edge to configure and maintain unique VPN's.This VPN configuration is done to the provider edge terminal connected to the unique customer edge terminal this in turn enables the creation of unique VPN's Numerous number of VPN's can be created and separately maintained with high quality of service (QoS)

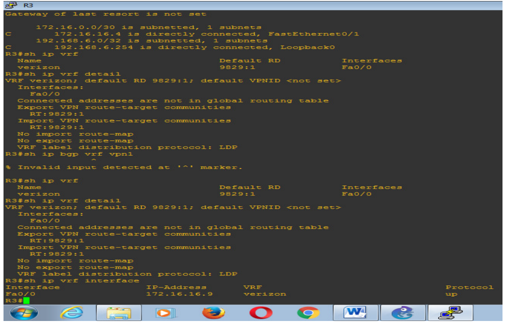


```
R3#sh ip bgp vpnv4 all summary
BGP router identifier 192.168.6.254, local AS number 9829
BGP table version is 9, main routing table version 9
4 network entries using 548 bytes of memory
4 path entries using 272 bytes of memory
3/2 BGP path/bestpath attribute entries using 372 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1216 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.5.254   4  9829      11      11        9    0    0 00:06:44        2
R3#sh ip bgp vpnv4 all neighbor
BGP neighbor is 192.168.5.254,  remote AS 9829, internal link
  BGP version 4, remote router ID 192.168.5.254
  BGP state = Established, up for 00:06:54
  Last read 00:00:56, last write 00:00:54, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                2          2
    Keepalives:             8          8
    Route Refresh:          0          0
    Total:                 11         11
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
```

Fig.3.11 configuring separate VPN's module

Inter As-As BGP VRF's module

To the created VPN's separate vrf's can be created using BGP protocol v4.This enables the deployment of inter As-As virtual tables and act as the connectivity.Accordance of the inter network connectivity This VRF enable high speed routing mechanism as well as the resource conception is ideally low



```
Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.16.4 is directly connected, FastEthernet0/1
     192.168.6.0/32 is subnetted, 1 subnets
C       192.168.6.254 is directly connected, Loopback0
R3#sh ip vrf
  Name                             Default RD          Interfaces
  verizon                          9829:1              Fa0/0
R3#sh ip vrf detail
VRF verizon; default RD 9829:1; default VPNID <not set>
  Interfaces:
    Fa0/0
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:9829:1
  Import VPN route-target communities
    RT:9829:1
  No import route-map
  No export route-map
  VRF label distribution protocol: LDP
R3#sh ip bgp vrf vpn1
                 ^
% Invalid input detected at '^' marker.

R3#sh ip vrf
  Name                             Default RD          Interfaces
  verizon                          9829:1              Fa0/0
R3#sh ip vrf detail
VRF verizon; default RD 9829:1; default VPNID <not set>
  Interfaces:
    Fa0/0
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:9829:1
  Import VPN route-target communities
    RT:9829:1
  No import route-map
  No export route-map
  VRF label distribution protocol: LDP
R3#sh ip vrf interface
Interface              IP-Address      VRF                              Protocol
Fa0/0                  172.16.16.9     verizon                          up
R3#
```

Fig.3.12 Inter As-As BGP VRF's module

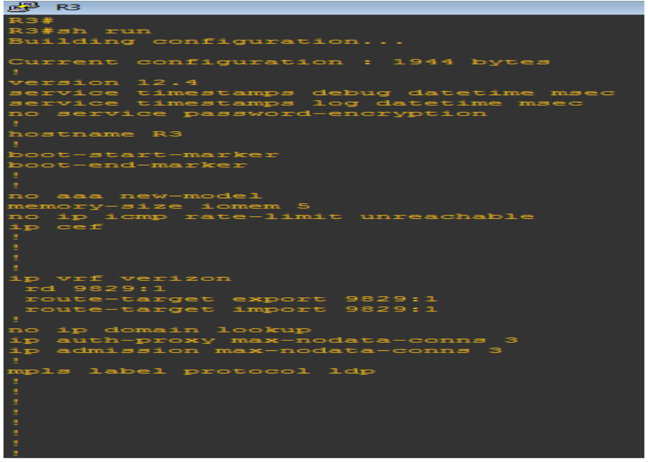
Summary

The configuration enabled in the entire l3vpnv4 services deployed is illustrated below the following parameters are very essential in maintaining the entire stream of network topology schematics of protocol used their reliability and dependency in using the resources efficiently

The following are specified below,

- Connectivity
- Protocol used
- Interfaces
- Services

- Domain name
- Coverage
- Routing mechanism



```
R3#
R3#sh run
Building configuration...

Current configuration : 1944 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf verizon
 rd 9829:1
 route-target export 9829:1
 route-target import 9829:1
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
```

Fig.3.13 Summary

4.1 Implementation

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 (see the How to Implement MPLS Layer 3 VPNs, page VPC-218

• The following tasks must be performed:

– Define VPN routing instances

– Configure BGP routing sessions in the MPLS core

– Configure PE-to-PE routing sessions in the MPLS core

– Configure BGP PE-to-CE routing sessions

– Configure a VPN-IPv4 eBGP session between directly connected ASBRs

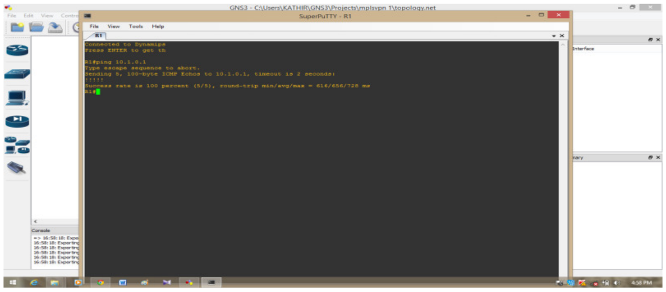
To configure MPLS Layer 3 VPNs, routers must support MPLS forwarding and Forwarding Information

Base (FIB).

Implementing MPLS Layer 3 VPNs

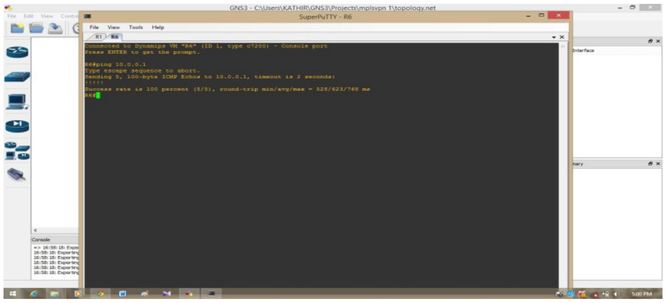
Sample Result

Ping module from customer 1 to same side router (Pune)



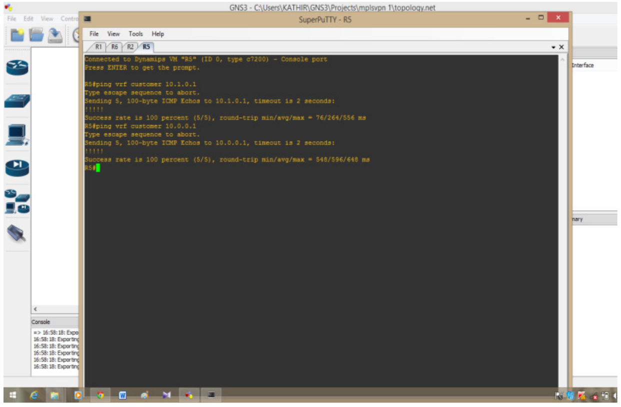
```
Connected to Dynamips
Press ENTER to get th

R1#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 = 616/656/728 ms
R1#
```

Ping module from customer 2 to same side router (Chennai)



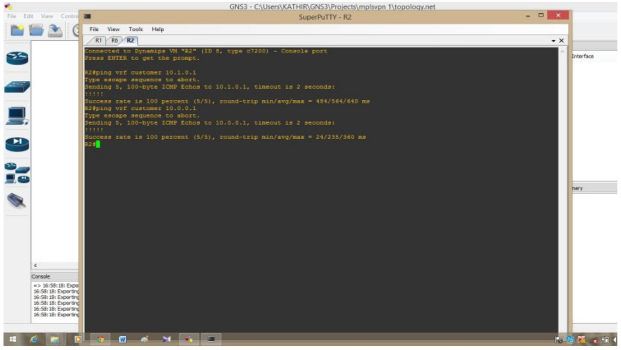
```
Connected to Dynamips VM "R6" (ID 1, type c7200) - Console port
Press ENTER to get the prompt.

R6#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 = 528/623/768 ms
R6#
```

Ping module from Chennai router to the other end router (customer 1)



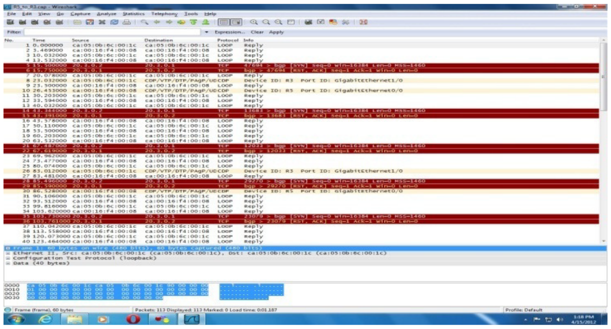
```
Connected to Dynamips VM "R5" (ID 0, type c7200) - Console port
Press ENTER to get the prompt.

R5#ping vrf customer 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 = 76/264/556 ms
R5#ping vrf customer 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 = 548/596/648 ms
R5#
```

Ping module from Pune router to the other end router (customer 2)



```
Connected to Dynamips VM "R2" (ID 8, type c7200) - Console port
Press ENTER to get the prompt.

R2#ping vrf customer 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 = 484/564/640 ms
R2#ping vrf customer 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 = 24/235/360 ms
R2#
```

4.2 Analyzing module



IV. CONCLUSIONS

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

V. 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

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. *Lan jun ,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, Anjulata Yadav,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.Arifur Rahman, 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) '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 Quoc Cuong, Ph.D, Tran Thi Thuy (2010) 'A Study on Any Transport over MPLS (AToM)'Functioning and Management of MPLS/QOS In the IMS architectureA. Saika*, R. El KOUCH International.*

10. *Zakaria Bin Ali,Mustaffa Samad,Habibah (2011) 'Performance Comparison of Video Multicasting over Asynchronous Transfer Mode (ATM) & Multiprotocol Label Switching (MPLS) Networks', IEEE International*