ISEL

INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA
SERVIÇO DE DOCUMENTAÇÃO E PUBLICAÇÕES

INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA
Área Departamental de Engenharia de Electrónica e Telecomunicações e de Computadores

Point-to-Point
IP VPN
VPLS

MPLS Layer 3 VPN

Hamid Khanpour
(Bachelor's degree in Electronic and Telecommunication)

Trabalho Final de Mestrado para Obtenção do Grau de Mestre em Engenharia de Electrónica e Telecomunicações

Orientador:
Professor Doutor Mário Pereira Véstias
Júri:
Presidente: Professora Doutora Paula Maria Garcia Louro
Vogais:
Professor Doutor Rui Policarpo Duarte
Professor Doutor Mário Pereira Véstias

December 2017

ACKNOWLEDGEMENTS

First and foremost, I wish to express my most sincere gratitude and appreciation to Professor Doutor Mário Pereira Véstias for his guidance, patience, encouragement and advice that he has provided throughout the development of the project and likewise being an extraordinary mentor. This project would not be nearly as good without his helps and also Professor Doutor Rui Policarpo Duarte.

Second, I would like to thank Professor Doutor Manuel Barata and Professor Doutor Edwardo Eusebio for their help and support.

I must express my gratitude to my wife, Ukabed has been encouragement and extremely supportive of me throughout this entire process and has made countless sacrifices to help me get to this point. My parents and Dr. Ahmad Shahsavan (my wife's father), deserve special thanks for their continued support and encouragement. Without such a team behind me, I doubt that I would be in this place today.

ABSTRACT

Multiprotocol Label Switching (MPLS) is the principal technology used in Service Provider Networks as this mechanism forwarding packet quickly. MPLS is a new way to increase the speed, capability and service supplying abilities for optimization of transmission resources. Service Provider networks use this technology to connect different remote sites. MPLS technology provides lower network delay, effective forwarding mechanism, ascendable and predictable performance of the services which makes it more appropriate for carry out real-time applications such as Voice and video. MPLS can be used to transport any type of data whether it is layer 2 data such as frame relay, Ethernet, ATM data etc. or layer 3 data such as IPV4, IPV6.

Keywords: - VPN, MPLS, MPLS VPNs, Layer 3, Layer 2, ATM, IPV4 and IPV6.

TABLE OF CONTENTS

CHAPTER ONE

CHAPTER TWO

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

LIST OF FIGURES

LIST OF TABLE

ACRONYMS

ABR	area border router
AFI	address family identifier
AS	autonomous system
ASN	autonomous system number
ASBR	autonomous system border router
ATM	Asynchronous Transfer Mode
BCD	Binary Coded Decimal
BDR	Backup Designated Router
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BoS	Bottom of Stack
CBGP	confederated Border Gateway Protocol
CE	Customer Edge (router)
CLNP	Connectionless Network Protocol
CLR	Conservation Label Retention Mode
CsC	Carrier Supporting Carrier
DCU	Destination Class Usage
DIS	designated intermediate system
DR	Designated Router
DUAL	Diffuse Update Algorithm
EBGP	exterior Border Gateway Protocol
ECMP	equal-cost multipath
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EL-BGP	external Labelled BGP, see L-EBGP
FA-LSP	Forwarding Adjacency LSP
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base (forwarding table)
GMPLS	Generalized Multiprotocol Label Switching
GNS3	Graphical Network Simulator-3
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
IBGP	interior Border Gateway Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IL-BGP	internal Labelled BGP, see L-IBGP
IOS	Internetworking Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS–IS	Intermediate System to Intermediate System routing protocol

ISO	International Standards Organization
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
L-BGP	Labelled BGP
L-EBGP	Labelled exterior Border Gateway Protocol
L-IBGP	Labelled interior Border Gateway Protocol
LDP	Label Distribution Protocol
LIB	Label Information Base
LFIB	Label Forwarding Information Base
LSDB	Link-State Database
LSA	Link-State advertisement
LSI	Label-Switched Interface
LSP	label-switched path
LSP	Link-State packet or Link-State PDU
LSR	label-switched router
MP-BGP	MultiProtocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MRAI	Minimum Route Advertisement Interval
MTR	Multi-Topology Routing
OSPF	Open Shortest Path First routing protocol
QoS	Quality of Service
P	Provider Router
PDU	Protocol Data Unit
PE	Provider Edge (router)
RD	Route Distinguisher
RFC	Request for Comments
RIB	Routing Information Base (routing table)
RIP	Routing Information Protocol
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RPM	Remote Performance Measurement
RR	Route Reflector
RR	Routing Registry
RRO	Route Record Object
RSVP	Resource Reservation Protocol
SLA	service-level agreement
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
TE	Traffic Engineering
TED	Traffic-Engineering Database
TLV	Type-Length-Value
TTL	Time-To-Live
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

CHAPTER ONE

1. Introduction

1.1 Motivation

Companies are in a global economy that requires the spread of information across several geographical areas. The possibility to exchange information among offices located apart from each other permits the flat operation of the company. Regional branches transparently communicate with their head offices regularly transmitting all kind of data. Customers usually seek for flexible, safe, manageable, scalable, and low-cost networking solutions that allows them to access all information and services provided by a company.

Usually, companies do not have their own global communication network, but obtain communication services from service providers. In the past, service providers used leased lines to provide such network services. However, these leased lines have significant disadvantages. For instance, leased lines are difficult to scale when there is a large number of branches or branches expand quickly. Besides, leased lines are relatively expensive and difficult to manage. Leased lines were gradually left for other technologies, including Asynchronous Transfer Mode (ATM) and Frame Relay (FR), which rely on the concept of virtual circuits.

Recently, Multi-Protocol Label Switching (MPLS) was proposed as a way to guarantee an efficient and scalable solution for large networks. It utilizes layer 3 routing protocols besides the widely obtainable layer 2 transport systems and protocols. The IETF set up the MPLS working group in 1997 to improve a standardized approach. The objective of the MPLS working group was to standardize protocols which utilized Label Swapping forwarding techniques. The utilization of label swapping has capable advantages. It separates the routing issue from the forwarding issue.

The key component of a MPLS network is the label switching router (LSR), which is accomplished of understanding and participating in IP routing, and Layer 2 switching. MPLS has supplied important new abilities in four areas that have ensured its popularity: QoS (Quality of Service) support, Traffic Engineering, Virtual Private Network, and Multiprotocol Support.

With these new technologies, companies were able to establish Layer 3 (L3) network connections based on virtual circuits. However, the virtual circuits only supported point-to-point links, are difficult to configure and maintain. To overcome these problems, IP-based packet switching networks became popular. Now, IP-based networks are used almost everywhere in the world. Initially, L3VPNs (L3 Virtual Private Networks) were the preferred choice for many service providers. However, L3VPNs still suffer from high operational expenses and compatibility subjects. This motivates service providers to look for alternative solutions to provide low-cost private network services.

1.2 Outcomes

This thesis mainly compares IP networks with MPLS networks in terms of different routing protocols. The study will provide better understanding and learning concepts, information regarding MPLS importance uses and deployment for the businesses. This study will help us to develop the solid theoretical background for simulation projects in MPLS.

The objective of this thesis is to implement, authenticate and design two different MPLS Virtual Private Network in two different infrastructure networks. The task included building a functioning MPLS Network which contains the MPLS Backbone together with a Client Edge and the Client Site equipment's. The MPLS Backbone is to contain of the Provider Devices and the Provider Edge devices that is utilized as a connection point to the Client Edge devices.

For the area between the Provider Edge and the Customer Edge, external Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) protocols are used and do not need any MPLS information or configuration. Then it is needed for an MPLS Layer 3 VPN to be built above the MPLS network which is normally from the Service Provider. This Layer 3 or Layer 2 VPNs are used to deliver and ensure connectivity between different customers in varied geographical locations.

The result of the project is that after the configurations, it is possible to get a connection and achieve an end-to-end connectivity between the Layer3 and Layer 2 VPN´s configured on either side of the CE but none of the different site in different VPN able to communicate each other which is a good adventure of VPN for companies and it is part of security for them. This goes to prove that even though different entities might be using different networking equipment from various vendors, it is possible to make the devices communicate with or to each other and therefore provide a seamless flow of traffic/packets as if the same producer made them.

1.3 Scope of the thesis

This thesis has five chapters. The contributions of each chapter are summarized as follows:

Chapter one: provides the motivation and expected outcomes.

Chapter two: describes an overview of MPLS technology, MPLS architecture and its components.

Chapter three: provides the detailed experimental work, network design, implementing network design in GNS3 emulator and explains the protocols, used by the MPLS network.

Chapter four: reports the simulation results.

Chapter five: concludes the work and provides recommendations for future work.

CHAPTER TWO

2. State of the Art

2.1 Technology Use Cases

At first glance, when business is developing in a quick-moving, interconnected world. To encourage the sharing of ideas and speed up decision making, you have to make the latest voice and video applications accessible so people can communicate with each other clearly and successfully, wherever they are. Nevertheless with great communication power, comes great network obligation. Delays in transmission, unclear images and bad sound affect the user experience, making these tools less effective. To stay ahead of the curve, it is required the right bandwidth to support innovative communication tools.

The WAN must provide voice, video, and information transport onto a single, centrally managed and secure infrastructure. Also, to decrease the time expected to convey new technologies that help developing business applications and interchanges, the WAN architecture needs a design that able to be adjusted easily.

Up to recent years, clients demanded to connect remote sites or offices in locations through the countries were limited to the restricted WAN alternatives that service providers offered, typically E1/T1 or Frame Relay dedicated links. The issue with these WAN technologies is that they are generally difficult to manage and charging high prices, but also not very flexible, making them trouble for both service provider and the end customer. Worst case scenario, as the distance between the client's end-points improved, consequently did the monthly bill. MPLS networks are the next-generation of networks designed to allow clients create end-to-end circuits through any type of transport medium using any available WAN technology. At the beginning, VPNs were created to secure customer traffic across public WAN infrastructures which clients would share. And also with MPLS VPN, you are able to communicate quickly and securely between different sites, over a single, private, or even fibre-optic network.

2.2 MPLS Overview and Architecture

MPLS is an IP technology developed by Internet Engineering Task Force **(**IETF) to forwards traffic using labels instead of destination IP address. MPLS is a technique used by service providers to provide better and single network infrastructure for real-time traffic such as voice and video. The main advantage of utilizing MPLS is to create Virtual Private Networks. MPLS has the capacity to develop both Layer 2 and Layer 3 MPLS VPNs. Additional advantages of MPLS are traffic engineering, utilization of one unified network infrastructure, optimal traffic flow and, better IP over ATM integration. MPLS is the innovation utilized by all Internet Service Providers (ISPs) in their core or backbone networks for packet forwarding [20].

Packets can move independently, from the network algorithms of Interior Gateway Protocol (IGP) protocols, using manually configured routes. Paths built up in a MPLS network are called Label Switched Path (LSP). Each MPLS enabled router is called Label Switching Router (LSR). Redirection is typically in view of the parcel header containing the numerical estimation of the label. An MPLS label switch path is one-way and is within a single autonomous system (Autonomous System - AS) or domain. Approaches to build up MPLS LSP are:

- **Dynamically:** Dynamic LSP is built up automatically by the signalling protocol. Only the edge router (ingress router) is set up with the data required to establish paths;
- **Statically:** In this case, the administrator chooses how to forward the traffic, and what labels are utilized to distinguish resource distribution. Static LSPs expend less resources, do not require signalling protocol and don't need to store data about their state. The disadvantage is that it has to be done manually and errors may be done while configuring them. Additionally, a single device failure causes complete traffic loss.

Any Label Switching Router (LSR) can handle the MPLS header and the actions associated. LSR can be of different types: input (ingress), intermediate (transit), penultimate (penultimate) or output (egress), as shown in Figure 1.

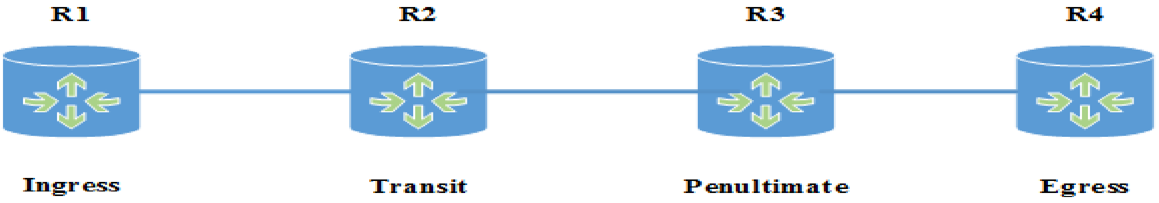


***Figure 1** - MPLS router types [20]*

In the LSR of type ingress the client IPv4 packet is encapsulated with an MPLS header. Packets are then forwarded to the egress router through the relating LSPs. Each LSP requires ingress router and just one router can be ingress for one LSP.

The Transit LSR (intermediary router) is placed between the ingress LSR and the egress LSR. One path may contain from 0 to 253 such devices. Operations performed by the transit LSR include:

- Reading the value of the label of a received packet;
- Accessing the MPLS forwarding table to find the output for a given input label;
- Label switching is utilized to forward the input label to the output label;
- The value of the Time-To-Live (TTL) field is decremented;
- The packet is forwarded to the next router along the path.
- During this operation the data in the IP header is never utilized.

The penultimate LSR is the last router before the egress LSR. Typically, its task is to remove the MPLS label from the data packet. This process is named penultimate hop popping. It supports network scalability and reduces the load on the egress router. Its tasks include:

- Determines the next and final router;
- Removes the stack of labels;
- Decreases the value of the TTL field by "1";
- Forwards the packet based on the label.

The Egress LSR (output router) is the definitive router for an LSP. It gets packets from the penultimate node and compares the IPv4 address with its routing table. Then redirects the packet to the next hop. Each LSP must have egress router and only one router can be egress for a given LSP [20].

Redirection of packets in MPLS backbone network depends on the labels that are set by the LSRs. The designation of the MPLS labels is done manually or automatically. Nodes exchange data about the compliance between the labels for the set up LSPs. An MPLS label is a short fixed length physically set up identifier (see figure 2).

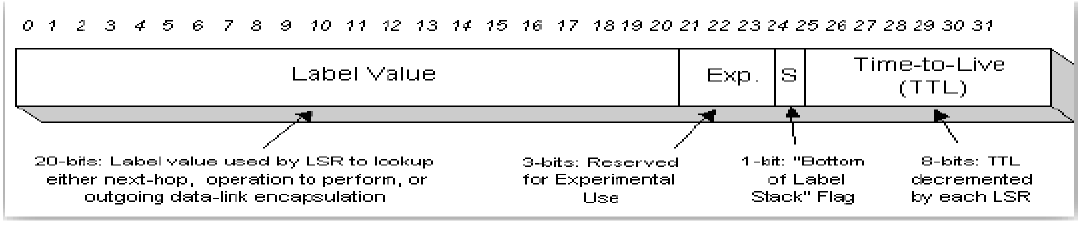

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Label Value
Exp.
S
Time-to-Live (TTL)
20-bits: Label value used by LSR to lookup either next-hop, operation to perform, or outgoing data-link encapsulation
3-bits: Reserved for Experimental Use
1-bit: "Bottom of Label Stack" Flag
8-bits: TTL decremented by each LSR

Figure 2 - *MPLS label format [20]*

2.3 Virtual Private Network

A Virtual Private Network (VPN) is a technology that helps to create a private network across a public network (e.g., the Internet), collection of virtual links which logically interconnect the different network components over a physical network and also is a network in which information is transmitted using cryptographic and authentication algorithms. It is virtual since there is no real physical connection between the sites. A VPN uses shared public telecom infrastructure, such as the Internet, to provide secure access to remote offices and users in a cheaper way than an owned or leased line. The virtual private network is mainly used to establish connections between different corporate branches or remote activities when using less secure network lines. With the help of data encryption, a network inside the Internet, for example, can only be accessed by those who have the necessary addresses and passwords.

One of the most capability of MPLS is to possibility to build Virtual Private Networks (VPNs). MPLS has the capability to construct both Layer 2 and Layer 3 MPLS VPNs. Both types of VPNs have their own merits and demerits. VPNs became popular during past two decades because of the evolution of related technologies. Primarily, the implementation cost of virtual networks had dropped drastically as a result of the availability of low-cost network equipment and communication systems [2, 9].

2.3.1 MPLS Layer 2 VPNs

In this approach, the customer network and the service provider network are separated and no exchange of paths between the CE and PE routers is done. The division between the client and the service provider simplifies the implementation of the VPN. MPLS L2VPNs offer services to transport the layer-2 frames from one client site to another. This approach is completely transparent to the CE devices. Working with layer-2 frames allows the ISP to provide services that are independent from layer-3 protocols. Layer 2 VPNs requires not router equipment, and traffic is tagged with a MAC address instead of an IP address. Since it works at a lower layer, the latency is lower compared to a layer 3 based solution. Also, it is easy to deploy since it does not require any specific configuration, like a device in a LAN [12].

As a layer 2 protocol it also has some disadvantages. Layer 2 networks are susceptible to broadcast storms. Services are difficult to monitor since the service provider has no visibility [23].

2.3.2 MPLS Layer 3 VPN

A MPLS Layer 3 VPN contains a provider router, a provider edge router and a CE router. At each customer site, one or more CE routers connect to one or more PE routers. A client network is a combination of VPN sites at various geographical areas. Each VPN Site is associated with carrier networks through the CE router, and CE gets to PE by means of single or double connections and interconnects VPN sites at various areas by means of carrier networks.

MPLS L3VPN can allocate different sites of a client to various VPNs to allocate one office to a few VPNs or isolate services for VPN shared to get to. Also, routing information from one customer is completely separated from other customers and tunnelled over the service provider MPLS network. MPLS L3VPN has strong client isolation flexibility to meet the prerequisites of various clients in flexible networking and service security. In the Layer 3, the service provider will be involved in routing with the customer. The customer will run appropriate IGP protocols, such as BGP, OSPF, EIGRP or any different routing protocol with the service provider [16].

Routing scenarios can sometimes be complex, however, an any-to-any topology where any customer device can connect directly to the L3 MPLS VPN it is the most common case. Data is encapsulated with MPLS labels to ensure proper tunnelling and de-multiplexing via the core and enterprise traffic [2].

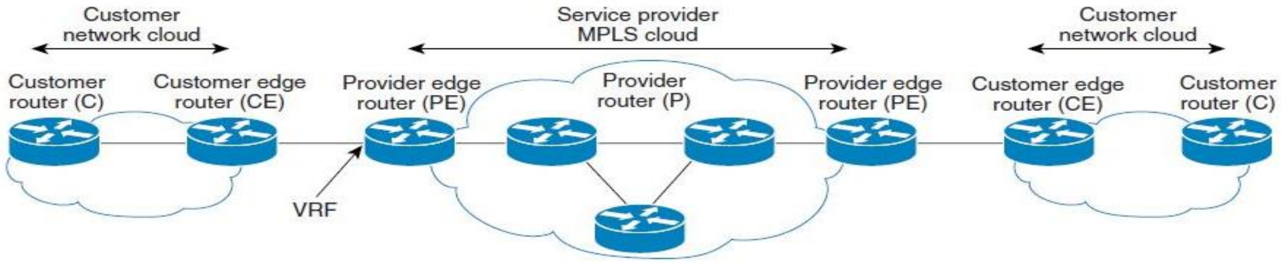

Customer network cloud
Service provider MPLS cloud
Customer network cloud
Customer router (C)
Customer edge router (CE)
Provider edge router (PE)
Provider router (P)
Provider edge router (PE)
Customer edge router (CE)
Customer router (C)
VRF

***Figure 3** - MPLS Layer 3 VPN Component Terminology [2]*

MPLS Layer 3 VPN builds a peer-to-peer VPN with customer sites (See Figure 3). It forms Layer 3 relations with service provider routers. Labels are added to customer IP routes when they enter from Customer Edge (CE) routers to Provider Edge (PE) routers. All forwarding is finished utilizing label switching with MPLS within service provider network and labels are removed when sending traffic from Provider Edge to Customer Edge routers.

MPLS L3VPN utilizes GRE/IP tunnel and MPLS tunnel. A tunnel isolates a client route from a provider router. Provider router is just related to a public network route rather and not to a client router. Tunnel management is complex for GRE with a weak protocol support. An IP network not supporting MPLS can transport VPN service through a GRE/IP tunnel to avoid the upgrade to put a cost pressure on the whole network.

The purpose of a tunnel is sending information over a network from one node to another, as though the two nodes were directly associated. This is accomplished by encapsulating the information – an additional header is added to information sent by the transmitting end of the tunnel, and the information is sent by intermediate nodes based on this external header without looking at the contents of the original packet.

This is illustrated in Figure 4, which shows information going from A to B being sent via a tunnel between X and Z. The halfway tunnel node, node Y, does not should know about the final destination B, but just forwards the data along the tunnel to Z. (In this scenario, X is known as the approaching to the tunnel and Z as the egress) [2].

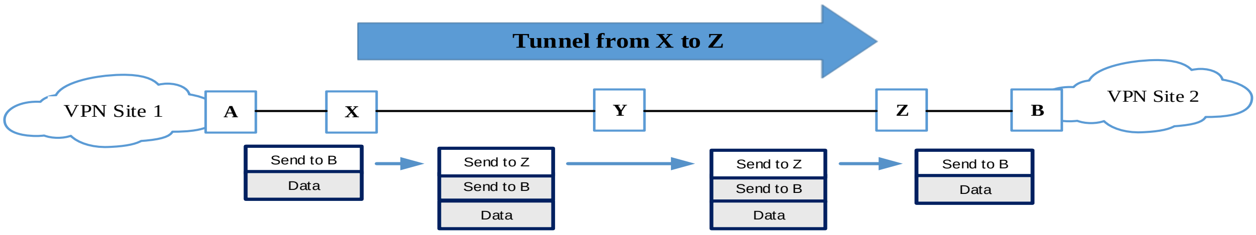


Figure 4 - Tunnel from X to Z

To build up these tunnels there are several of protocols that may be utilised, and the properties of the tunnel have an essential result on the general properties of the VPN utilising that tunnel [16].

MPLS Layer3 VPN has some advantages over Layer 2 and others, including address overlay, standard protocols to allocate labels and routes, scalable bandwidth and routing, reduced cost, intelligent QoS, any-to-any connectivity, support for a diversity of topologies (-mesh, P2P, Hub-Spoke, VPN overlay and HoVPN) and high reliability.

2.7 Criteria for Assessing the Suitability of VPN Solutions

There are many various VPN technologies to choose from, and network operators need to put together a list of their necessities and choice a solution that meets these necessities. For a VPN user, such a list will typically include the following criteria.

- **VPN Service:** The VPN service must match a specific sort of service demanded by the VPN user. Different VPN solutions supply either layer 2 or layer 3 connectivity between VPN sites.
- **Quality of Service Considerations:** For the connections between VPN sites, the VPN user may demand a certain quality of service (QoS). If this is the case, the service provider backbone must support the provisioning of QoS-constrained tunnels;
- **Security:** If significant or sensitive information is to be sent throughout the backbone between VPN sites, then the solution should support encryption, integrity checking of information in the VPN tunnels and authentication;
- **Capital Cost (to the VPN user):** The VPN user may demand a solution which does not involve a costly replacement of their existing equipment. The solution should be fully possible with the VPN user's existing switches and routers [12];
- **Manageability:** The VPN user will need a simple solution to minimizes and also manage the migration costs. Neither should the solution demand a significant overhaul of the VPN user's existing network architecture. In equal, the ongoing day-to-day management should not be too onerous – for instance, it should be easy to add new sites to the VPN [12].

CHAPTER THREE

3.1 Network Design and Modelling

In this chapter, I describe an Internet Service Provider (ISP) using MPLS VPNs. MPLS supplies good performance with its label switching method. When MPLS is used, the VPN feature allows several sites to interconnect transparently via a service provider's network. One service provider network can support several different IP VPNs. Each of these appears to its users as a private network, separate from all other networks. Within a VPN, each site can send IP packets to any other site in the same VPN.

Each VPN is associated with one or more VPN routing and forwarding instances (VRFs). A VRF consists of an IP routing table, a derived Cisco express forwarding (CEF) table, and a set of interfaces that use this forwarding table. The router maintains a separate routing and CEF table for each VRF. This prevents information being sent outside the VPN and allows the same subnet to be used in several VPNs without causing duplicate IP address problems.

To implement and design my network topology, I used three different protocols such as BGP, OSPF and RIP and also to implement and design the topology, I used the GNS3 platform. The reason this simulation was chosen, it provides the opportunity to study, modify and create the behaviour of proposed design so that you can predict its strengths and weakness before implementing the model in a real environment. The GNS3 platform can simulate the functions of a real Cisco Router since it is able to load an actual IOS. The selected router model is the 7200, with this IOS we can implement almost any technology available. Nevertheless, we could choose a newer Router model with more features.

3.2 Protocols of the Proposed Networks

There are many different ways to transmit data in networks, in this scenario I am going to design and implement a sample configuration base of a MPLS Layer 2 (for one customer) and Layer 3 (for two customers) VPN with three different protocols for each customer, namely Border Gateway Protocol (BGP), Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). The idea behind it to compare and analyse them together and see how they compare in terms of performance and configurability.

3.2.1 Open Shortest Path First (OSPF)

Open Shortest Path First routing protocol, always seeks the fastest route to reach its destination. Routers that are on an OSPF network will always check the status of other routers that they have access to and send messages to each other whenever necessary. Using this mechanism, routers will understand the status of other routers in the network and understand whether a router is online. One of the features that OSPF offers to us is that routers, in addition to finding the fastest and closest route to reach the destination, also notice all possible routes and routes for passing the packet from origin to destination. In such a case, there is the ability to implement Load Balancing on the routers so that information packets can be divided into different parts and shipped to different destinations on different routes. OSPF is commonly used in medium to medium sized networks and is commonly used in large networks for less frequent protocols.

3.2.2 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is used in large networks. For example, Internet uses the BGP routing protocol. BGP can also be used for internal networks. BGP can also be used in an internal network, as a single autonomous system. The main differences between OSPF and BGP routing protocols are as follows:

- BGP works on very large networks with more than one Autonomous System, while OSPF is an intermediate protocol;
- BGP is used on the Internet, but OSPF is on the internal network;
- BGP has more complexity than OSPF.

3.2.3 The Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) protocol is one of the oldest distance vector routing protocols that uses the hop count parameter as a metric. The RIP protocol exchanges information with its closest neighbours, which is a set of known purposes for participating routers.

3.3 Simulation Tools

The simulation program which will be used to implement the scenario is the Graphical Network Simulator 3 (GNS3). GNS3 platform is a graphical network simulator that allows designing complex network topologies and also process of testing a designed model on a platform which imitates the real environment, it can also be used to experiment features of Cisco IOS or to check configurations that need to be deployed later on real routers.

3.4 Network topology

In the Provider's core (see Figure 5), there are three P (Provider) routers and two PE (Provider Edge) routers. The IGP protocol is used in order to advertise their subnets to the Routers of the Core network between them (such as directly connected networks and Loopback IP addresses) is the OSPF (Open Shortest Path First). Next the MPLS protocol was activated in all the Core Routers of the network, where each router using the LDP [1] protocol exchanges labels corresponding to each subnet.

The topology in Figure 5 shows a basic configuration of Layer3 and Layer2 VPN functions. It is an ISP with three customers connected to a service provider network, Customer1, Customer2 and Customer3 each has two sites, using the same IP ranges. Meanwhile, "CUST1-R1" and "CUST1-R3" are in one VPN and the other "CUST2-R2" and "CUST2-R4" are in the other VPN for Layer3 and also "CUST3-R5" and "CUST3-R6" are in the other VPN for Layer2. After proper configuration, "CUST1-R1" and "CUST1-R3", "CUST2-R2" and "CUST2-R4", "CUST3-R5", and "CUST3-R6" can learn routes from each other and also everything from these customers is completely separated by the service provider.

[1] Label Distribution Protocol (LDP)

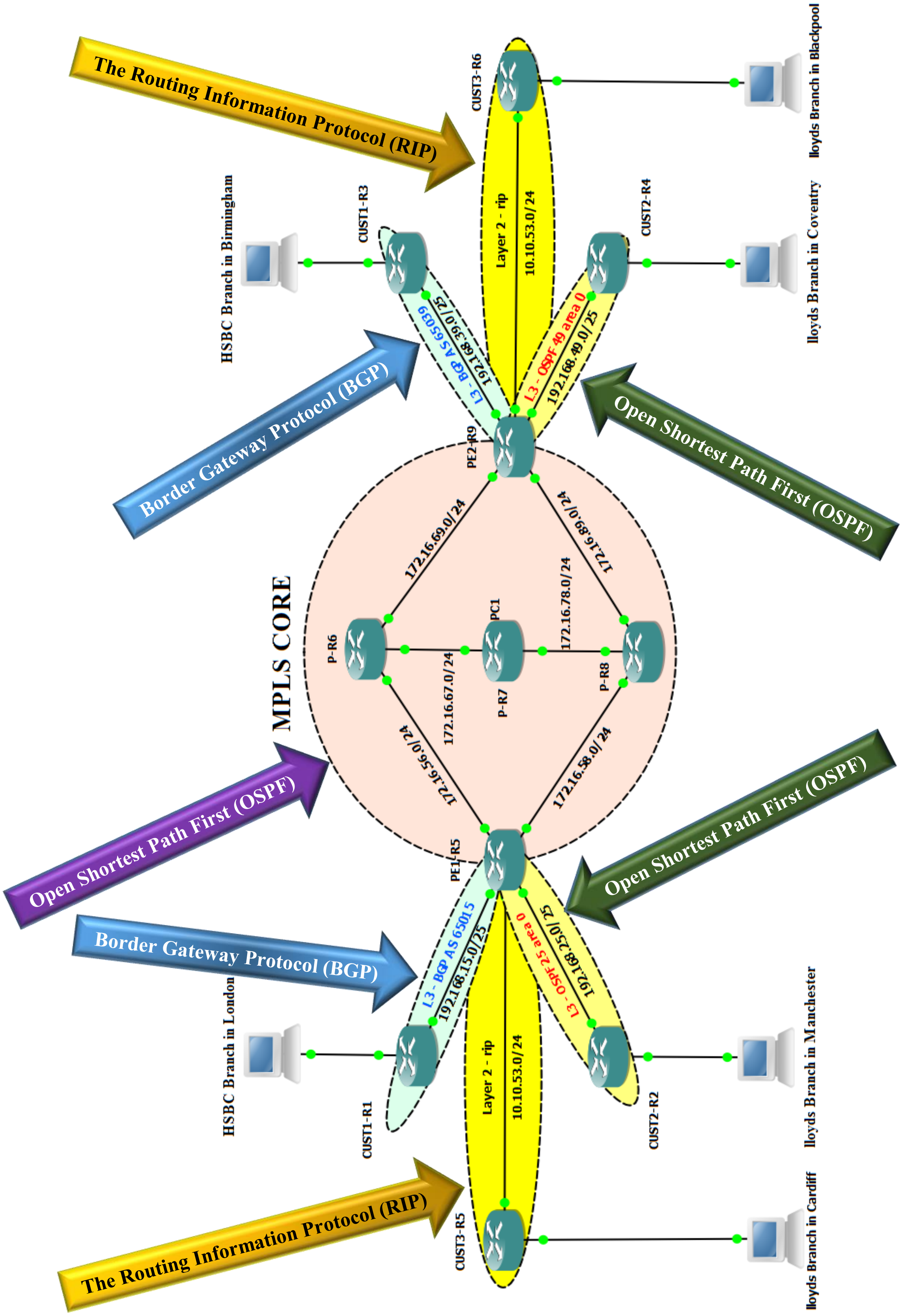


Figure 5 *- MPLS Layer 3 and 2 VPN Topology*

To accomplish my goal, the ISP is running MP-BGP protocol at the top sites topology between PE1-R5 to CE1-R1 and PE2-R9 to CE1-R3 routers and OSPF protocol between the bottom sites topology between PE1-R5 to CE2R2 and PE2-R9 to CE2-R4 routers for Layer3 and also RIP protocol at the middle sites topology between PE1-R5 to CE3-R5 and PE2-R9 to CE3-R6 routers for layer2 to exchange prefixes. This means all internal (P) routers of the ISP have to run OSPF protocol and they don't know where to forward their packets to.

To resume the elements and protocols of the topology:

- P (provider) routers (P-R6, P-R7 and P-R8) are ISP core routers which don't connect to Customer routers and generally run just MPLS and OSPF.
- PE (provider edge) routers (PE-R5 and PE-R9) connect to customer sites and form the edge of a VPN.
- CE (customer edge) routers (CE–R1, CE–R3, CE –R2, CE-R4, CE–R5 and CE-R6) exist at the edge of a customer site; they have no VPN awareness
- An IGP running between all P and PE routers is used to support LDP, OSPF and BGP adjacencies within the provider network.
- MP-BGP, OSPF and RIP are run between PE and CE routers and its upstream PE router
- An IGP (typically) is run between.

In this scenario, OSPF is already in operation as the provider network IGP. OSPF processes have also been preconfigured on the CE (R2 and R4) routers; however, these OSPF topologies will remain separate from the provider OSPF.

There are five principal tasks to achieve an MPLS VPN up and running:

1. Enable MPLS on the provider backbone.
2. Create VRFs and assign routed interfaces to them.
3. Configure OSPF between the PE routers.
4. Configure OSPF (CUST2-R2 to CUST2-R4) and MP-BGP (CUST1-R1 to CUST1-R3) between each PE router and its attached CE routers for Layer3.
5. Configure RIP (CUST3-R5 to CUST3-R6) between each PE router and its attached CE routers for Layer2.
6. Enable route redistribution between the customer sites and the backbone.

3.4.1 Generic Routing Encapsulation (GRE) Tunnels

In the proposed scenario, I added three GRE tunnels (see Figure 6):

- The two **PE** routers at the top will use a **GRE** tunnel for the customer 1 (CUST-A) sites (Layer3).
- The two **PE** routers at the bottom will use a **GRE** tunnel for the customer 2 (CUST-B) sites (Layer3).
- The two **PE** routers at the middle will use a **GRE** tunnel for the customer 3 sites (Layer2).

With a solution like this, we can have a **BGP** at the top, **RIP** in the middle and **OSPF** at the bottom.

There's two places where we need **BGP** (Layer3):

- eBGP between the **PE**, **CE1-R1** and **CE1-R3** routers.
- iBGP between two PE routers.

And also there's two places where we need **OSPF** (Layer3):

- OSPF between the **PE**, **CE2-R2** and **CE2-R4** routers.
- OSPF between two **PE** routers.

And also for "Layer2" there's two places where **RIP** need to be configured:

- OSPF between the **CE3-R5** and **CE3-R6** routers.
- VPN L2 between two **PE** routers.

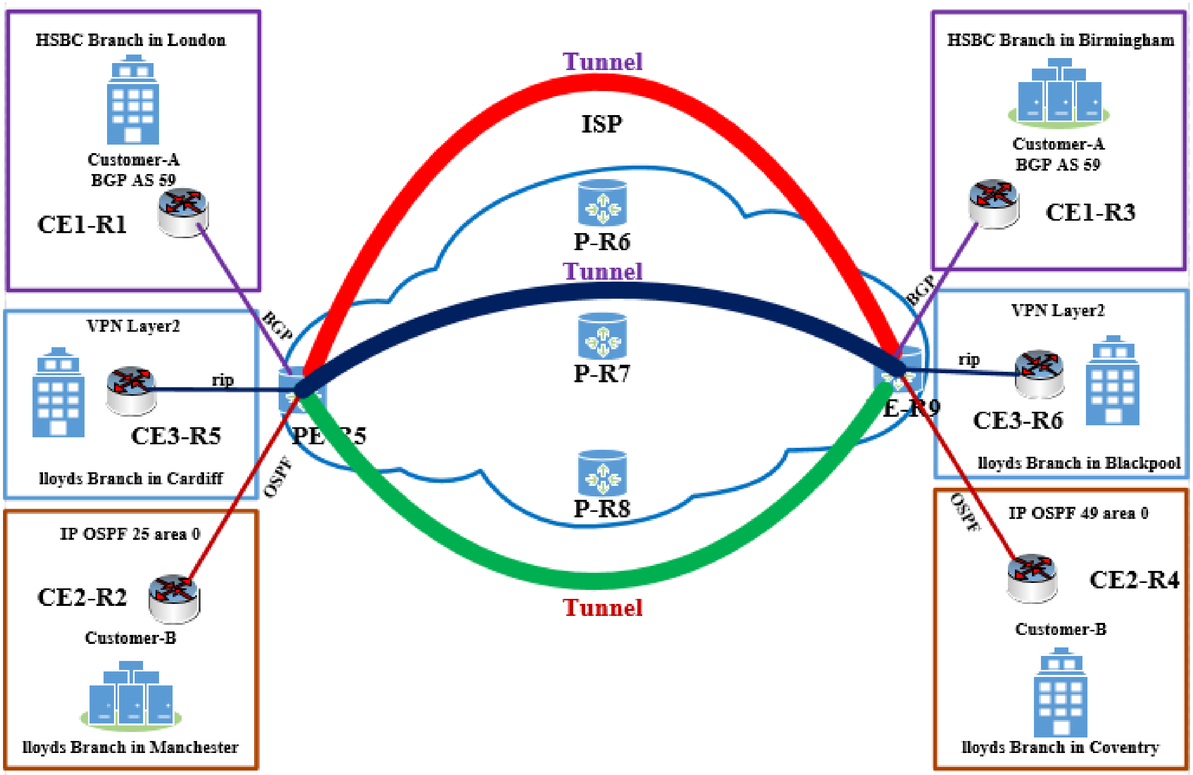


***Figure 6** - GRE tunnels*

3.4.2 IP addresses

IP addresses to be used for all Routers and PCs in this scenario is as the following and all of ports are configured by them.

IP addresses for each Router and PCs				
Device	**Port**	**IP Address**	**Loopback**	**Gateway**
P-R6	g1/0	172.16.56.6	6.6.6.6	-
	g2/0	172.16.67.6		-
	g5/0	172.16.69.6		-
P-R7	g2/0	172.16.67.7	7.7.7.7	-
	g3/0	172.16.78.7		-
P-R8	g4/0	172.16.58.8	8.8.8.8	-
	g3/0	172.16.78.8		-
	g6/0	172.16.89.8		-
PE-R5	g1/0	172.16.56.5	5.5.5.5	-
	g4/0	172.16.58.5		-
	f0/0	192.168.15.5		-
	f0/1	192.168.25.5		-
	g2/0	L2		
PE-R9	g5/0	172.16.69.9	9.9.9.9	-
	g6/0	172.16.89.9		-
	f0/0	192.168.39.9		-
	f0/1	192.168.49.9		-
	g1/0	L2		
CE1-R1	f1/0	192.168.35.2	1.1.1.1	-
	f0/0	192.168.15.1		-
CE1-R2	f0/1	192.168.25.2	2..2.2.2	-
	f0/0	192.168.35.3		-
CE2-R3	f1/0	192.168.29.4	3.3.3.3	-
	f0/0	192.168.39.3		-
CE2-R4	f0/1	192.168.49.4	4.4.4.4	-
	f0/0	192.168.59.4		-
CE3-R5	g1/0	10.53.12.1	10.10.52.11.1	-
	f0/0	10.53.13.1		
CE3-R6	g1/0	10.53.12.2	10.10.53.22.2	-
	f0/0	10.53.10.1		
PC1	-	192.168.35.11	-	192.168.35.2
PC2	-	192.168.35.22	-	192.168.35.3
PC3	-	192.168.29.33	-	192.168.29.4
PC4	-	192.168.59.44	-	192.168.59.4
PC5	-	10.53.13.2	-	10.53.13.2
PC6	-	10.53.10.2	-	10.53.10.1

Table 1 - *IP addressing scheme of the designed network architectures*

3.5 VPN Layer3 implement and Configuration in the ISP Core

In this stage, I will start to implement and configure all the Provider routers in the Core. The task of the core routers is to transport packets as quickly as possible. All the routers in the Core have no knowledge of the client edge network. After finishing the configuration all providers in the core should know how to communicate to the edge routers.

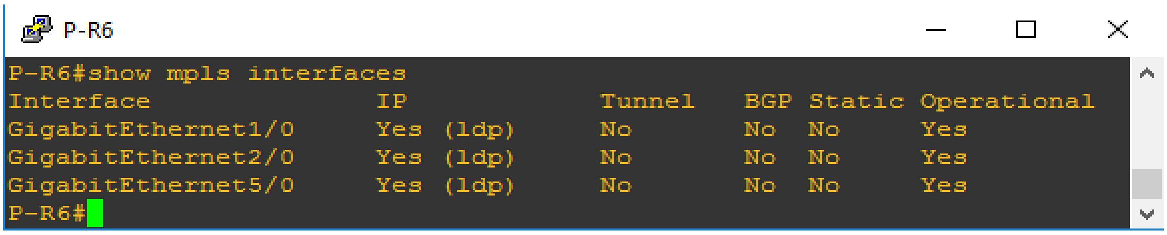
3.5.1 MPLS configuration of the Core ISP (Provider ➔ R6, R7 and R8)

The first prerequisite that needs to be configured in all routers in the core and also all the PE routers that must be able to support CEF and MPLS forwarding. MPLS will not work if CEF is not enable.

After enable MPLS on all Provider and PE with the ***mpls ip*** command. As CE routers do not run MPLS, consequently MPLS is not enabled on any CE-facing interfaces, only plain IP routing. LDP is enabled automatically as the default label distribution protocol. Generally, LDP runs between loopback addresses not directly reachable by LDP peers.

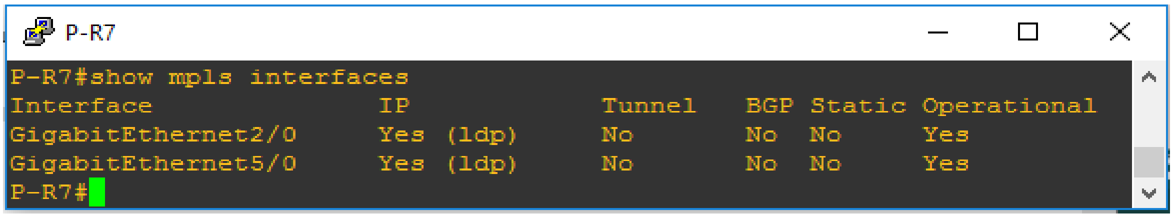
In the additional configuration, all interfaces facing to the Core (Provider) network are in OSPF area 0 and interfaces connected to the edge routers are in OSPF area 1. Also we have forcefully configured P6, P7 and P8 to utilize IP address of Loopback0 as mpls ldp router-id i.e. router ID of mpls ldp process will change immediately after executing the command, without waiting to restart the device.

To verify the configuration of MPLS interfaces with "***show mpls interfaces***".



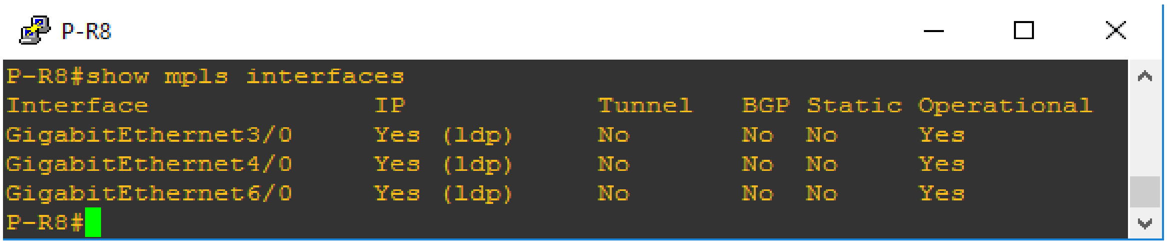
```
P-R6#show mpls interfaces
Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet1/0     Yes (ldp)     No       No  No     Yes
GigabitEthernet2/0     Yes (ldp)     No       No  No     Yes
GigabitEthernet5/0     Yes (ldp)     No       No  No     Yes
P-R6#
```

Figure 7 *- Show mpls interfaces*



```
P-R7#show mpls interfaces
Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet2/0     Yes (ldp)     No       No  No     Yes
GigabitEthernet5/0     Yes (ldp)     No       No  No     Yes
P-R7#
```

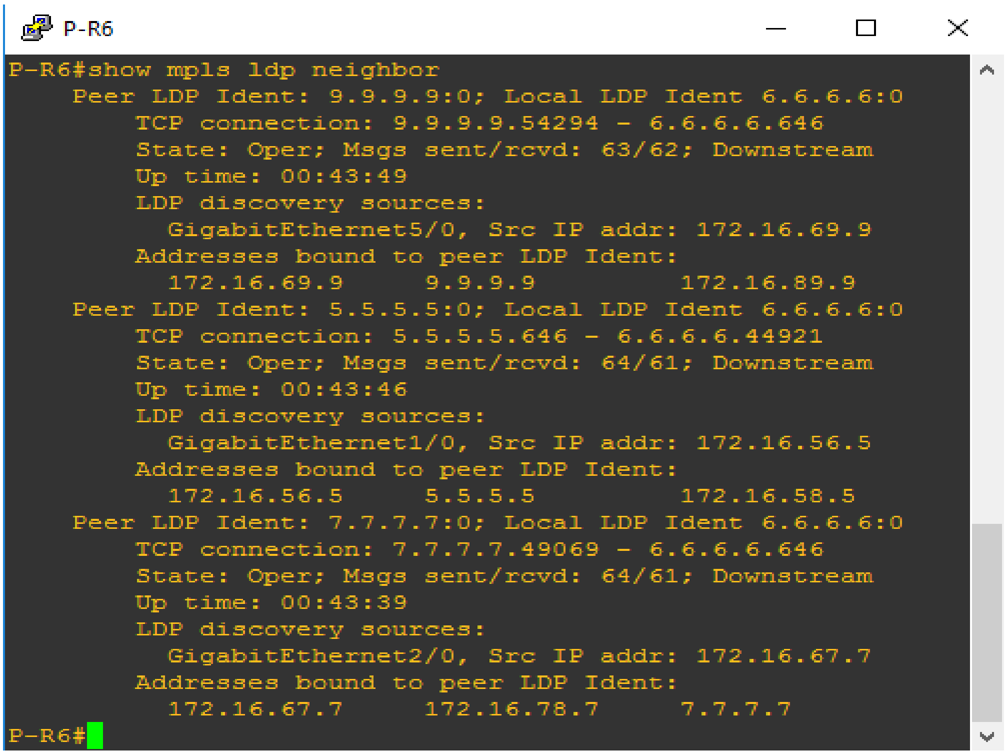
Figure 8 *- Show mpls interfaces*



```
P-R8#show mpls interfaces
Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet3/0     Yes (ldp)     No       No  No     Yes
GigabitEthernet4/0     Yes (ldp)     No       No  No     Yes
GigabitEthernet6/0     Yes (ldp)     No       No  No     Yes
P-R8#
```

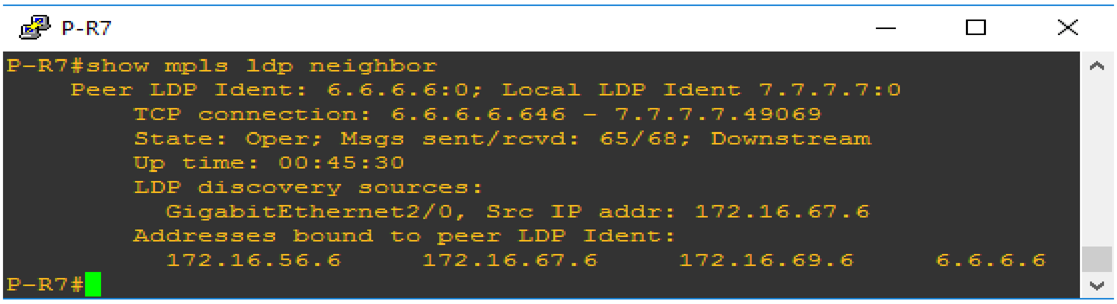
Figure 9 *- Show mpls interfaces*

LDP adjacencies can be verified with the command ***show mpls ldp neighbor***:



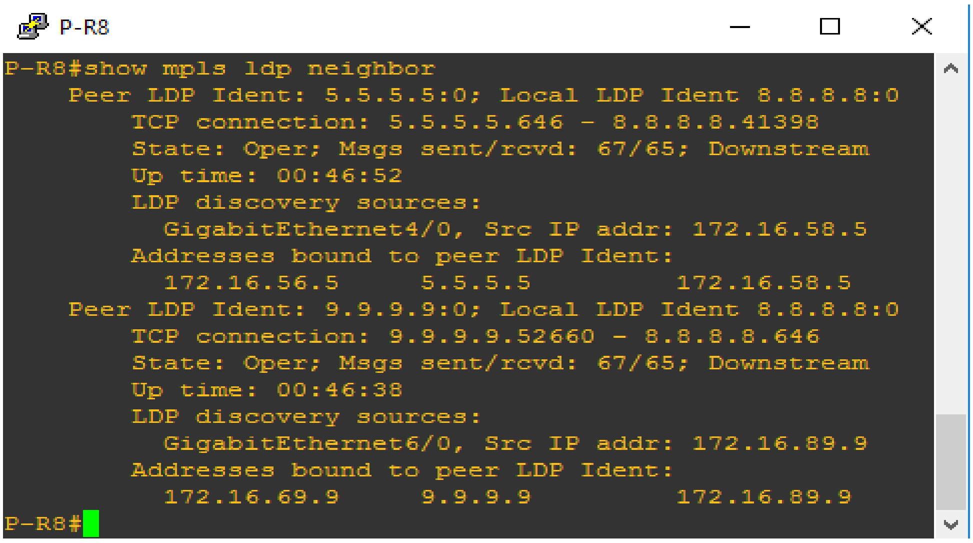
```
P-R6#show mpls ldp neighbor
    Peer LDP Ident: 9.9.9.9:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 9.9.9.9.54294 - 6.6.6.6.646
        State: Oper; Msgs sent/rcvd: 63/62; Downstream
        Up time: 00:43:49
        LDP discovery sources:
          GigabitEthernet5/0, Src IP addr: 172.16.69.9
        Addresses bound to peer LDP Ident:
          172.16.69.9     9.9.9.9         172.16.89.9
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 5.5.5.5.646 - 6.6.6.6.44921
        State: Oper; Msgs sent/rcvd: 64/61; Downstream
        Up time: 00:43:46
        LDP discovery sources:
          GigabitEthernet1/0, Src IP addr: 172.16.56.5
        Addresses bound to peer LDP Ident:
          172.16.56.5     5.5.5.5         172.16.58.5
    Peer LDP Ident: 7.7.7.7:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 7.7.7.7.49069 - 6.6.6.6.646
        State: Oper; Msgs sent/rcvd: 64/61; Downstream
        Up time: 00:43:39
        LDP discovery sources:
          GigabitEthernet2/0, Src IP addr: 172.16.67.7
        Addresses bound to peer LDP Ident:
          172.16.67.7     172.16.78.7     7.7.7.7
P-R6#
```

Figure 10 *- Show mpls ldp neighbor*



```
P-R7#show mpls ldp neighbor
    Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 7.7.7.7:0
        TCP connection: 6.6.6.6.646 - 7.7.7.7.49069
        State: Oper; Msgs sent/rcvd: 65/68; Downstream
        Up time: 00:45:30
        LDP discovery sources:
          GigabitEthernet2/0, Src IP addr: 172.16.67.6
        Addresses bound to peer LDP Ident:
          172.16.56.6     172.16.67.6     172.16.69.6     6.6.6.6
P-R7#
```

Figure 11 *- Show mpls ldp neighbor*



```
P-R8#show mpls ldp neighbor
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 8.8.8.8:0
        TCP connection: 5.5.5.5.646 - 8.8.8.8.41398
        State: Oper; Msgs sent/rcvd: 67/65; Downstream
        Up time: 00:46:52
        LDP discovery sources:
          GigabitEthernet4/0, Src IP addr: 172.16.58.5
        Addresses bound to peer LDP Ident:
          172.16.56.5     5.5.5.5         172.16.58.5
    Peer LDP Ident: 9.9.9.9:0; Local LDP Ident 8.8.8.8:0
        TCP connection: 9.9.9.9.52660 - 8.8.8.8.646
        State: Oper; Msgs sent/rcvd: 67/65; Downstream
        Up time: 00:46:38
        LDP discovery sources:
          GigabitEthernet6/0, Src IP addr: 172.16.89.9
        Addresses bound to peer LDP Ident:
          172.16.69.9     9.9.9.9         172.16.89.9
P-R8#
```

Figure 12 *- Show mpls ldp neighbor*

3.5.2 Create and Assign VRFs on the PE routers (R5 and R9)

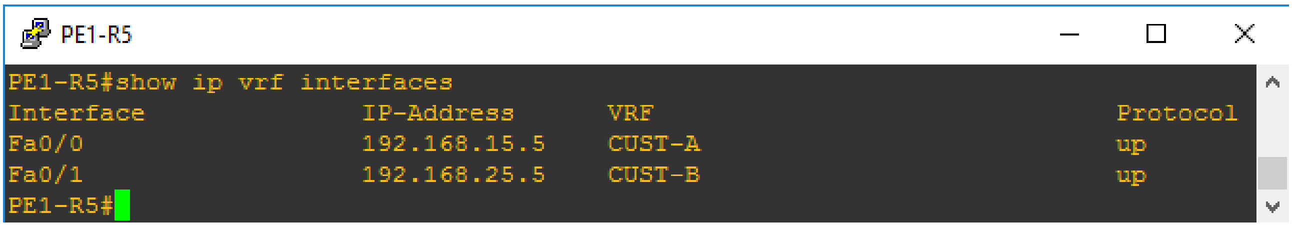
Next step is to establish customer VRFs on PE routers and assign the customer-facing interfaces to them. The requirements are to assign each VRF a route distinguisher (RD) to uniquely identify prefixes as belonging to that VRF and one or more route targets (RTs) to specify how routes should be imported to and exported from the VRF.

A route distinguisher was used for each VRF. For simplicity, I reuse similar value as both an import and export route target within each VRF. VRF configuration must be performed on both PE routers.

The command route-target both is used as a shortcut for the two commands route-target import and route-target export, which appear separately in the running configuration.

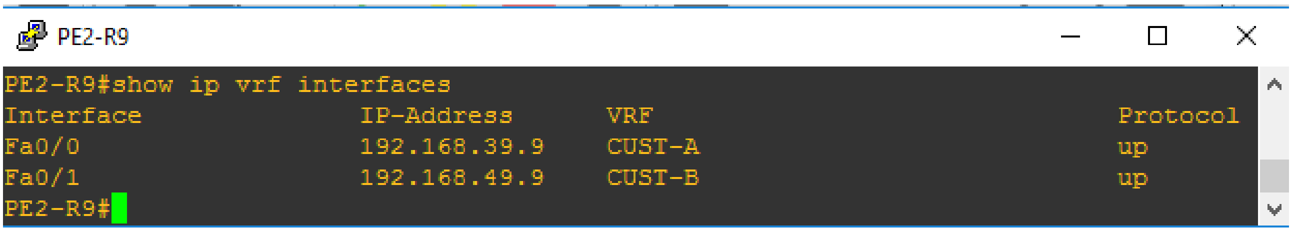
First I will create a VRF called CUST-A and CUST-B. The next step will be configuring a RD (Route Distinguisher). The route distinguisher is two 32-bit numbers which are colon-separated. The initial segment can be the autonomous system number of the client or a number in dotted decimal format. The route distinguisher is prepended to an advertised IP address to make it unique. Consequently, if another client associated with this edge router with a similar private network advertised through Loopback0, the router would have the capacity to separate the two networks. The **route-target** is the same structured number to the route distinguisher. Nevertheless, its utilization is various. The export number states the router what label to add to the prefix while exporting it from the VRF and into BGP. Also, the import number states the router which prefixes to get from BGP and import into the VRF. The other edge router would have the import and export numbers exchanged.

Next, we need to assign the appropriate interfaces to each VRF and reapply their IP addresses. (Assigning an interface to a VRF automatically wipes it of any configured IP addresses. The command "***show ip vrf interfaces***" can be used to verify interface VRF assignment and addressing.



```
PE1-R5#show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Fa0/0                  192.168.15.5    CUST-A                           up
Fa0/1                  192.168.25.5    CUST-B                           up
PE1-R5#
```

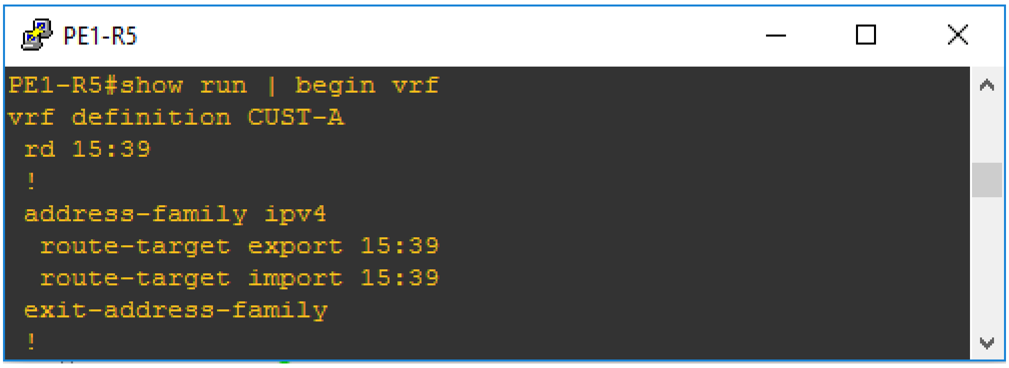
Figure 13 *- Show ip vrf interface.*



```
PE2-R9#show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Fa0/0                  192.168.39.9    CUST-A                           up
Fa0/1                  192.168.49.9    CUST-B                           up
PE2-R9#
```

Figure 14 *- Show ip vrf interface.*

The RD is to make sure that all prefixes are unique. The customer prefix + RD together are a VPNv4 route. The RD will be 15:39. The next item to configure is the RT (Route Target). This defines where we will import and export our VPNv4 routes.

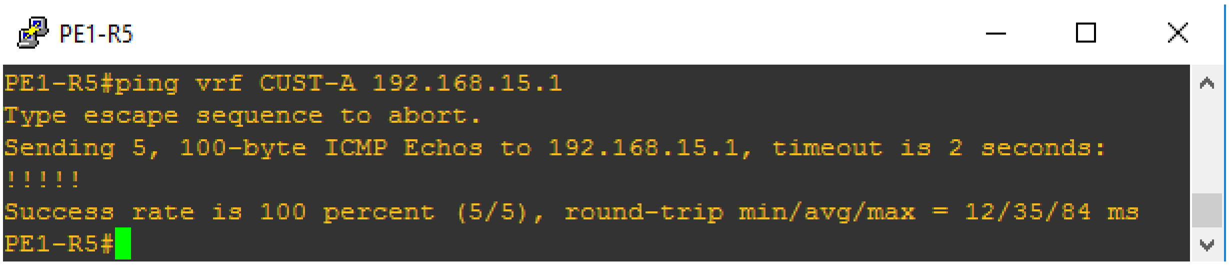


```
PE1-R5#show run | begin vrf
vrf definition CUST-A
 rd 15:39
 !
 address-family ipv4
  route-target export 15:39
  route-target import 15:39
 exit-address-family
 !
```

Figure 15 *- VPN Route Distribution.*

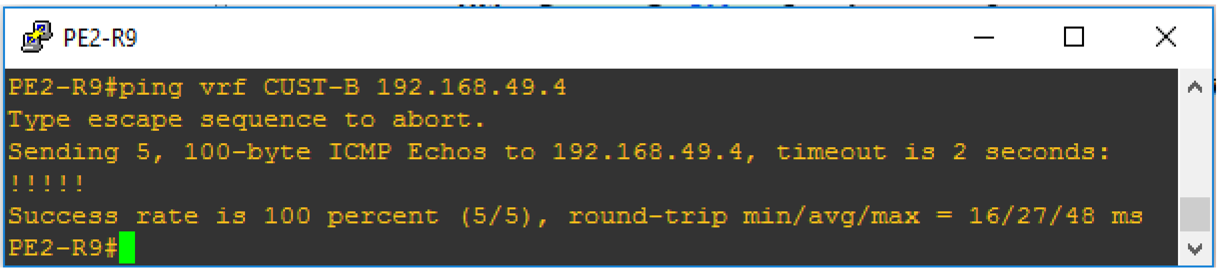
After creating the VRF globally, we have to assign the interface that is facing the customer to the VRF. The VRF configuration of PE1 is now complete. Now PE2 needs to be configured the exact same thing.

The VRFs are now configured.



```
PE1-R5#ping vrf CUST-A 192.168.15.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.15.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/35/84 ms
PE1-R5#
```

Figure 16 *- VRF configuration (CUST-A).*



```
PE2-R9#ping vrf CUST-B 192.168.49.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.49.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/48 ms
PE2-R9#
```

Figure 17 *- VRF configuration (CUST-B).*

3.5.3 Configuring the PE and CE Routers

3.5.3.1 Configuring Multiprotocol BGP on the PE to CE Routers and Route Reflectors

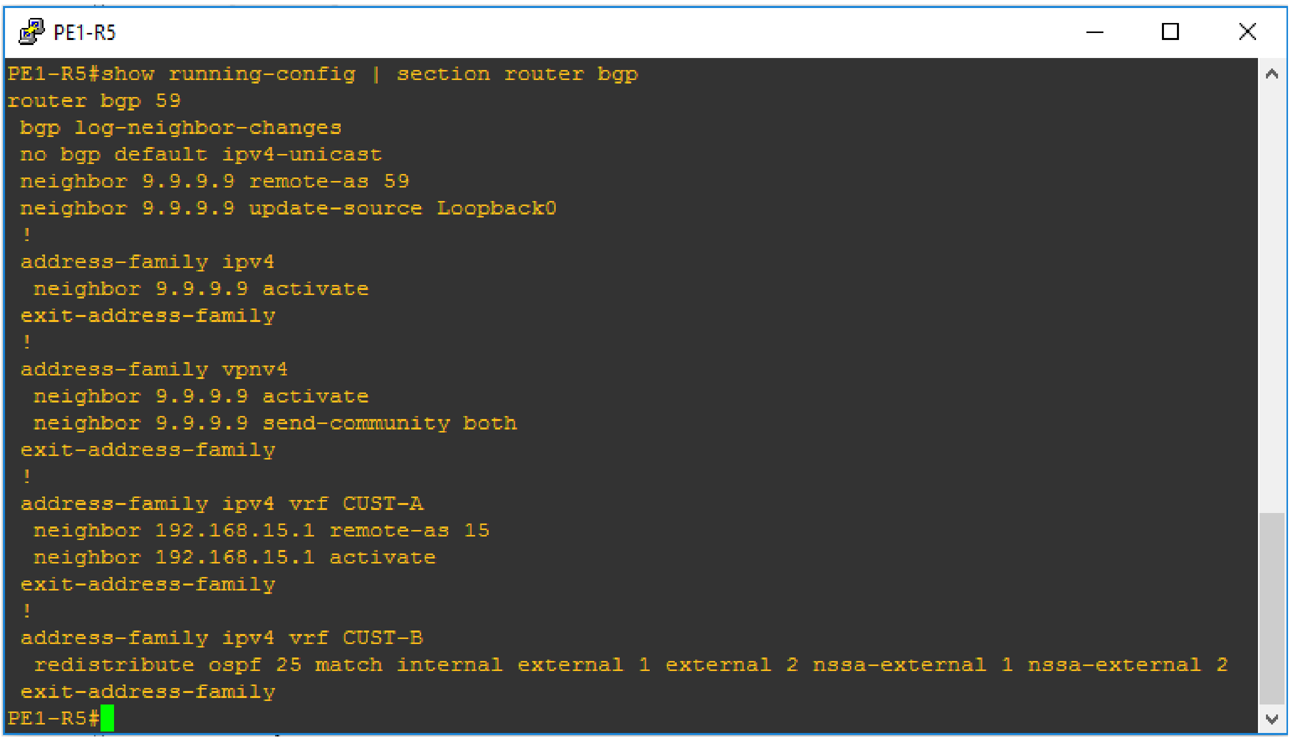
Perform this configuration of multiprotocol BGP (MP-BGP) connectivity on the PE routers and route reflectors.

- eBGP between PE1-R5 to CE1-R1 and PE2-R9 to CE1-R3 routers.

MP-BGP runs only on the PE routers: P routers rely entirely on the provider IGP and MPLS to forward traffic through the provider network, and CE routers have no knowledge of routes outside their own VRF. Both PE routers exist in BGP AS 59.

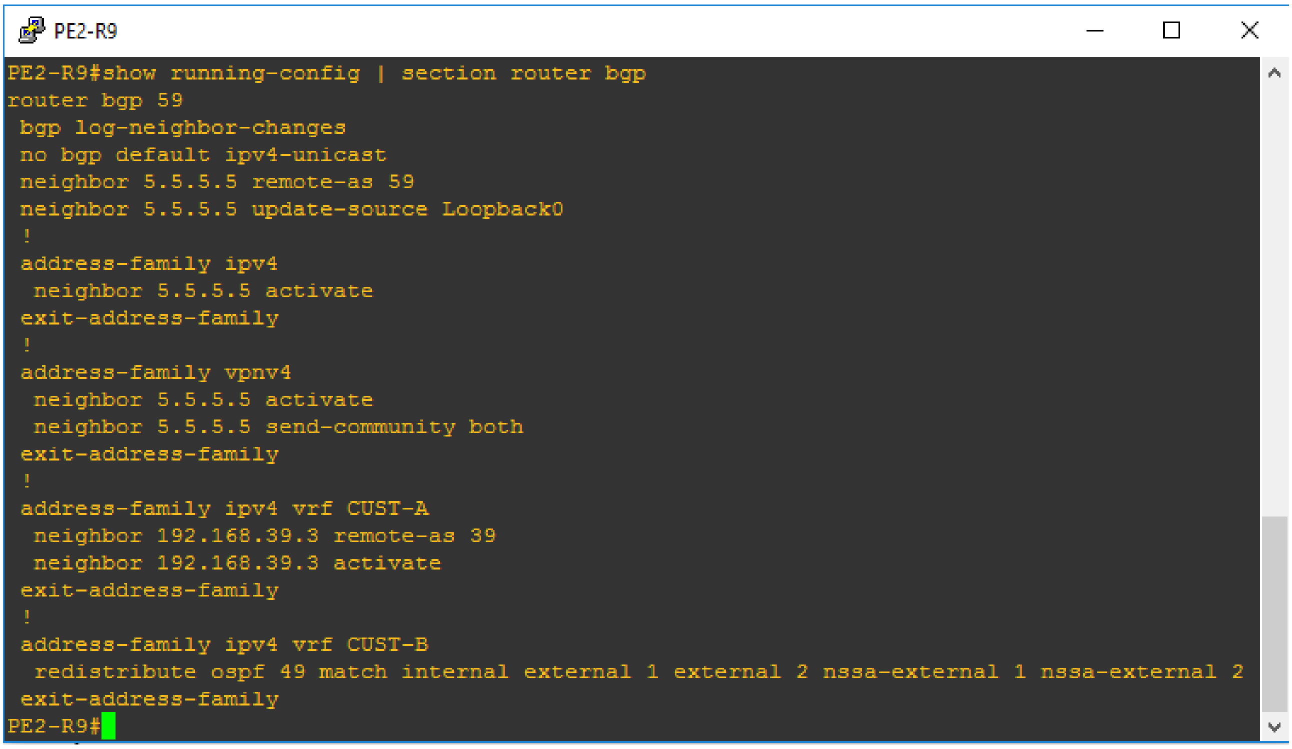
A very simple BGP configuration. This setup just advertises the networks belonging to all interfaces that are present up. This means the networks on PE and Loopback0 would be advertised by BGP.

BGP configuration can be verified with the command ***show running-config* | *section router bgp***:



```
PE1-R5#show running-config | section router bgp
router bgp 59
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 9.9.9.9 remote-as 59
 neighbor 9.9.9.9 update-source Loopback0
 !
 address-family ipv4
  neighbor 9.9.9.9 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 9.9.9.9 activate
  neighbor 9.9.9.9 send-community both
 exit-address-family
 !
 address-family ipv4 vrf CUST-A
  neighbor 192.168.15.1 remote-as 15
  neighbor 192.168.15.1 activate
 exit-address-family
 !
 address-family ipv4 vrf CUST-B
  redistribute ospf 25 match internal external 1 external 2 nssa-external 1 nssa-external 2
 exit-address-family
PE1-R5#
```

Figure 18 *– Show bgp configuration details*

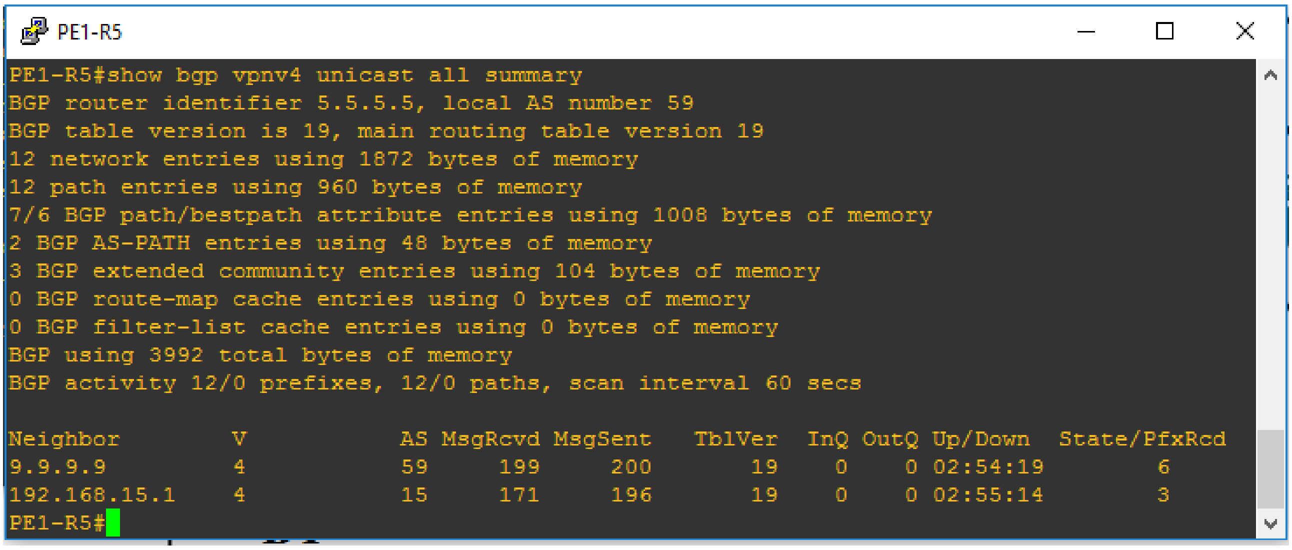


```
PE2-R9#show running-config | section router bgp
router bgp 59
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 5.5.5.5 remote-as 59
 neighbor 5.5.5.5 update-source Loopback0
 !
 address-family ipv4
  neighbor 5.5.5.5 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community both
 exit-address-family
 !
 address-family ipv4 vrf CUST-A
  neighbor 192.168.39.3 remote-as 39
  neighbor 192.168.39.3 activate
 exit-address-family
 !
 address-family ipv4 vrf CUST-B
  redistribute ospf 49 match internal external 1 external 2 nssa-external 1 nssa-external 2
 exit-address-family
PE2-R9#
```

Figure 19 *– Show bgp configuration details*

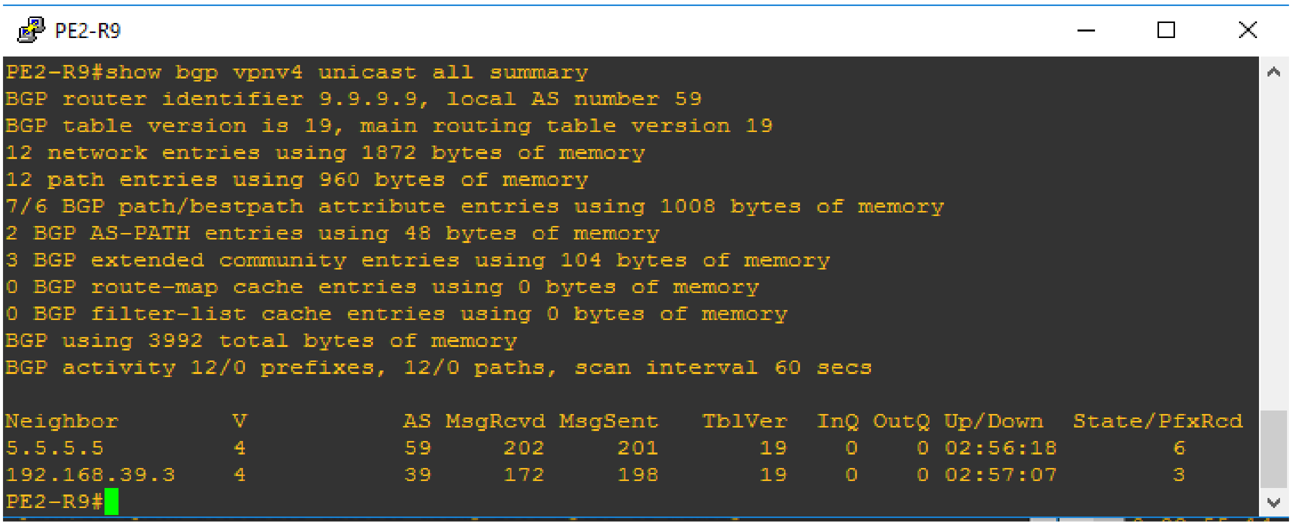
In addition to our VPNv4 address family, address families for the two customer VRFs have been created automatically. In addition, support for extended community strings has been added to the VPNv4 neighbor configuration.

Verify that the MP-BGP adjacency between PE1 and PE2 was formed successfully with the command ***show bgp vpnv4 unicast all summary***:



```
PE1-R5#show bgp vpnv4 unicast all summary
BGP router identifier 5.5.5.5, local AS number 59
BGP table version is 19, main routing table version 19
12 network entries using 1872 bytes of memory
12 path entries using 960 bytes of memory
7/6 BGP path/bestpath attribute entries using 1008 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
3 BGP extended community entries using 104 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 3992 total bytes of memory
BGP activity 12/0 prefixes, 12/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
9.9.9.9         4           59     199     200       19    0    0 02:54:19        6
192.168.15.1    4           15     171     196       19    0    0 02:55:14        3
PE1-R5#
```

Figure 20 *– Show bgp vpnv4 unicast all summary.*



```
PE2-R9#show bgp vpnv4 unicast all summary
BGP router identifier 9.9.9.9, local AS number 59
BGP table version is 19, main routing table version 19
12 network entries using 1872 bytes of memory
12 path entries using 960 bytes of memory
7/6 BGP path/bestpath attribute entries using 1008 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
3 BGP extended community entries using 104 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 3992 total bytes of memory
BGP activity 12/0 prefixes, 12/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
5.5.5.5         4           59     202     201       19    0    0 02:56:18        6
192.168.39.3    4           39     172     198       19    0    0 02:57:07        3
PE2-R9#
```

***Figure 21** – Show bgp vpnv4 unicast all summary.*

3.5.3.2 Configuring OSPF on the PE to CE Routers and Route Reflectors

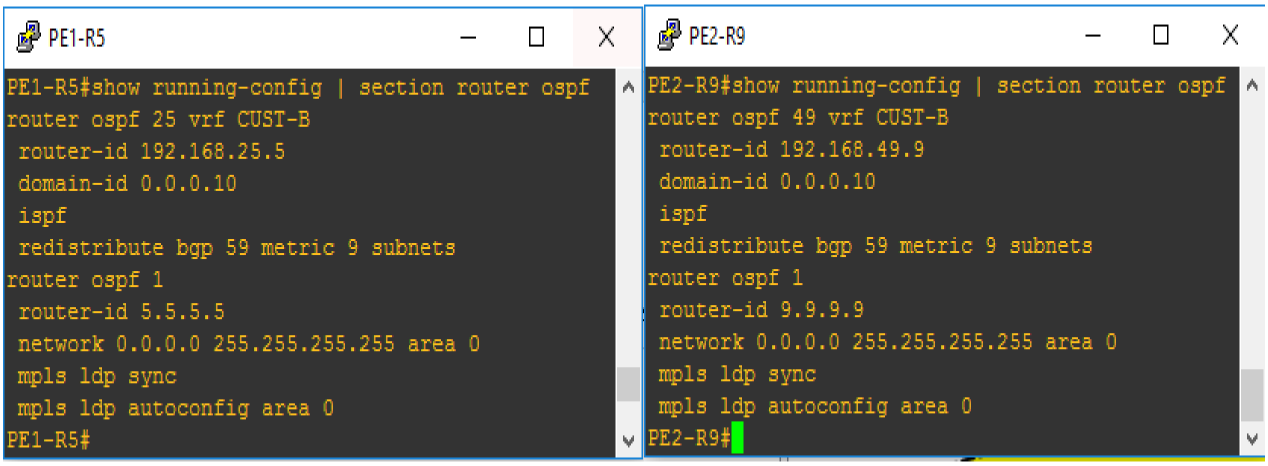
As the MP-BGP is configured at the top sites topology between **PE1-R5** to **CE1-R1** and **PE2-R9** to **CE1-R3** routers. Now, it needs to configure an IGP for the bottom sites topology between **PE-R5** to **CE2R2** and **PE2-R9** to **CE2-R4** routers to exchange routes with the customer sites, OSPF implement for this part. All CE interfaces are in area 0. OSPF processes are isolated from the provider OSPF topology.

Perform this configuration of OSPF connectivity on the PE routers and route reflectors.

- OSPF between **PE-R5** to **CE2R2** and **PE2-R9** to **CE2-R4** routers.

It should be seen each PE router form an OSPF adjacency with both of its attached CE routers, and the customer routes should appear in the VRF tables on the PE routers.

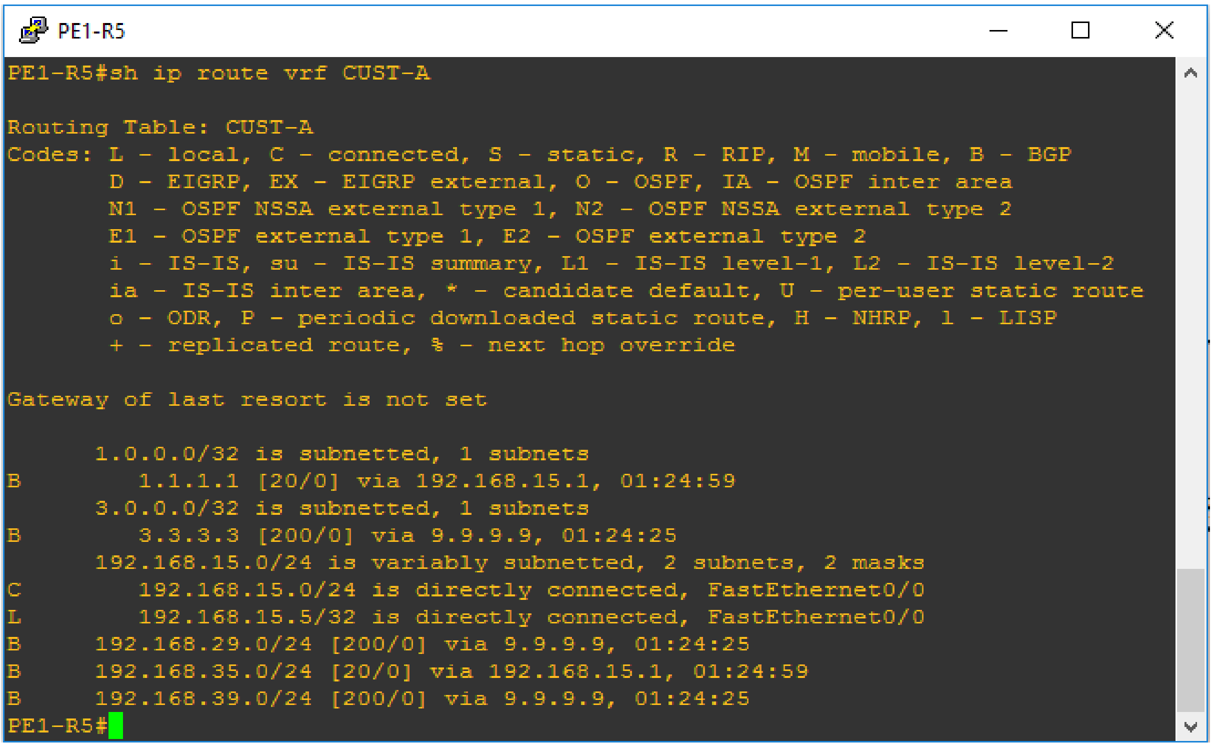
OSPF configuration can be verified with the command ***show running-config* | *section router ospf***:



```
PE1-R5#show running-config | section router ospf
router ospf 25 vrf CUST-B
 router-id 192.168.25.5
 domain-id 0.0.0.10
 ispf
 redistribute bgp 59 metric 9 subnets
router ospf 1
 router-id 5.5.5.5
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig area 0
PE1-R5#
```

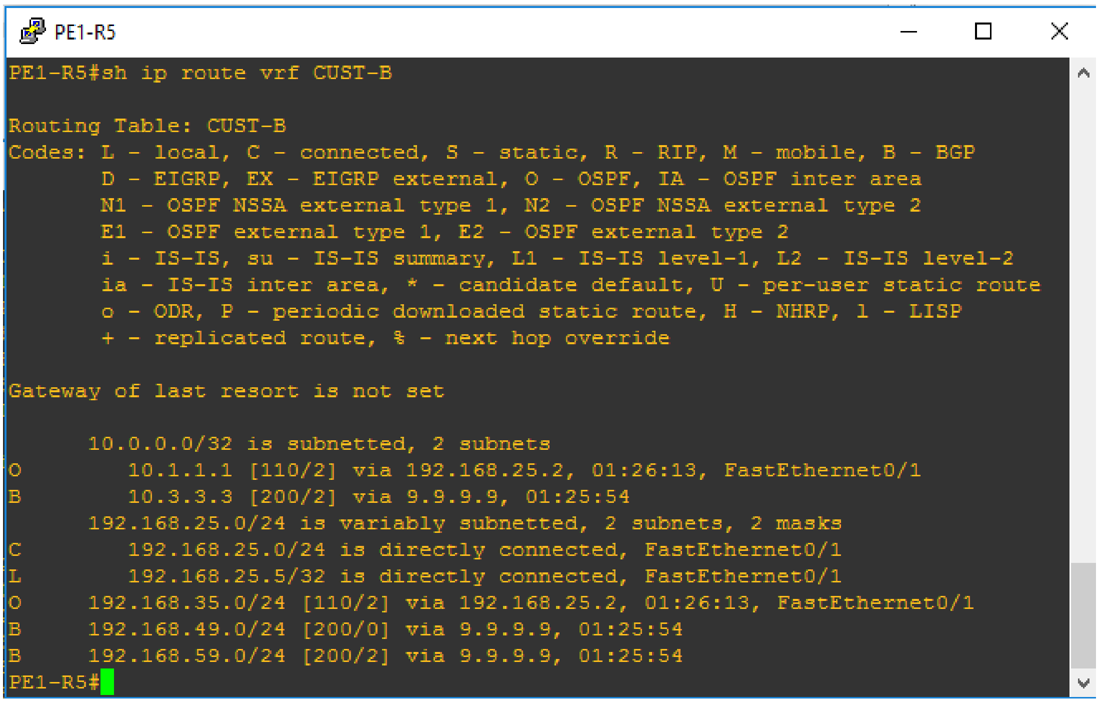
```
PE2-R9#show running-config | section router ospf
router ospf 49 vrf CUST-B
 router-id 192.168.49.9
 domain-id 0.0.0.10
 ispf
 redistribute bgp 59 metric 9 subnets
router ospf 1
 router-id 9.9.9.9
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig area 0
PE2-R9#
```

***Figure 22** – Show OSPF configuration details in PE1-R5 and PE2-R9.*



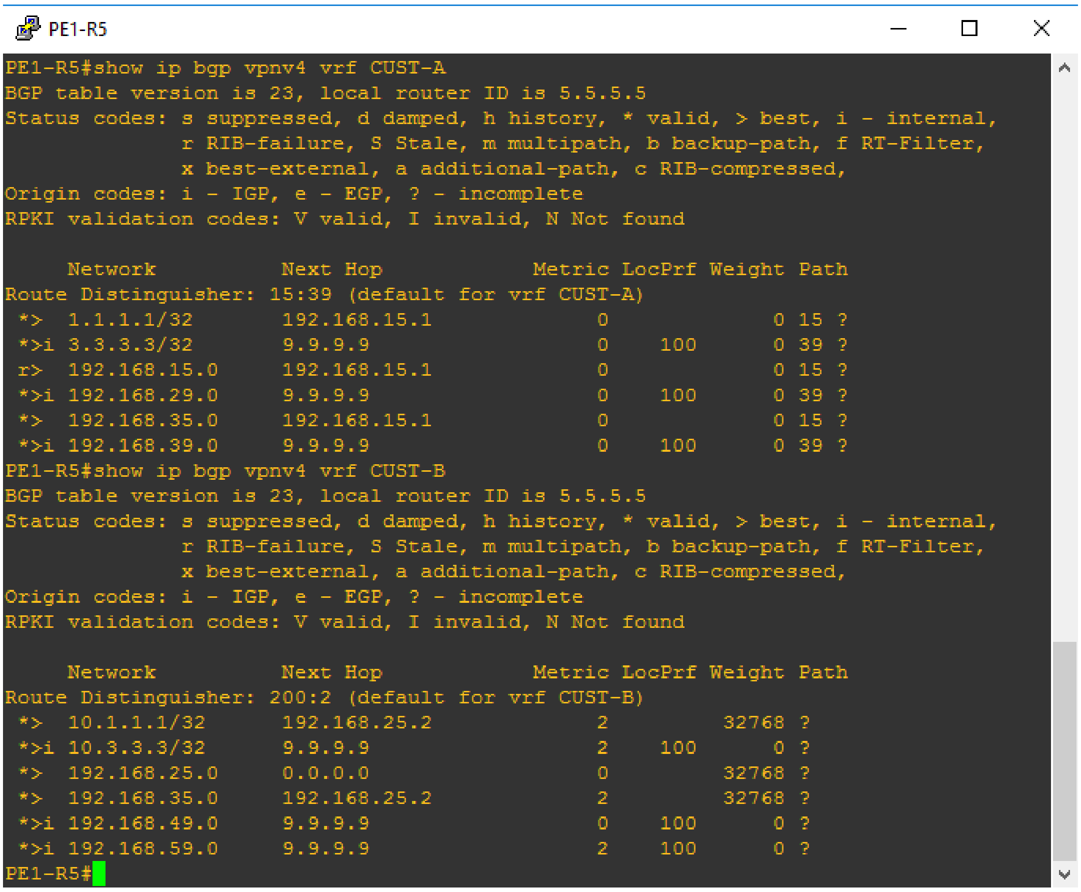
```
PE1-R5#sh ip route vrf CUST-A

Routing Table: CUST-A
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [20/0] via 192.168.15.1, 01:24:59
      3.0.0.0/32 is subnetted, 1 subnets
B        3.3.3.3 [200/0] via 9.9.9.9, 01:24:25
      192.168.15.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.15.0/24 is directly connected, FastEthernet0/0
L        192.168.15.5/32 is directly connected, FastEthernet0/0
B     192.168.29.0/24 [200/0] via 9.9.9.9, 01:24:25
B     192.168.35.0/24 [20/0] via 192.168.15.1, 01:24:59
B     192.168.39.0/24 [200/0] via 9.9.9.9, 01:24:25
PE1-R5#
```

Figure 23 - *VPN Routes of customer A (CUST-A)*



```
PE1-R5#sh ip route vrf CUST-B

Routing Table: CUST-B
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 2 subnets
O        10.1.1.1 [110/2] via 192.168.25.2, 01:26:13, FastEthernet0/1
B        10.3.3.3 [200/2] via 9.9.9.9, 01:25:54
      192.168.25.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.25.0/24 is directly connected, FastEthernet0/1
L        192.168.25.5/32 is directly connected, FastEthernet0/1
O     192.168.35.0/24 [110/2] via 192.168.25.2, 01:26:13, FastEthernet0/1
B     192.168.49.0/24 [200/0] via 9.9.9.9, 01:25:54
B     192.168.59.0/24 [200/2] via 9.9.9.9, 01:25:54
PE1-R5#
```

Figure 24 - *VPN Routes of customer B (CUST-B)*



```
PE1-R5#show ip bgp vpnv4 vrf CUST-A
BGP table version is 23, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 15:39 (default for vrf CUST-A)
 *>  1.1.1.1/32       192.168.15.1             0             0 15 ?
 *>i 3.3.3.3/32       9.9.9.9                  0    100      0 39 ?
 r>  192.168.15.0     192.168.15.1             0             0 15 ?
 *>i 192.168.29.0     9.9.9.9                  0    100      0 39 ?
 *>  192.168.35.0     192.168.15.1             0             0 15 ?
 *>i 192.168.39.0     9.9.9.9                  0    100      0 39 ?
PE1-R5#show ip bgp vpnv4 vrf CUST-B
BGP table version is 23, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:2 (default for vrf CUST-B)
 *>  10.1.1.1/32      192.168.25.2             2         32768 ?
 *>i 10.3.3.3/32      9.9.9.9                  2    100      0 ?
 *>  192.168.25.0     0.0.0.0                  0         32768 ?
 *>  192.168.35.0     192.168.25.2             2         32768 ?
 *>i 192.168.49.0     9.9.9.9                  0    100      0 ?
 *>i 192.168.59.0     9.9.9.9                  2    100      0 ?
PE1-R5#
```

Figure 25 *- VPN Routes of customer A*

3.5.3.3 Configure Route Redistribution

In this step MPLS and MP-BGP backbone up and running, and the CE routers are sending routes to the PE routers within their VRFs. The last step is to join everything together by turning on route redistribution from the customer-side OSPF processes into MP-BGP and vice versa on the PE routers.

First we'll configure redistribution of CE routes in each VRF into MP-BGP. This is done under the BGP IPv4 address family for each VRF.

This enables redistribution of OSPF routes into BGP for transport across the provider network between the two sites. It can be verified that the routes learned from the customer sites (the 192.168.0.0/24 networks) now appear in the BGP tables for their respective VRFs.

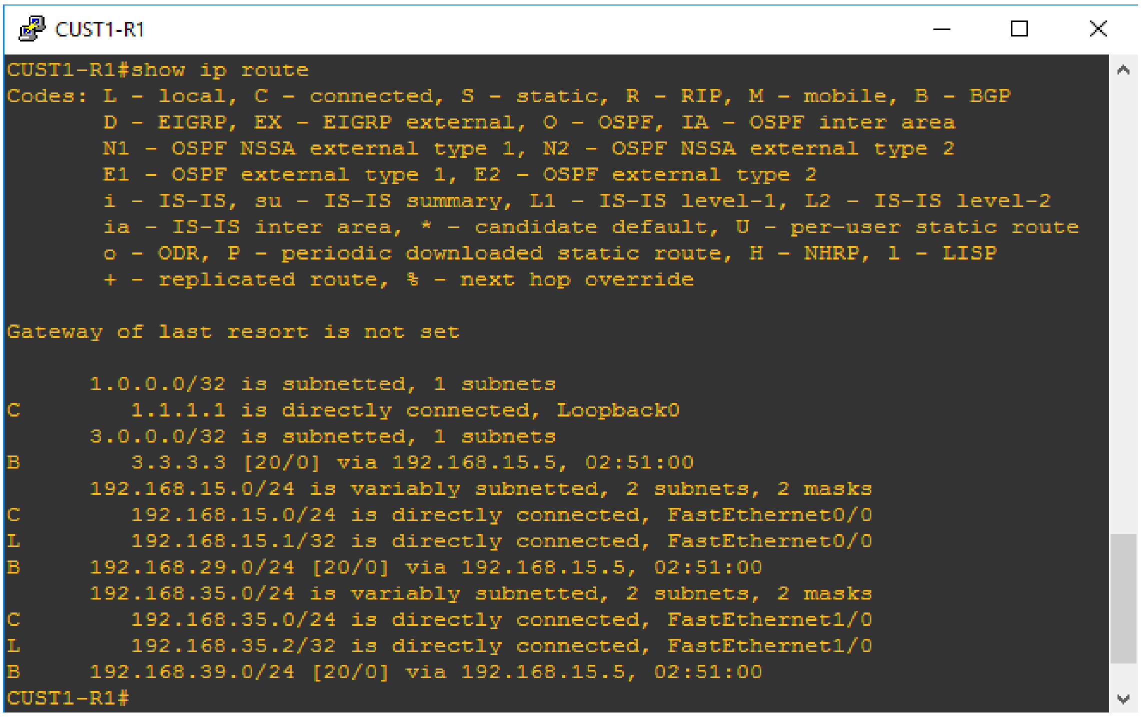
In Figure 25, it can be seen customer's A VPN Routes of the two Remotes Sites.

All the customer edge routers are connected to ISP through a point-to-point link and using BGP for advertising their LAN segment. Loopback0 is configured to emulate inside network of customer. A default route is configured on all CE devices pointing towards ISP.

The last step is to complete the redistribution in the opposite direction, from BGP into the customer OSPF processes.

3.5.4 Testing and Confirmation

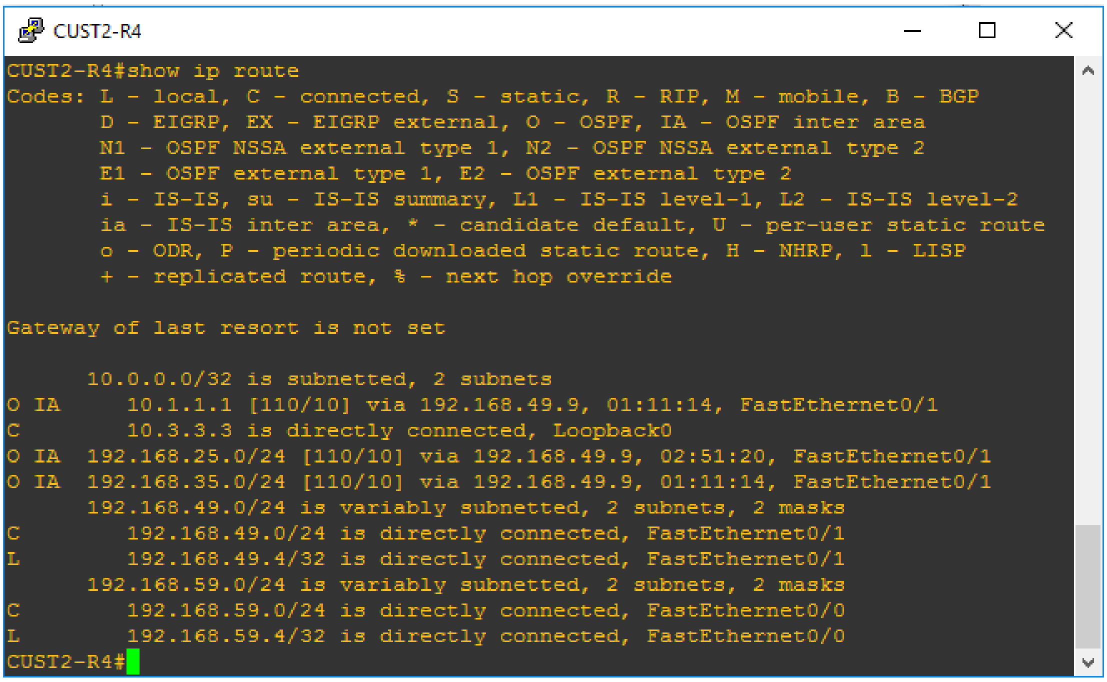
We should now have end-to-end connectivity between the CE routers within each VRF. Both routers for each customer should now have complete routing tables. Here are customer A's routes:



```
CUST1-R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      3.0.0.0/32 is subnetted, 1 subnets
B        3.3.3.3 [20/0] via 192.168.15.5, 02:51:00
      192.168.15.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.15.0/24 is directly connected, FastEthernet0/0
L        192.168.15.1/32 is directly connected, FastEthernet0/0
B     192.168.29.0/24 [20/0] via 192.168.15.5, 02:51:00
      192.168.35.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.35.0/24 is directly connected, FastEthernet1/0
L        192.168.35.2/32 is directly connected, FastEthernet1/0
B     192.168.39.0/24 [20/0] via 192.168.15.5, 02:51:00
CUST1-R1#
```

Figure 26 *- Routing Table of Customer A (CUST1-R1)*

And customer B's routes



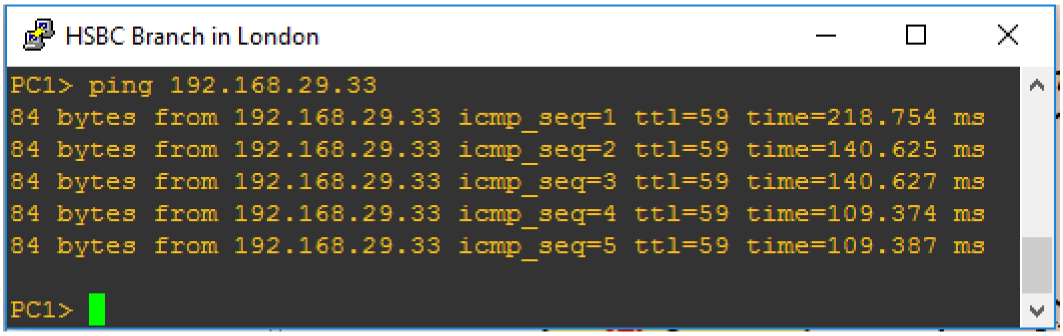
```
CUST2-R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 2 subnets
O IA     10.1.1.1 [110/10] via 192.168.49.9, 01:11:14, FastEthernet0/1
C        10.3.3.3 is directly connected, Loopback0
O IA  192.168.25.0/24 [110/10] via 192.168.49.9, 02:51:20, FastEthernet0/1
O IA  192.168.35.0/24 [110/10] via 192.168.49.9, 01:11:14, FastEthernet0/1
      192.168.49.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.49.0/24 is directly connected, FastEthernet0/1
L        192.168.49.4/32 is directly connected, FastEthernet0/1
      192.168.59.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.59.0/24 is directly connected, FastEthernet0/0
L        192.168.59.4/32 is directly connected, FastEthernet0/0
CUST2-R4#
```

Figure 27 *- Routing Table of Customer B (CUST2-R4)*

You may notice that OSPF routes sent between two sites belonging to the same customer appear as inter-area routes. Although OSPF area 0 is being used at both sites, each site exists as a separate link-state topology connected by the MPLS VPN.

After finished all configuration, now it is able to ping from one CE router or one PC to the other. (It does not need to specify a VRF when doing so due to CE routers have no knowledge that they're in a VRF).

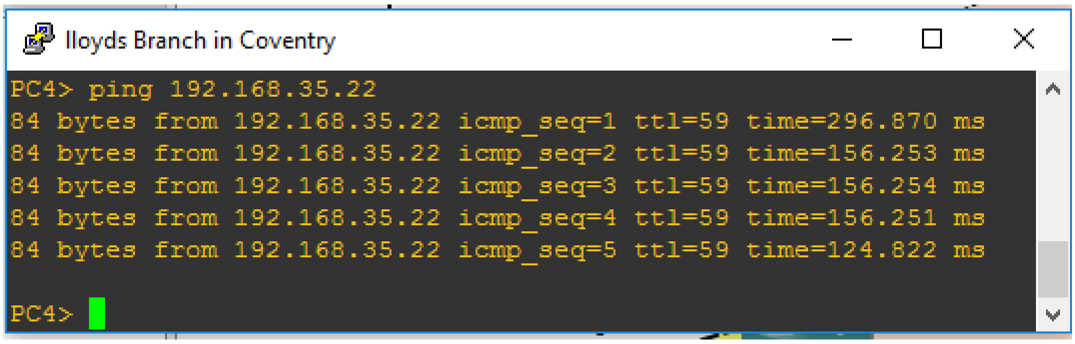
Quick ping between HSBC Branch in London (PC1) to HSBC Branch in Birmingham (PC3):



```
PC1> ping 192.168.29.33
84 bytes from 192.168.29.33 icmp_seq=1 ttl=59 time=218.754 ms
84 bytes from 192.168.29.33 icmp_seq=2 ttl=59 time=140.625 ms
84 bytes from 192.168.29.33 icmp_seq=3 ttl=59 time=140.627 ms
84 bytes from 192.168.29.33 icmp_seq=4 ttl=59 time=109.374 ms
84 bytes from 192.168.29.33 icmp_seq=5 ttl=59 time=109.387 ms

PC1>
```

Figure 28 - *HSBC Branch in London can ping the HSBC Branch in Birmingham.*

Quick ping between lloyds Branch in Coventry (PC2) to lloyds Branch in Manchester (PC4):

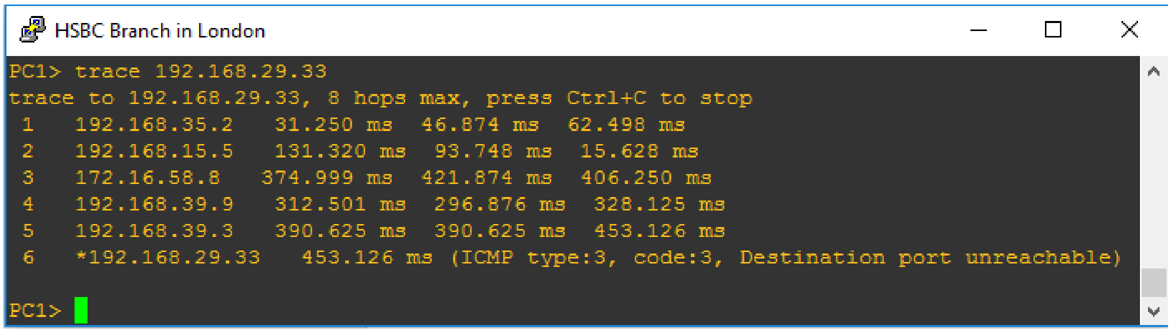


```
PC4> ping 192.168.35.22
84 bytes from 192.168.35.22 icmp_seq=1 ttl=59 time=296.870 ms
84 bytes from 192.168.35.22 icmp_seq=2 ttl=59 time=156.253 ms
84 bytes from 192.168.35.22 icmp_seq=3 ttl=59 time=156.254 ms
84 bytes from 192.168.35.22 icmp_seq=4 ttl=59 time=156.251 ms
84 bytes from 192.168.35.22 icmp_seq=5 ttl=59 time=124.822 ms

PC4>
```

Figure 29 - *lloyds Branch in Coventry can ping the lloyds Branch in Manchester.*

I can be performed a traceroute to verify the path taken as well as the MPLS labels used to traverse the provider network. Figures 44, 45, 46, and 49 show the connectivity between the two MPLS VPNs.

Quick traceroute from HSBC Branch in London to HSBC Branch in Birmingham:



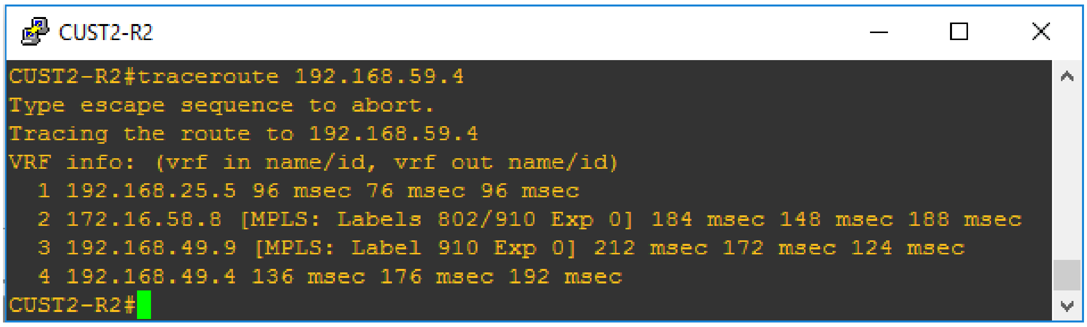
```
PC1> trace 192.168.29.33
trace to 192.168.29.33, 8 hops max, press Ctrl+C to stop
 1   192.168.35.2   31.250 ms  46.874 ms  62.498 ms
 2   192.168.15.5   131.320 ms  93.748 ms  15.628 ms
 3   172.16.58.8   374.999 ms  421.874 ms  406.250 ms
 4   192.168.39.9   312.501 ms  296.876 ms  328.125 ms
 5   192.168.39.3   390.625 ms  390.625 ms  453.126 ms
 6   *192.168.29.33   453.126 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure 30 - *Traceroute from HSBC Branch in London to HSBC Branch in Birmingham.*

Figure 30 shows the connectivity between the two MPLS VPNs and the Label Switched Path is:

HSBC Branch in London (PC1) ➔ CE1-R3 ➔ PE1-R5➔ P-R8 ➔PE2-R9 ➔ CE1-R3 ➔ HSBC Branch in Birmingham (PC3)

Quick traceroute between CE2-R2 to CE2-R4:



```
CUST2-R2#traceroute 192.168.59.4
Type escape sequence to abort.
Tracing the route to 192.168.59.4
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.25.5 96 msec 76 msec 96 msec
  2 172.16.58.8 [MPLS: Labels 802/910 Exp 0] 184 msec 148 msec 188 msec
  3 192.168.49.9 [MPLS: Label 910 Exp 0] 212 msec 172 msec 124 msec
  4 192.168.49.4 136 msec 176 msec 192 msec
CUST2-R2#
```

Figure 31 - *CUST2-R2 traceroute CUST2-R4.*

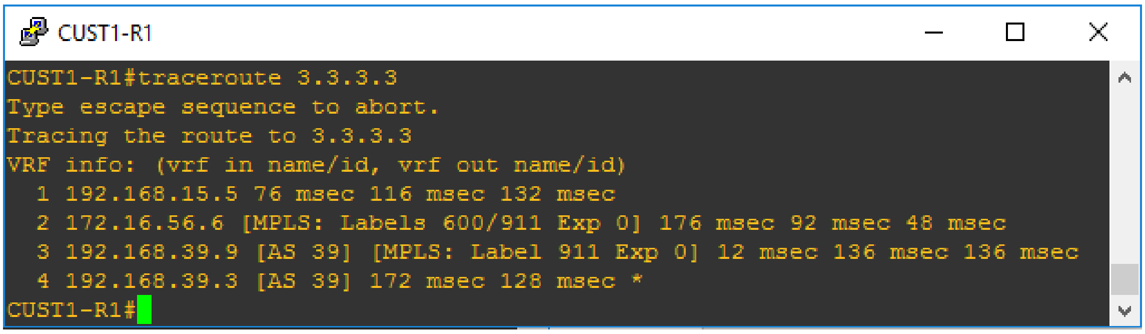
Figure 31 shows the connectivity between the two MPLS VPNs and the Label Switched Path is:

CE2-R2 ➔ PE1-R5 ➔ P-R8 ➔PE2-R9 ➔ CE2-R4

Label 910 is assigned to the VPNv4 route and the top label is for the convenience of the LDP neighbor. Label 910 would remain for the entire transit via the core until being removed by edge router PE1-R5.

Wireshark network analyser is utilized to capture the forwarded packets via the MPLS network.

Quick traceroute between CE1-R1 and CE1-R3:

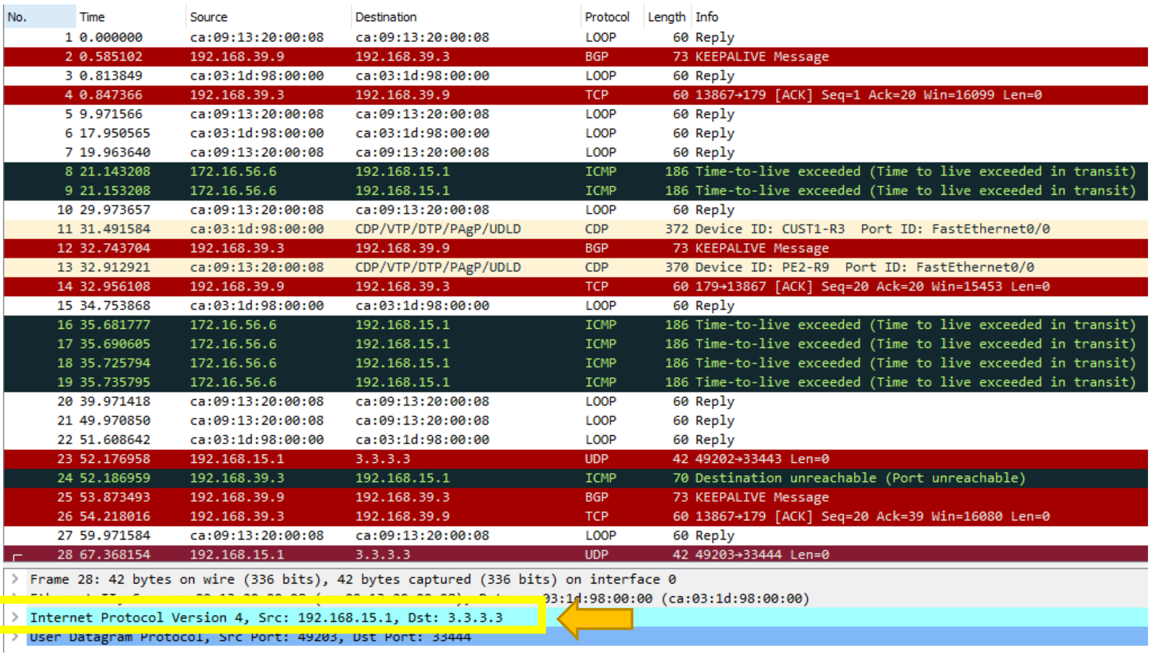


```
CUST1-R1#traceroute 3.3.3.3
Type escape sequence to abort.
Tracing the route to 3.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.15.5 76 msec 116 msec 132 msec
  2 172.16.56.6 [MPLS: Labels 600/911 Exp 0] 176 msec 92 msec 48 msec
  3 192.168.39.9 [AS 39] [MPLS: Label 911 Exp 0] 12 msec 136 msec 136 msec
  4 192.168.39.3 [AS 39] 172 msec 128 msec *
CUST1-R1#
```

Figure 32 - *CUST1-R1 traceroute CUST1-R3.*

Figure 33 shows the connectivity between the two MPLS VPNs and the Label Switched Path is:

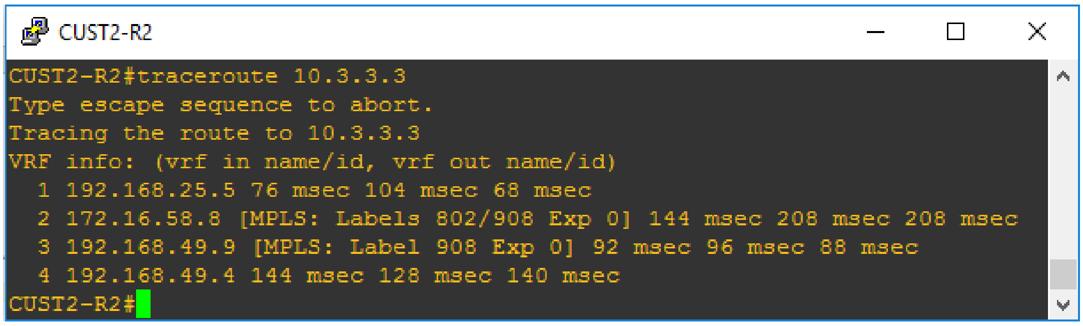
CE1-R1 ➔ PE1-R5 ➔ P-R6 ➔PE2-R9 ➔ CE1-R3



```
No.   Time       Source             Destination           Protocol Length Info
    1 0.000000   ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
    2 0.585102   192.168.39.9       192.168.39.3          BGP        73 KEEPALIVE Message
    3 0.813849   ca:03:1d:98:00:00  ca:03:1d:98:00:00     LOOP       60 Reply
    4 0.847366   192.168.39.3       192.168.39.9          TCP        60 13867→179 [ACK] Seq=1 Ack=20 Win=16099 Len=0
    5 9.971566   ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
    6 17.950565  ca:03:1d:98:00:00  ca:03:1d:98:00:00     LOOP       60 Reply
    7 19.963640  ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
    8 21.143208  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
    9 21.153208  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   10 29.973657  ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
   11 31.491584  ca:03:1d:98:00:00  CDP/VTP/DTP/PAgP/UDLD CDP       372 Device ID: CUST1-R3  Port ID: FastEthernet0/0
   12 32.743704  192.168.39.3       192.168.39.9          BGP        73 KEEPALIVE Message
   13 32.912921  ca:09:13:20:00:08  CDP/VTP/DTP/PAgP/UDLD CDP       370 Device ID: PE2-R9  Port ID: FastEthernet0/0
   14 32.956108  192.168.39.9       192.168.39.3          TCP        60 179→13867 [ACK] Seq=20 Ack=20 Win=15453 Len=0
   15 34.753868  ca:03:1d:98:00:00  ca:03:1d:98:00:00     LOOP       60 Reply
   16 35.681777  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   17 35.690605  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   18 35.725794  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   19 35.735795  172.16.56.6        192.168.15.1          ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   20 39.971418  ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
   21 49.970850  ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
   22 51.608642  ca:03:1d:98:00:00  ca:03:1d:98:00:00     LOOP       60 Reply
   23 52.176958  192.168.15.1       3.3.3.3               UDP        42 49202→33443 Len=0
   24 52.186959  192.168.39.3       192.168.15.1          ICMP       70 Destination unreachable (Port unreachable)
   25 53.873493  192.168.39.9       192.168.39.3          BGP        73 KEEPALIVE Message
   26 54.218016  192.168.39.3       192.168.39.9          TCP        60 13867→179 [ACK] Seq=20 Ack=39 Win=16080 Len=0
   27 59.971584  ca:09:13:20:00:08  ca:09:13:20:00:08     LOOP       60 Reply
   28 67.368154  192.168.15.1       3.3.3.3               UDP        42 49203→33444 Len=0

> Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: ca:09:13:20:00:08 (ca:09:13:20:00:08), Dst: ca:03:1d:98:00:00 (ca:03:1d:98:00:00)
> Internet Protocol Version 4, Src: 192.168.15.1, Dst: 3.3.3.3
> User Datagram Protocol, Src Port: 49203, Dst Port: 33444
```

Figure 33 - *CUST1-R1 traceroute CUST1-R3.*

Quick traceroute between CE2-R2 and CE2-R4:



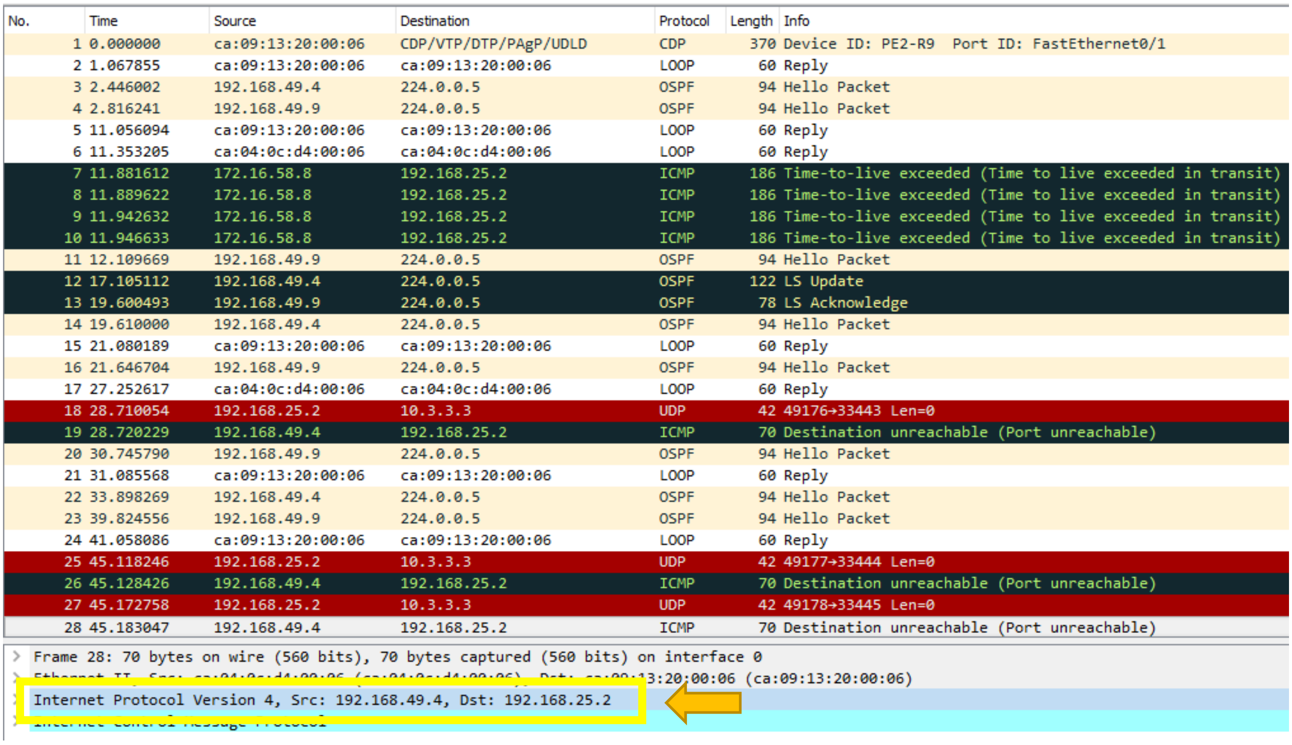
CUST2-R2

```
CUST2-R2#traceroute 10.3.3.3
Type escape sequence to abort.
Tracing the route to 10.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.25.5 76 msec 104 msec 68 msec
  2 172.16.58.8 [MPLS: Labels 802/908 Exp 0] 144 msec 208 msec 208 msec
  3 192.168.49.9 [MPLS: Label 908 Exp 0] 92 msec 96 msec 88 msec
  4 192.168.49.4 144 msec 128 msec 140 msec
CUST2-R2#
```

Figure 34 – *CUST2-R2 traceroute CUST2-R4.*

Figure 35 shows the connectivity between the two MPLS VPNs and the Label Switched Path is:

CE2-R2 ➔ PE1-R5 ➔ P-R8 ➔PE2-R9 ➔ CE2-R4



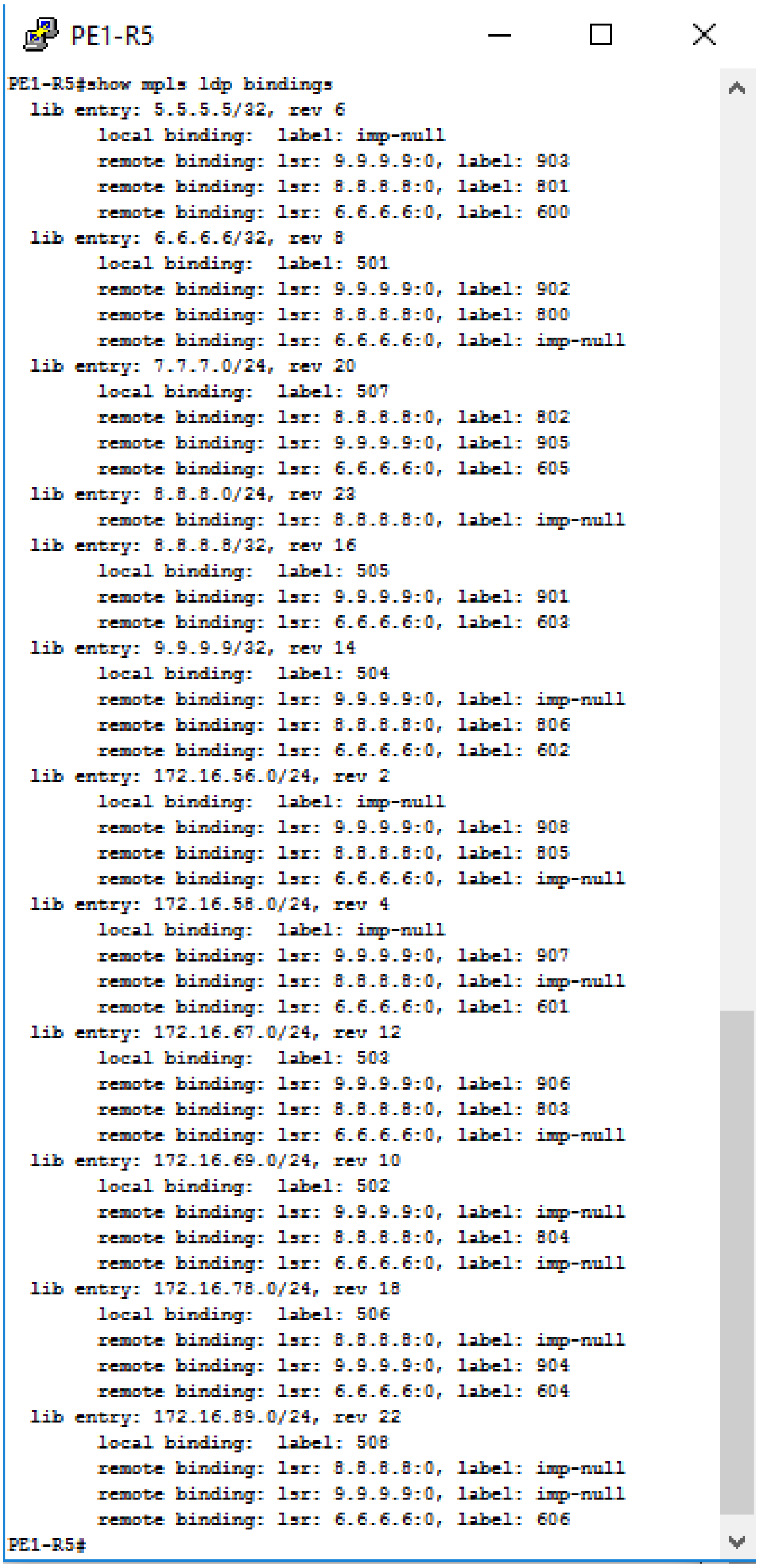
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ca:09:13:20:00:06	CDP/VTP/DTP/PAgP/UDLD	CDP	370	Device ID: PE2-R9 Port ID: FastEthernet0/1
2	1.067855	ca:09:13:20:00:06	ca:09:13:20:00:06	LOOP	60	Reply
3	2.446002	192.168.49.4	224.0.0.5	OSPF	94	Hello Packet
4	2.816241	192.168.49.9	224.0.0.5	OSPF	94	Hello Packet
5	11.056094	ca:09:13:20:00:06	ca:09:13:20:00:06	LOOP	60	Reply
6	11.353205	ca:04:0c:d4:00:06	ca:04:0c:d4:00:06	LOOP	60	Reply
7	11.881612	172.16.58.8	192.168.25.2	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
8	11.889622	172.16.58.8	192.168.25.2	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
9	11.942632	172.16.58.8	192.168.25.2	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
10	11.946633	172.16.58.8	192.168.25.2	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
11	12.109669	192.168.49.9	224.0.0.5	OSPF	94	Hello Packet
12	17.105112	192.168.49.4	224.0.0.5	OSPF	122	LS Update
13	19.600493	192.168.49.9	224.0.0.5	OSPF	78	LS Acknowledge
14	19.610000	192.168.49.4	224.0.0.5	OSPF	94	Hello Packet
15	21.080189	ca:09:13:20:00:06	ca:09:13:20:00:06	LOOP	60	Reply
16	21.646704	192.168.49.9	224.0.0.5	OSPF	94	Hello Packet
17	27.252617	ca:04:0c:d4:00:06	ca:04:0c:d4:00:06	LOOP	60	Reply
18	28.710054	192.168.25.2	10.3.3.3	UDP	42	49176→33443 Len=0
19	28.720229	192.168.49.4	192.168.25.2	ICMP	70	Destination unreachable (Port unreachable)
20	30.745790	192.168.49.9	224.0.0.5	OSPF	94	Hello Packet
21	31.085568	ca:09:13:20:00:06	ca:09:13:20:00:06	LOOP	60	Reply
22	33.898269	192.168.49.4	224.0.0.5	OSPF	94	Hello Packet
23	39.824556	192.168.49.9	224.0.0.5	OSPF	94	Hello Packet
24	41.058086	ca:09:13:20:00:06	ca:09:13:20:00:06	LOOP	60	Reply
25	45.118246	192.168.25.2	10.3.3.3	UDP	42	49177→33444 Len=0
26	45.128426	192.168.49.4	192.168.25.2	ICMP	70	Destination unreachable (Port unreachable)
27	45.172758	192.168.25.2	10.3.3.3	UDP	42	49178→33445 Len=0
28	45.183047	192.168.49.4	192.168.25.2	ICMP	70	Destination unreachable (Port unreachable)

```
> Frame 28: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: ca:04:0c:d4:00:06 (ca:04:0c:d4:00:06), Dst: ca:09:13:20:00:06 (ca:09:13:20:00:06)
> Internet Protocol Version 4, Src: 192.168.49.4, Dst: 192.168.25.2
> Internet Control Message Protocol
```

Figure 35 *- CUST2-R2 traceroute CUST2-R4.*

In the illustration in the figure 36 below, demonstrations the (LIB) [2] table in PE1-R5. The LIB table is an MPLS table where all the labels are stored. It contains all the local labels and mapping of the labels that are received from the adjacent routers.

[2] The Label Information Base (LIB) is an MPLS table. This is the place where the router will keep all known MPLS labels.

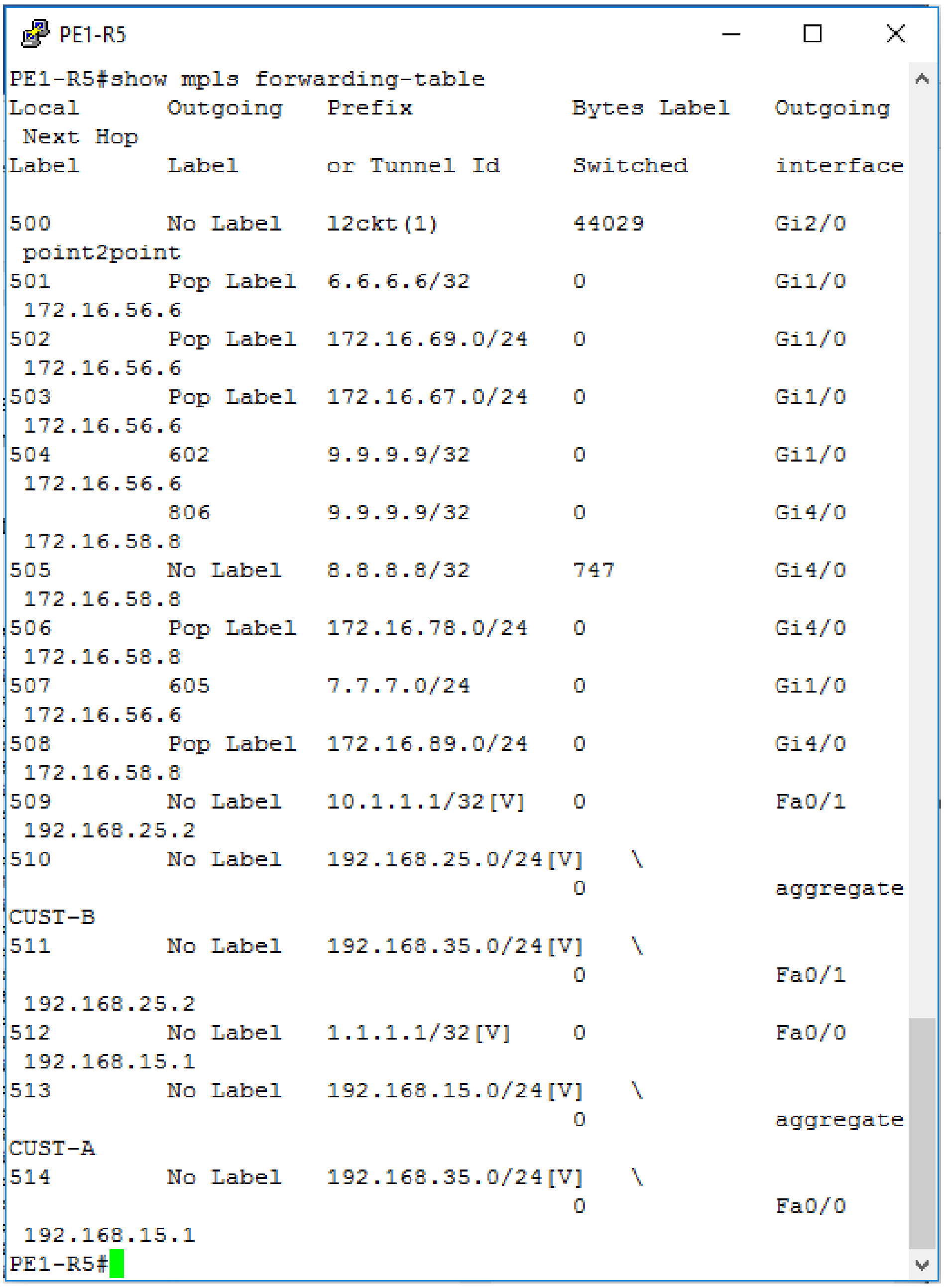


```
PE1-R5#show mpls ldp bindings
  lib entry: 5.5.5.5/32, rev 6
        local binding:  label: imp-null
        remote binding: lsr: 9.9.9.9:0, label: 903
        remote binding: lsr: 8.8.8.8:0, label: 801
        remote binding: lsr: 6.6.6.6:0, label: 600
  lib entry: 6.6.6.6/32, rev 8
        local binding:  label: 501
        remote binding: lsr: 9.9.9.9:0, label: 902
        remote binding: lsr: 8.8.8.8:0, label: 800
        remote binding: lsr: 6.6.6.6:0, label: imp-null
  lib entry: 7.7.7.0/24, rev 20
        local binding:  label: 507
        remote binding: lsr: 8.8.8.8:0, label: 802
        remote binding: lsr: 9.9.9.9:0, label: 905
        remote binding: lsr: 6.6.6.6:0, label: 605
  lib entry: 8.8.8.0/24, rev 23
        remote binding: lsr: 8.8.8.8:0, label: imp-null
  lib entry: 8.8.8.8/32, rev 16
        local binding:  label: 505
        remote binding: lsr: 9.9.9.9:0, label: 901
        remote binding: lsr: 6.6.6.6:0, label: 603
  lib entry: 9.9.9.9/32, rev 14
        local binding:  label: 504
        remote binding: lsr: 9.9.9.9:0, label: imp-null
        remote binding: lsr: 8.8.8.8:0, label: 806
        remote binding: lsr: 6.6.6.6:0, label: 602
  lib entry: 172.16.56.0/24, rev 2
        local binding:  label: imp-null
        remote binding: lsr: 9.9.9.9:0, label: 908
        remote binding: lsr: 8.8.8.8:0, label: 805
        remote binding: lsr: 6.6.6.6:0, label: imp-null
  lib entry: 172.16.58.0/24, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 9.9.9.9:0, label: 907
        remote binding: lsr: 8.8.8.8:0, label: imp-null
        remote binding: lsr: 6.6.6.6:0, label: 601
  lib entry: 172.16.67.0/24, rev 12
        local binding:  label: 503
        remote binding: lsr: 9.9.9.9:0, label: 906
        remote binding: lsr: 8.8.8.8:0, label: 803
        remote binding: lsr: 6.6.6.6:0, label: imp-null
  lib entry: 172.16.69.0/24, rev 10
        local binding:  label: 502
        remote binding: lsr: 9.9.9.9:0, label: imp-null
        remote binding: lsr: 8.8.8.8:0, label: 804
        remote binding: lsr: 6.6.6.6:0, label: imp-null
  lib entry: 172.16.78.0/24, rev 18
        local binding:  label: 506
        remote binding: lsr: 8.8.8.8:0, label: imp-null
        remote binding: lsr: 9.9.9.9:0, label: 904
        remote binding: lsr: 6.6.6.6:0, label: 604
  lib entry: 172.16.89.0/24, rev 22
        local binding:  label: 508
        remote binding: lsr: 8.8.8.8:0, label: imp-null
        remote binding: lsr: 9.9.9.9:0, label: imp-null
        remote binding: lsr: 6.6.6.6:0, label: 606
PE1-R5#
```

Figure 36 *- LIB table*

In the illustration in the figure 37 below, demonstrations the Base (LFIB) [3] table that is a MPLS table utilized by routers to create decision where to forward the labelled packets.

[3] The Label Forwarding Instance LFIB is another MPLS table. This is a table that the router uses to forward labelled packets going through the network. The Label Information Base (LIB) uses the LFIB to forward traffic.



```
PE1-R5#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing
 Next Hop
Label      Label      or Tunnel Id     Switched      interface

500        No Label   l2ckt(1)         44029         Gi2/0
 point2point
501        Pop Label  6.6.6.6/32       0             Gi1/0
 172.16.56.6
502        Pop Label  172.16.69.0/24   0             Gi1/0
 172.16.56.6
503        Pop Label  172.16.67.0/24   0             Gi1/0
 172.16.56.6
504        602        9.9.9.9/32       0             Gi1/0
 172.16.56.6
           806        9.9.9.9/32       0             Gi4/0
 172.16.58.8
505        No Label   8.8.8.8/32       747           Gi4/0
 172.16.58.8
506        Pop Label  172.16.78.0/24   0             Gi4/0
 172.16.58.8
507        605        7.7.7.0/24       0             Gi1/0
 172.16.56.6
508        Pop Label  172.16.89.0/24   0             Gi4/0
 172.16.58.8
509        No Label   10.1.1.1/32[V]   0             Fa0/1
 192.168.25.2
510        No Label   192.168.25.0/24[V]   \
                                       0             aggregate
CUST-B
511        No Label   192.168.35.0/24[V]   \
                                       0             Fa0/1

 192.168.25.2
512        No Label   1.1.1.1/32[V]    0             Fa0/0
 192.168.15.1
513        No Label   192.168.15.0/24[V]   \
                                       0             aggregate
CUST-A
514        No Label   192.168.35.0/24[V]   \
                                       0             Fa0/0

 192.168.15.1
PE1-R5#
```

Figure 37 *- LFIB table*

3.6 VPN Layer2 implement and Configuration

In this stage, I will start to implement and configure VPN Layer 2.

In MPLS Layer 2 VPN topology utilized in this scenario, the network topology figure 51 has two customer sites at CUST3-R5 and CUST3-R6 at distant locations connected utilizing MPLS L2 VPN technology. CEs at both end are connected with Provider Edge routers using serial links running Point-to-Point protocol (PPP). In the topology utilized for PPP over MPLS or Any Transport over MPLS, CUST3-R5 is connected to PE1-R5 and CUST3-R6 is connected to PE2-R9, PE1-R5 has two paths to reach PE2-R9, one via P-R6 and other one via P-R8.

To configure MPLS Layer 2 VPN functionality on routers, the PE routers must be configured to distribute routing information to other routers in the VPN. However, because the tunnel information is maintained at both PE routers, neither the provider core routers nor the customer edge (CE) routers need to maintain any VPN information in their configuration databases.

3.6.1 Network topology

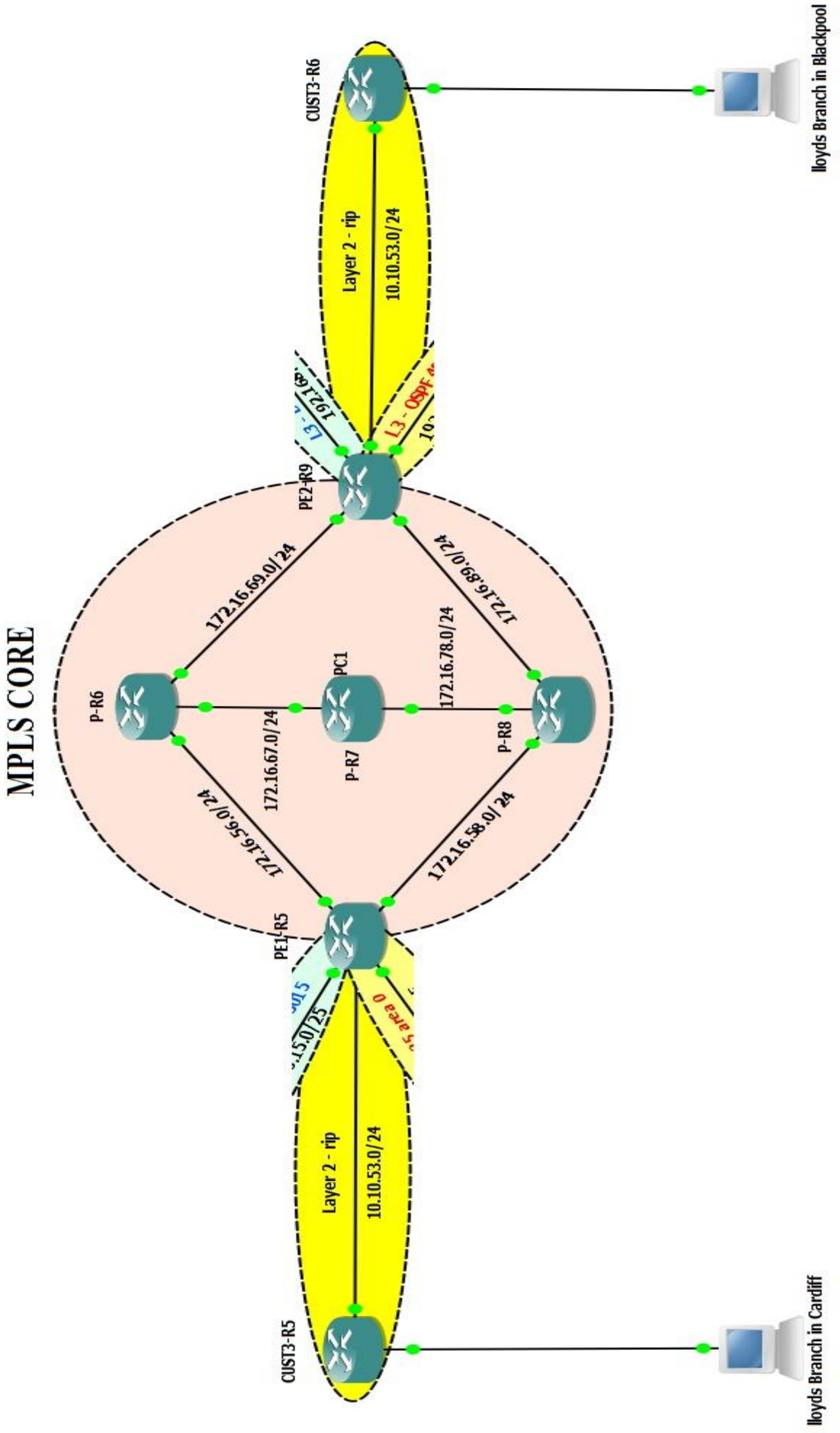


***Figure 38** –MPLS Layer2 VPN (Customer 2 in the middle)*

Configure all the PE and P routers with OSPF as the IGP. Enable the MPLS, LDP, and OSPF protocols in all interfaces in the Core. LDP is used as the signalling protocol on Router PE1 and PE2 for the Layer 2 circuit but all necessarily configuration had been done at previous stage for Layer3 in the MPLS Core, PE1 and PE2; just interface g2/0 from PE1 and interface g1/0 from PE2 should be configured for Layer2 VPN.

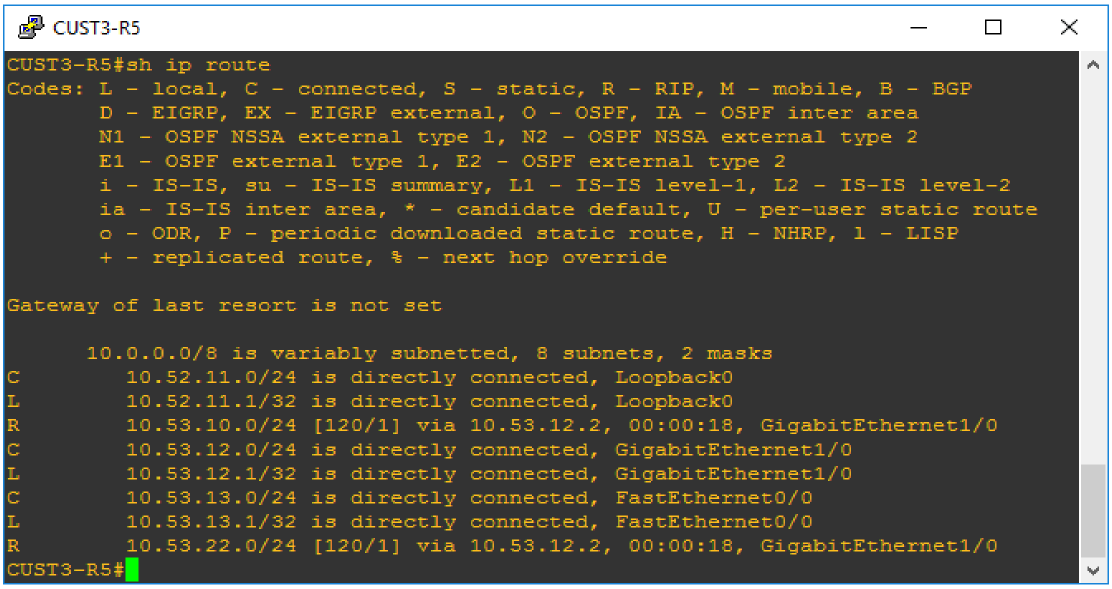
After that CUST3-R5 and CUST3-R6 need to be configured the following configuration:

1. IP address configuration.
2. Configure RIP protocol.
3. Configure VPN Layer 2 between PE1-R5 and PE2-R9.

And also I put two PCs stand for two branch office which just need IP address and default gateway to be able to ping each other.

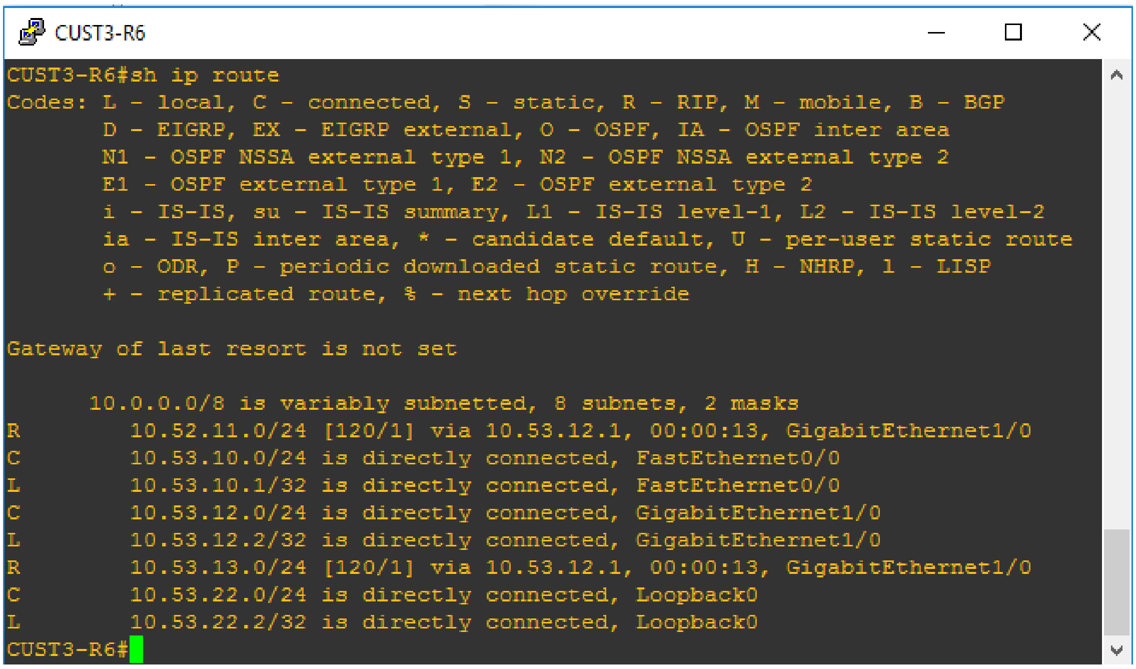
3.6.2 Testing and Confirmation

Figures 39 and 40 show the IP route between CUST3-R5 to CUST3-R6.



```
CUST3-R5#sh ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.52.11.0/24 is directly connected, Loopback0
L        10.52.11.1/32 is directly connected, Loopback0
R        10.53.10.0/24 [120/1] via 10.53.12.2, 00:00:18, GigabitEthernet1/0
C        10.53.12.0/24 is directly connected, GigabitEthernet1/0
L        10.53.12.1/32 is directly connected, GigabitEthernet1/0
C        10.53.13.0/24 is directly connected, FastEthernet0/0
L        10.53.13.1/32 is directly connected, FastEthernet0/0
R        10.53.22.0/24 [120/1] via 10.53.12.2, 00:00:18, GigabitEthernet1/0
CUST3-R5#
```

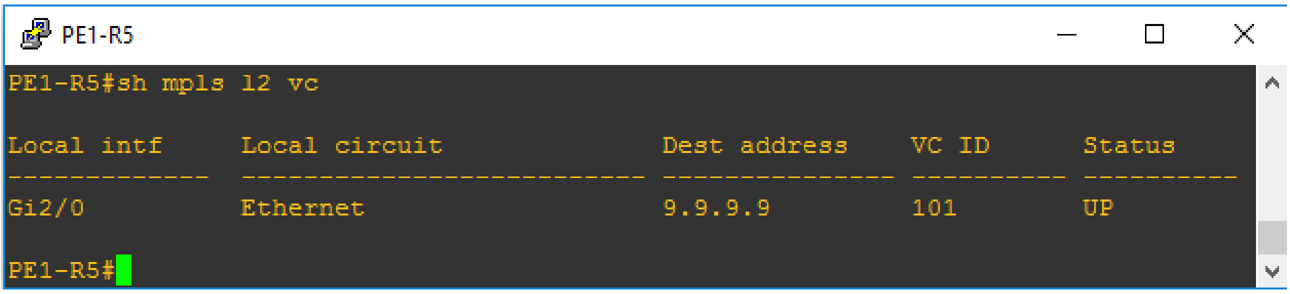
Figure 39 *– Show ip route in CUST3-R5.*



```
CUST3-R6#sh ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
R        10.52.11.0/24 [120/1] via 10.53.12.1, 00:00:13, GigabitEthernet1/0
C        10.53.10.0/24 is directly connected, FastEthernet0/0
L        10.53.10.1/32 is directly connected, FastEthernet0/0
C        10.53.12.0/24 is directly connected, GigabitEthernet1/0
L        10.53.12.2/32 is directly connected, GigabitEthernet1/0
R        10.53.13.0/24 [120/1] via 10.53.12.1, 00:00:13, GigabitEthernet1/0
C        10.53.22.0/24 is directly connected, Loopback0
L        10.53.22.2/32 is directly connected, Loopback0
CUST3-R6#
```

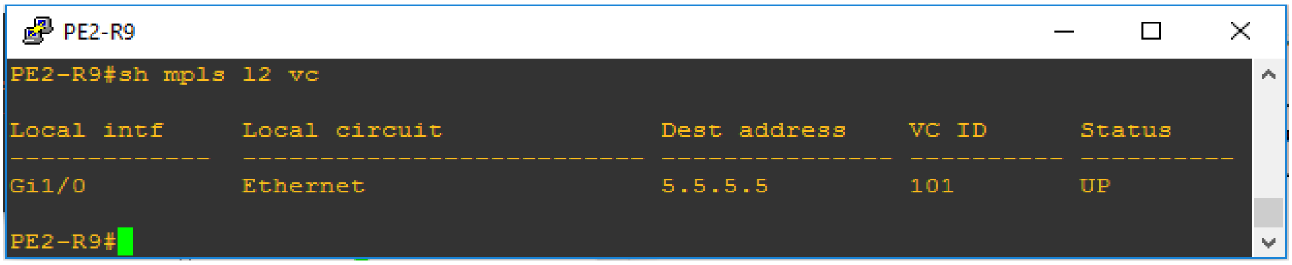
Figure 40 *– Show ip route in CUST3-R6.*

Figures 41 and 42 show L2 VPN on PE1-R5 and PE2-R9.



```
PE1-R5#sh mpls l2 vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi2/0          Ethernet                   9.9.9.9         101        UP

PE1-R5#
```

Figure 41 *– Show mpls l2 in PE1-R5.*

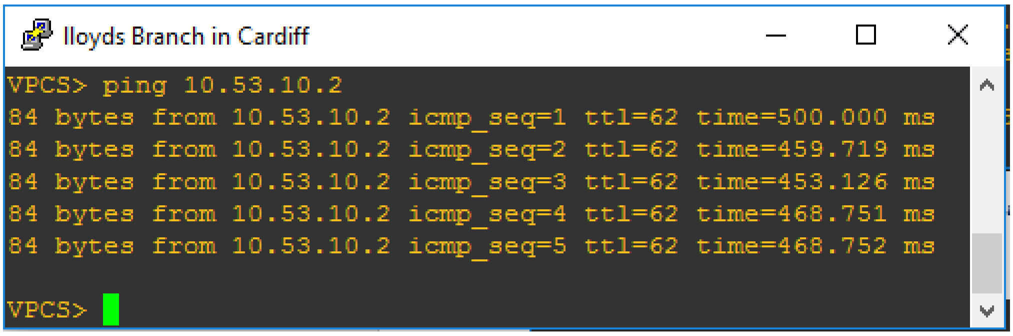


```
PE2-R9#sh mpls l2 vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1/0          Ethernet                   5.5.5.5         101        UP

PE2-R9#
```

Figure 42 *– Show mpls l2 in PE2-R9.*

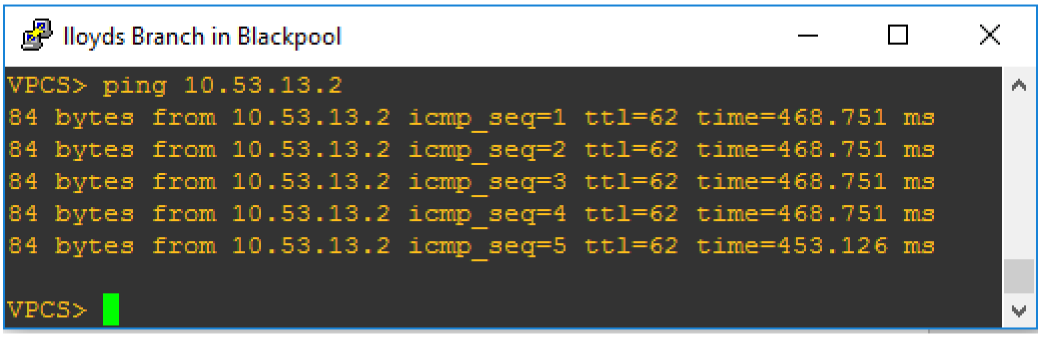
After finished all configuration, now it is possible to ping from one CE router or one PC to the other.

Quick ping between lloyds Branch in Cardiff (PC5) and lloyds Branch in Blackpool (PC6):



```
VPCS> ping 10.53.10.2
84 bytes from 10.53.10.2 icmp_seq=1 ttl=62 time=500.000 ms
84 bytes from 10.53.10.2 icmp_seq=2 ttl=62 time=459.719 ms
84 bytes from 10.53.10.2 icmp_seq=3 ttl=62 time=453.126 ms
84 bytes from 10.53.10.2 icmp_seq=4 ttl=62 time=468.751 ms
84 bytes from 10.53.10.2 icmp_seq=5 ttl=62 time=468.752 ms

VPCS>
```

Figure 43 *– Ping from lloyds Branch in Cardiff (PC5) to lloyds Branch in Blackpool (PC6).*

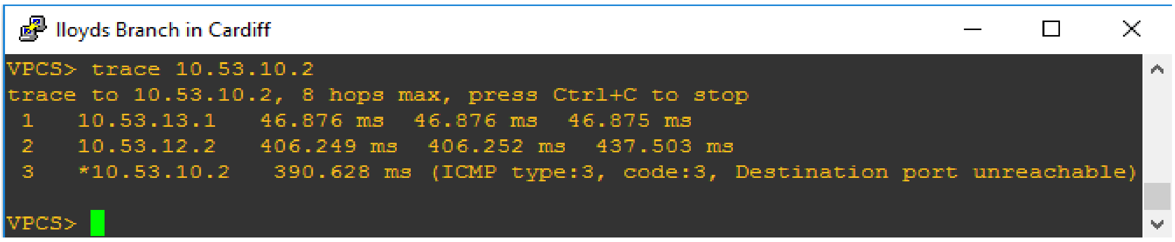


```
VPCS> ping 10.53.13.2
84 bytes from 10.53.13.2 icmp_seq=1 ttl=62 time=468.751 ms
84 bytes from 10.53.13.2 icmp_seq=2 ttl=62 time=468.751 ms
84 bytes from 10.53.13.2 icmp_seq=3 ttl=62 time=468.751 ms
84 bytes from 10.53.13.2 icmp_seq=4 ttl=62 time=468.751 ms
84 bytes from 10.53.13.2 icmp_seq=5 ttl=62 time=453.126 ms

VPCS>
```

Figure 44 *– Ping from lloyds Branch in Blackpool (PC6) to lloyds Branch in Cardiff (PC5).*

I can be performed a traceroute to verify the path taken as well as the MPLS labels used to traverse the provider network.

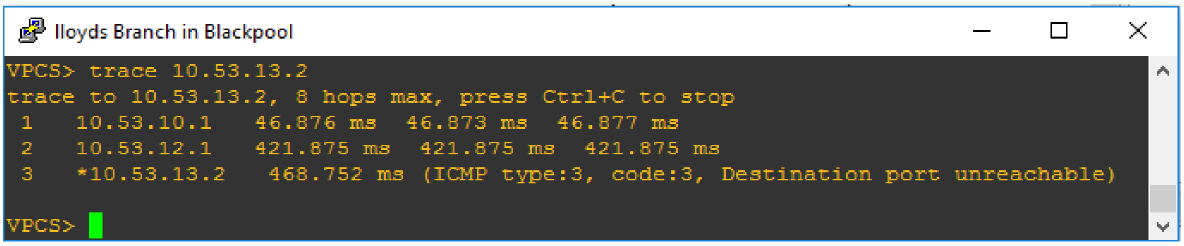
Quick traceroute between lloyds Branch in Cardiff (PC5) and lloyds Branch in Blackpool (PC6):



```
VPCS> trace 10.53.10.2
trace to 10.53.10.2, 8 hops max, press Ctrl+C to stop
 1   10.53.13.1   46.876 ms  46.876 ms  46.875 ms
 2   10.53.12.2   406.249 ms  406.252 ms  437.503 ms
 3   *10.53.10.2   390.628 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>
```

Figure 45 *– Traceroute from lloyds Branch in Blackpool (PC6) to lloyds Branch in Cardiff (PC5).*

lloyds Branch in Cardiff (PC5) ➔ CUST3-R5 ➔ CUST3-R6 ➔ lloyds Branch in Blackpool (PC6)

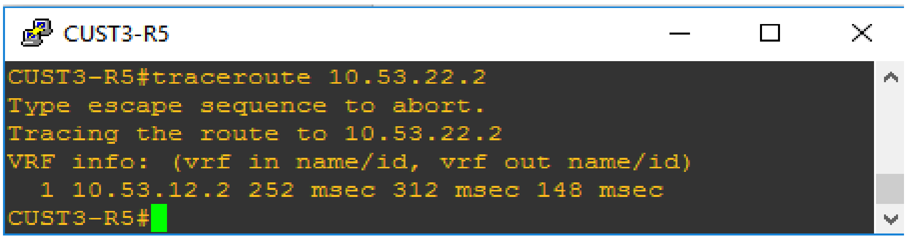


```
VPCS> trace 10.53.13.2
trace to 10.53.13.2, 8 hops max, press Ctrl+C to stop
 1   10.53.10.1   46.876 ms  46.873 ms  46.877 ms
 2   10.53.12.1   421.875 ms  421.875 ms  421.875 ms
 3   *10.53.13.2   468.752 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>
```

Figure 46 *–Ttraceroute from lloyds Branch in Blackpool (PC6) to lloyds Branch in Cardiff (PC5).*

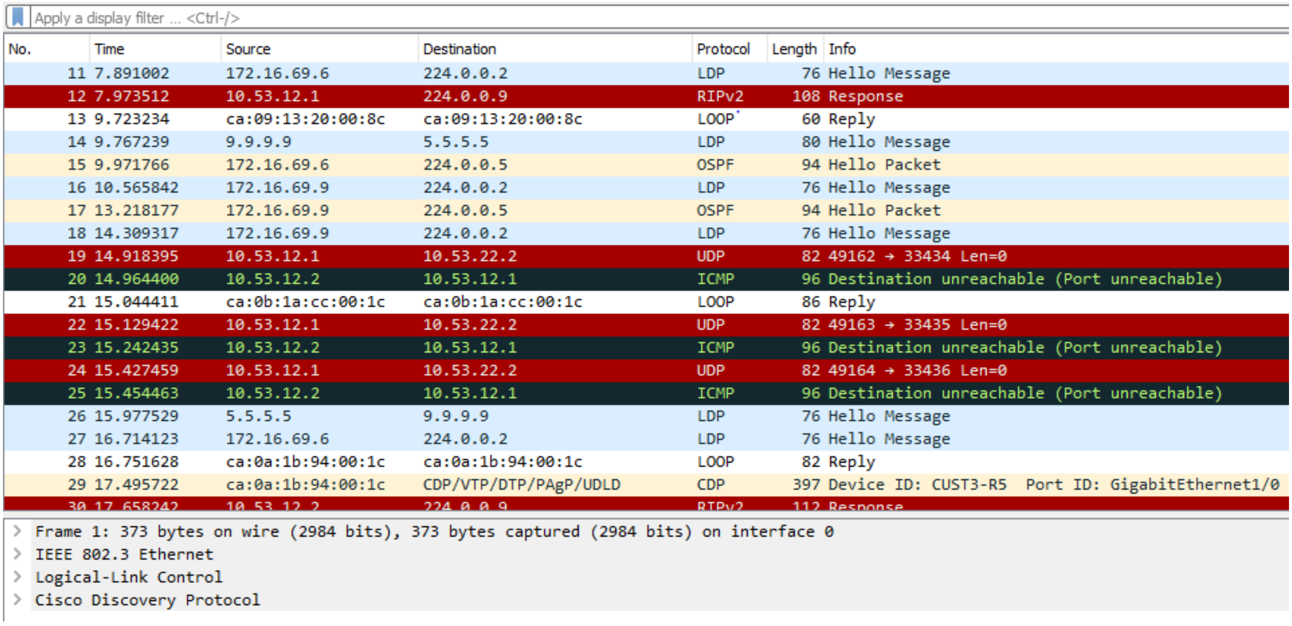
lloyds Branch in Blackpool (PC6) ➔ CUST3-R6 ➔ CUST3-R5 ➔ lloyds Branch in Cardiff (PC5)

Wireshark network analyser was again utilized to capture the forwarded packets via the MPLS network. A quick traceroute between CE3-R5 and CE3-R6 (see Figures 47 and 48).



```
CUST3-R5#traceroute 10.53.22.2
Type escape sequence to abort.
Tracing the route to 10.53.22.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.53.12.2 252 msec 312 msec 148 msec
CUST3-R5#
```

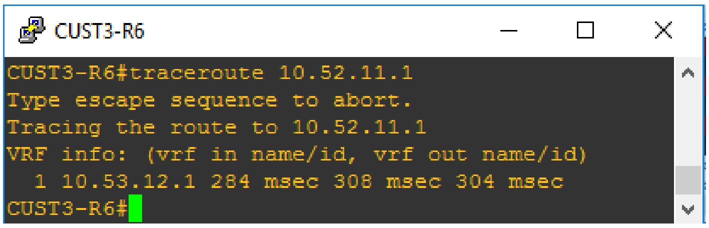
Figure 47 *– CUST3-R5 traceroute CUST3-R6.*



```
Apply a display filter ... <Ctrl-/>
No.   Time         Source              Destination          Protocol  Length  Info
   11 7.891002     172.16.69.6         224.0.0.2            LDP         76 Hello Message
   12 7.973512     10.53.12.1          224.0.0.9            RIPv2      108 Response
   13 9.723234     ca:09:13:20:00:8c   ca:09:13:20:00:8c    LOOP        60 Reply
   14 9.767239     9.9.9.9             5.5.5.5              LDP         80 Hello Message
   15 9.971766     172.16.69.6         224.0.0.5            OSPF        94 Hello Packet
   16 10.565842    172.16.69.9         224.0.0.2            LDP         76 Hello Message
   17 13.218177    172.16.69.9         224.0.0.5            OSPF        94 Hello Packet
   18 14.309317    172.16.69.9         224.0.0.2            LDP         76 Hello Message
   19 14.918395    10.53.12.1          10.53.22.2           UDP         82 49162 → 33434 Len=0
   20 14.964400    10.53.12.2          10.53.12.1           ICMP        96 Destination unreachable (Port unreachable)
   21 15.044411    ca:0b:1a:cc:00:1c   ca:0b:1a:cc:00:1c    LOOP        86 Reply
   22 15.129422    10.53.12.1          10.53.22.2           UDP         82 49163 → 33435 Len=0
   23 15.242435    10.53.12.2          10.53.12.1           ICMP        96 Destination unreachable (Port unreachable)
   24 15.427459    10.53.12.1          10.53.22.2           UDP         82 49164 → 33436 Len=0
   25 15.454463    10.53.12.2          10.53.12.1           ICMP        96 Destination unreachable (Port unreachable)
   26 15.977529    5.5.5.5             9.9.9.9              LDP         76 Hello Message
   27 16.714123    172.16.69.6         224.0.0.2            LDP         76 Hello Message
   28 16.751628    ca:0a:1b:94:00:1c   ca:0a:1b:94:00:1c    LOOP        82 Reply
   29 17.495722    ca:0a:1b:94:00:1c   CDP/VTP/DTP/PAgP/UDLD CDP        397 Device ID: CUST3-R5  Port ID: GigabitEthernet1/0
   30 17.658242    10.53.12.2          224.0.0.9            RIPv2      112 Response
> Frame 1: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
> Cisco Discovery Protocol
```

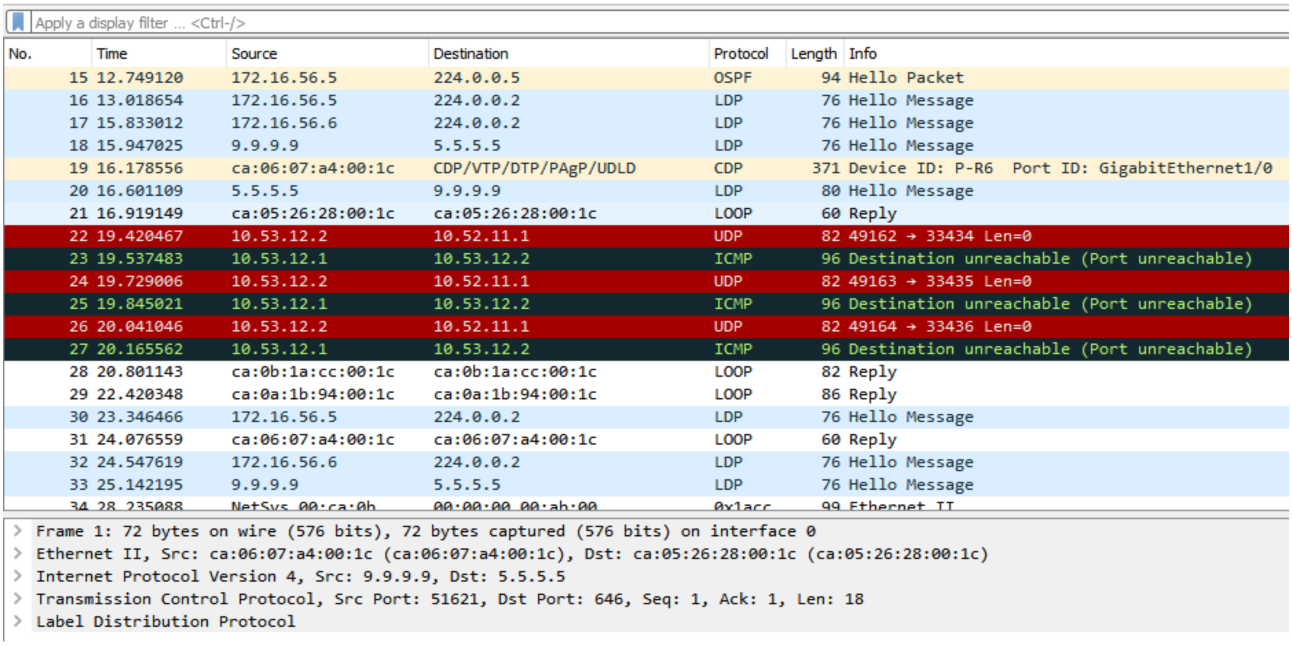
***Figure 48** – CUST3-R5 traceroute CUST3-R6.*

Figures 49 and 50 show CE3-R5 can traceroute CE3-R6.



```
CUST3-R6#traceroute 10.52.11.1
Type escape sequence to abort.
Tracing the route to 10.52.11.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.53.12.1 284 msec 308 msec 304 msec
CUST3-R6#
```

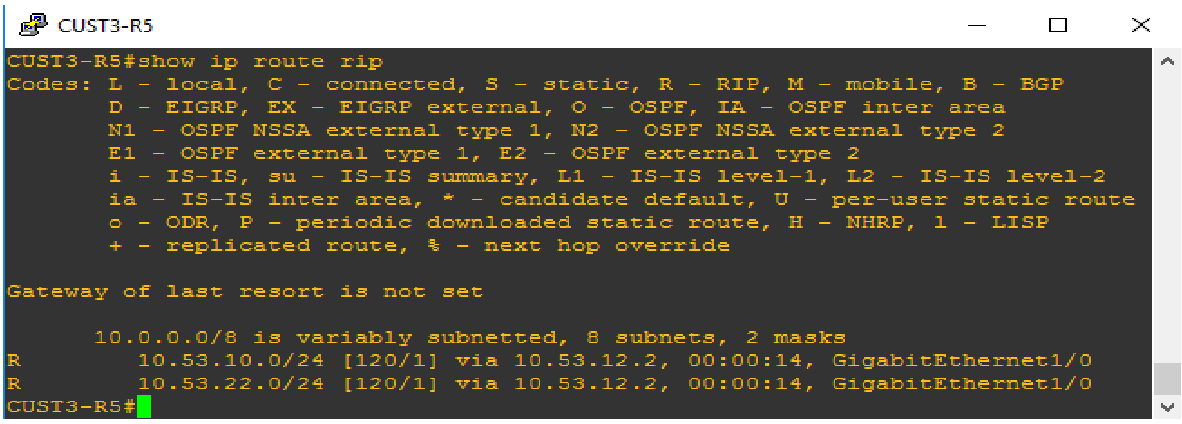
***Figure 49** – CUST3-R6 traceroute CUST3-R5.*



```
Apply a display filter ... <Ctrl-/>
No.   Time         Source              Destination          Protocol  Length  Info
   15 12.749120    172.16.56.5         224.0.0.5            OSPF        94 Hello Packet
   16 13.018654    172.16.56.5         224.0.0.2            LDP         76 Hello Message
   17 15.833012    172.16.56.6         224.0.0.2            LDP         76 Hello Message
   18 15.947025    9.9.9.9             5.5.5.5              LDP         76 Hello Message
   19 16.178556    ca:06:07:a4:00:1c   CDP/VTP/DTP/PAgP/UDLD CDP        371 Device ID: P-R6  Port ID: GigabitEthernet1/0
   20 16.601109    5.5.5.5             9.9.9.9              LDP         80 Hello Message
   21 16.919149    ca:05:26:28:00:1c   ca:05:26:28:00:1c    LOOP        60 Reply
   22 19.420467    10.53.12.2          10.52.11.1           UDP         82 49162 → 33434 Len=0
   23 19.537483    10.53.12.1          10.53.12.2           ICMP        96 Destination unreachable (Port unreachable)
   24 19.729006    10.53.12.2          10.52.11.1           UDP         82 49163 → 33435 Len=0
   25 19.845021    10.53.12.1          10.53.12.2           ICMP        96 Destination unreachable (Port unreachable)
   26 20.041046    10.53.12.2          10.52.11.1           UDP         82 49164 → 33436 Len=0
   27 20.165562    10.53.12.1          10.53.12.2           ICMP        96 Destination unreachable (Port unreachable)
   28 20.801143    ca:0b:1a:cc:00:1c   ca:0b:1a:cc:00:1c    LOOP        82 Reply
   29 22.420348    ca:0a:1b:94:00:1c   ca:0a:1b:94:00:1c    LOOP        86 Reply
   30 23.346466    172.16.56.5         224.0.0.2            LDP         76 Hello Message
   31 24.076559    ca:06:07:a4:00:1c   ca:06:07:a4:00:1c    LOOP        60 Reply
   32 24.547619    172.16.56.6         224.0.0.2            LDP         76 Hello Message
   33 25.142195    9.9.9.9             5.5.5.5              LDP         76 Hello Message
   34 28.235088    NetSys_00:ca:0b     00:00:00_00:ab:00    0x1acc      99 Ethernet II
> Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: ca:06:07:a4:00:1c (ca:06:07:a4:00:1c), Dst: ca:05:26:28:00:1c (ca:05:26:28:00:1c)
> Internet Protocol Version 4, Src: 9.9.9.9, Dst: 5.5.5.5
> Transmission Control Protocol, Src Port: 51621, Dst Port: 646, Seq: 1, Ack: 1, Len: 18
> Label Distribution Protocol
```

***Figure 50** – CUST3-R6 traceroute CUST3-R5.*

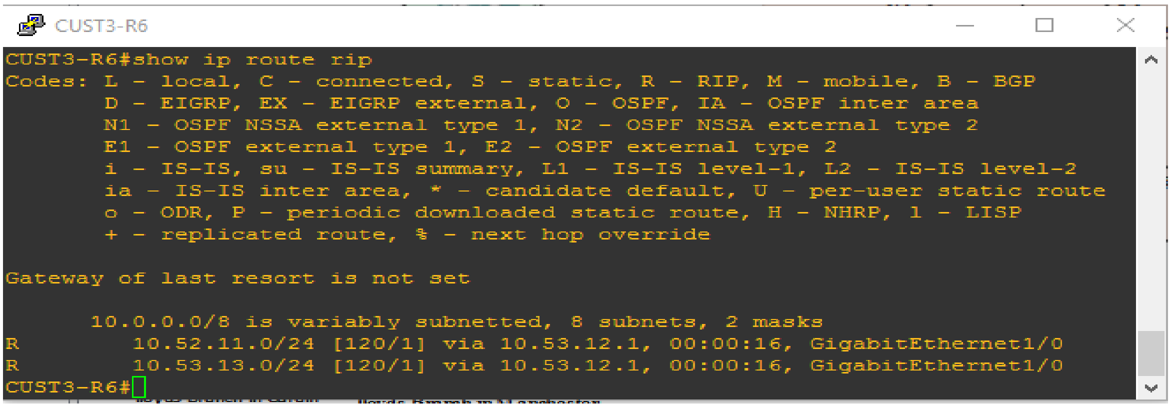
Figure 51 shows that CUST3-R6 can traceroute CUST3-R5.



CUST3-R5

```
CUST3-R5#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
R        10.53.10.0/24 [120/1] via 10.53.12.2, 00:00:14, GigabitEthernet1/0
R        10.53.22.0/24 [120/1] via 10.53.12.2, 00:00:14, GigabitEthernet1/0
CUST3-R5#
```

***Figure 51** – Show ip route rip in CUST3-R5.*



CUST3-R6

```
CUST3-R6#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
R        10.52.11.0/24 [120/1] via 10.53.12.1, 00:00:16, GigabitEthernet1/0
R        10.53.13.0/24 [120/1] via 10.53.12.1, 00:00:16, GigabitEthernet1/0
CUST3-R6#
```

***Figure 52** – Show ip route RIP in CUST3-R6.*

3.7 IP Service Level Agreements (IP SLA)

IP Service Level Agreements (IP SLA) is a tool from Cisco IOS to check the performance and quality of services and communications on the IP SLA platform. IP allows us to investigate and collect information about packet delay, packet loss, communication, jitter rate, voice quality in VoIP communications, analysis a path called hop by hop, availability of a service and etc. All of these features increase the network stability and quality of service and reduce downtime and network outages, as well as allows you to check and gather information about network performance and service quality with the tools such as “SNMP” and “CiscoWorks Internetwork Performance Monitor” and even the “third-party” software.

One of the simplest examples is the implementation of an IP SLA, tracking a path, the latency, the packet level of lasts, as well as the establishment and disconnection of a sensor that is evaluated by a sensor. This sensor sends ICMP packets to specified destinations at specified intervals, and reports the result either in the form of delay paths or as UP or Down paths.

To do it, we follow a set of steps: (1) set the "IP SLA" for the destination, to send ICMP packets in specified periods, (2) define a "schedule" for it, and (3) then "tracking object" is used to check the "up/down" of the path:

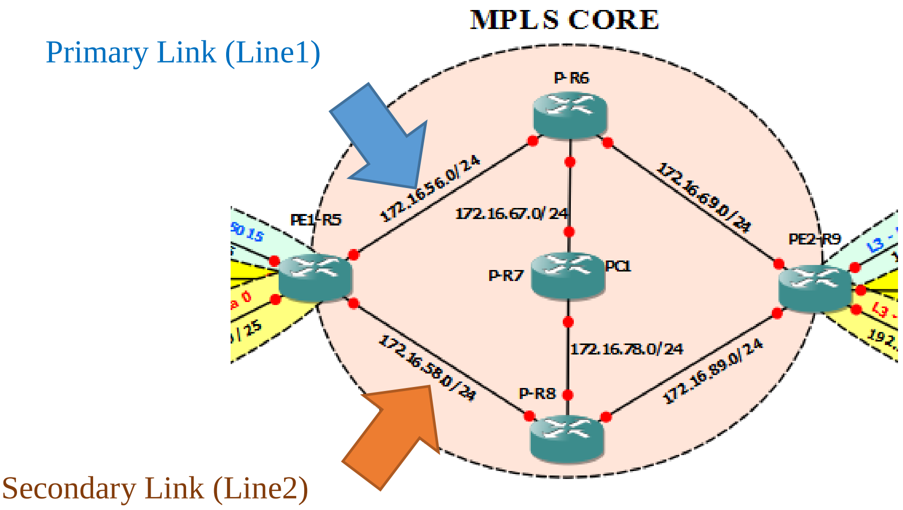


Figure 53 *– IP SLA route for the topology.*

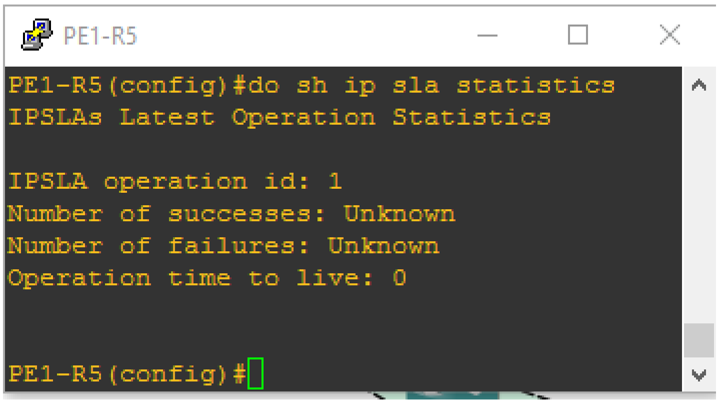
In figure 53, the “PE1-R5” device is connected to two Providers (P-R6 and P-R8). The link between PE1-R5 router and P-R6 is Primary Link (Line1) and the link between PE1-R5 router and “P-R8” is Secondary Link (Line2), as long as the "track 10" is "UP", the traffic goes to "P-R6" because of less metric, when the connection with " P-R6 " collides, "Track 10" is set to "Down" the traffic will go to "P-R8".

The IP SLA was used to monitor the connection to the P-R6 router so that it sends ICMP packets every 3 seconds with timeout of 1 second, and checks the link latency (to access availability).

To configure IP SLA in this scenario, we have to perform three phases as the following:

1. Create SLA
2. Schedule SLA
3. Attach SLA with track

3.7.1 Create SLA

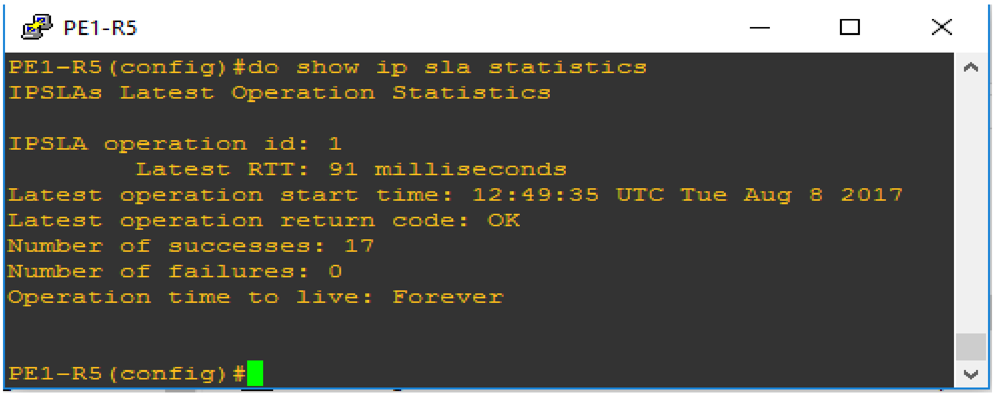


```
PE1-R5(config)#do sh ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Number of successes: Unknown
Number of failures: Unknown
Operation time to live: 0


PE1-R5(config)#
```

***Figure 54** – Create IP SLA*

3.7.2 Schedule SLA

Then, with the help of "Object Tracking", which is the Cisco IOS internal facility, we examine the "IP SLA" output:

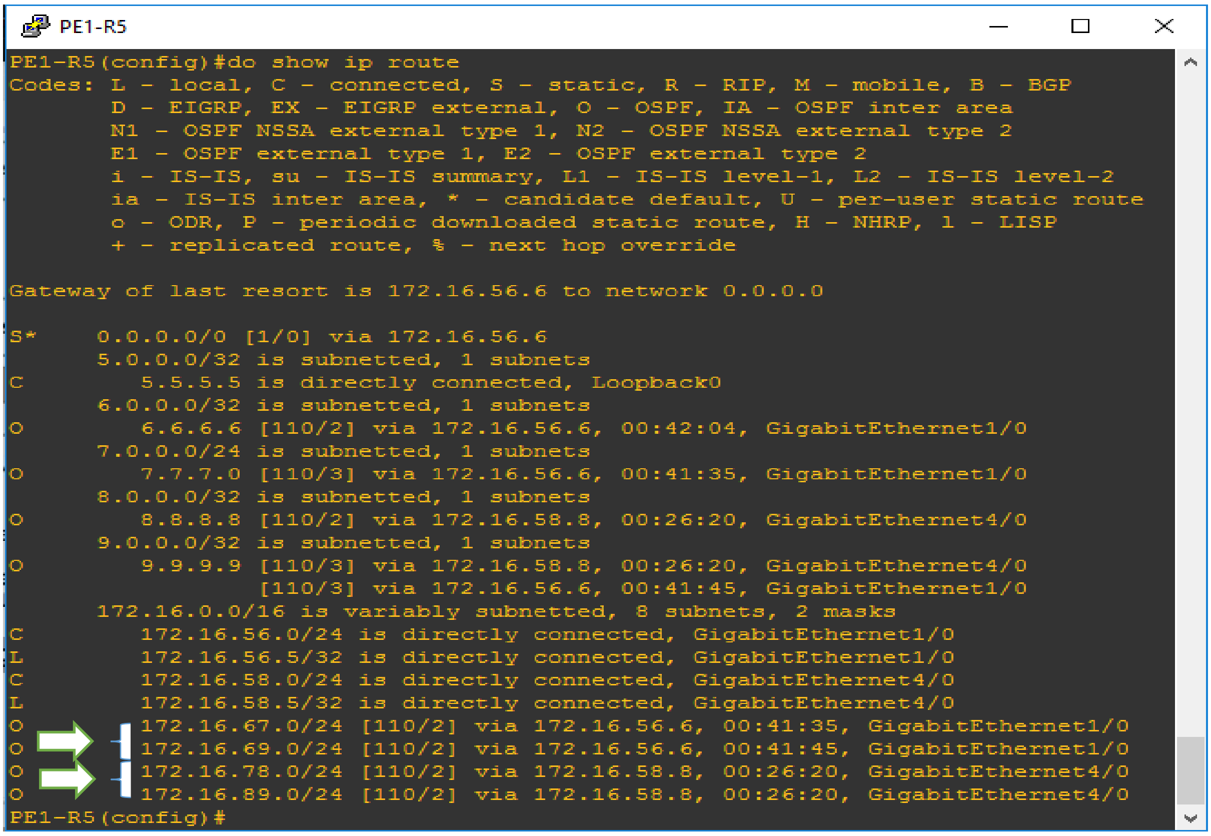


```
PE1-R5(config)#do show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: 91 milliseconds
Latest operation start time: 12:49:35 UTC Tue Aug 8 2017
Latest operation return code: OK
Number of successes: 17
Number of failures: 0
Operation time to live: Forever


PE1-R5(config)#
```

***Figure 55** – Schedule SLA.*

3.7.3 Attach SLA with track

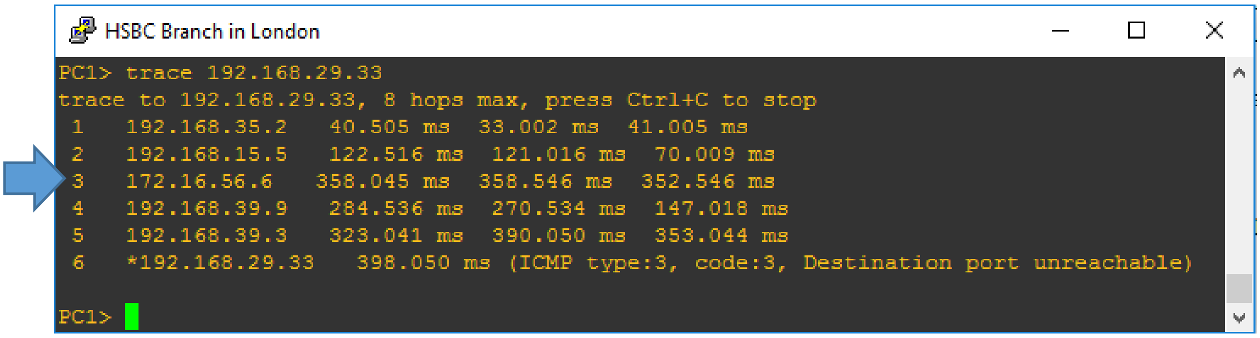
Figure 57 shows the performance of "IP SLA" as well as the "Tracker". In the route, we have two routes, one is the Primary Link and the other one is the Secondary Link. The figure shows the IP of the primary link (192.168.56.6) and the IP of Secondary Link (192.168.58.8) which display in the ip route.



```
PE1-R5(config)#do show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.56.6 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.56.6
      5.0.0.0/32 is subnetted, 1 subnets
C        5.5.5.5 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/2] via 172.16.56.6, 00:42:04, GigabitEthernet1/0
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/3] via 172.16.56.6, 00:41:35, GigabitEthernet1/0
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/2] via 172.16.58.8, 00:26:20, GigabitEthernet4/0
      9.0.0.0/32 is subnetted, 1 subnets
O        9.9.9.9 [110/3] via 172.16.58.8, 00:26:20, GigabitEthernet4/0
                 [110/3] via 172.16.56.6, 00:41:45, GigabitEthernet1/0
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.56.0/24 is directly connected, GigabitEthernet1/0
L        172.16.56.5/32 is directly connected, GigabitEthernet1/0
C        172.16.58.0/24 is directly connected, GigabitEthernet4/0
L        172.16.58.5/32 is directly connected, GigabitEthernet4/0
O        172.16.67.0/24 [110/2] via 172.16.56.6, 00:41:35, GigabitEthernet1/0
O        172.16.69.0/24 [110/2] via 172.16.56.6, 00:41:45, GigabitEthernet1/0
O        172.16.78.0/24 [110/2] via 172.16.58.8, 00:26:20, GigabitEthernet4/0
O        172.16.89.0/24 [110/2] via 172.16.58.8, 00:26:20, GigabitEthernet4/0
PE1-R5(config)#
```

***Figure 56** - IP of Primary Link and the IP of Secondary Link display in the Routing table.*

By default, traffic passes through Link1 (Primary Link). Figure 58 shows the route from “HSBC Branch in London” passes the traffic through the primary link to reach the destination “HSBC Branch in Birmingham”.

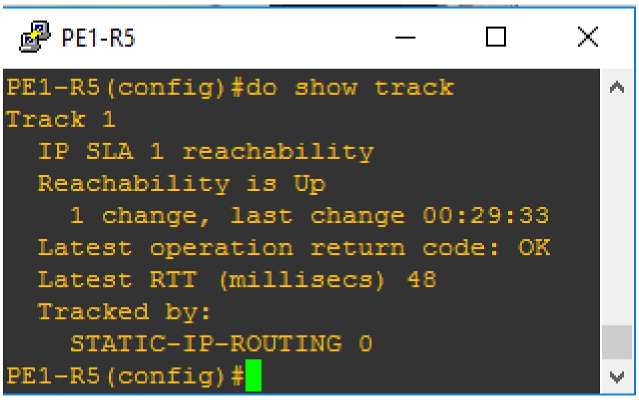


```
PC1> trace 192.168.29.33
trace to 192.168.29.33, 8 hops max, press Ctrl+C to stop
 1   192.168.35.2    40.505 ms  33.002 ms  41.005 ms
 2   192.168.15.5    122.516 ms  121.016 ms  70.009 ms
 3   172.16.56.6   358.045 ms  358.546 ms  352.546 ms
 4   192.168.39.9    284.536 ms  270.534 ms  147.018 ms
 5   192.168.39.3    323.041 ms  390.050 ms  353.044 ms
 6   *192.168.29.33   398.050 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

***Figure 57** – Traceroute from “HSBC Branch in London” to “HSBC Branch in Birmingham”.*

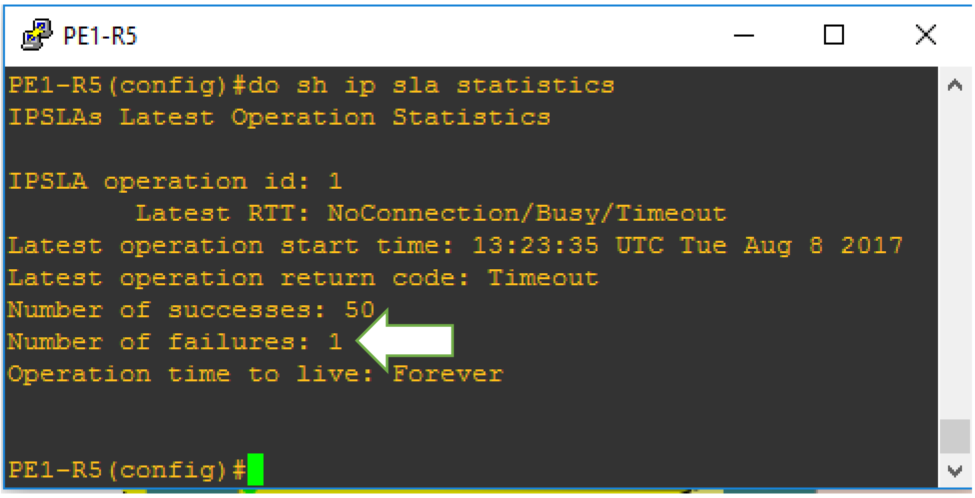
HSBC Branch in London (PC1) ➔ CE1-R1 ➔ PE1-R5 ➔ P-R6 ➔ PE2-R9 ➔ CE1-R3 ➔ HSBC Branch in Birmingham (PC3)

To change the route, we should make the Primary Link down and then the Secondary Line route will be used to forward all the traffic. To verify the track status, use the **show track** command as shown below:



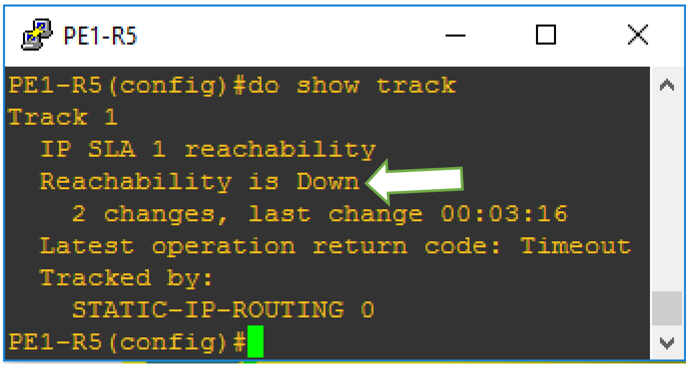
```
PE1-R5(config)#do show track
Track 1
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 00:29:33
  Latest operation return code: OK
  Latest RTT (millisecs) 48
  Tracked by:
    STATIC-IP-ROUTING 0
PE1-R5(config)#
```

Figure 58 *- Reachability is UP*



```
PE1-R5(config)#do sh ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 13:23:35 UTC Tue Aug 8 2017
Latest operation return code: Timeout
Number of successes: 50
Number of failures: 1
Operation time to live: Forever


PE1-R5(config)#
```

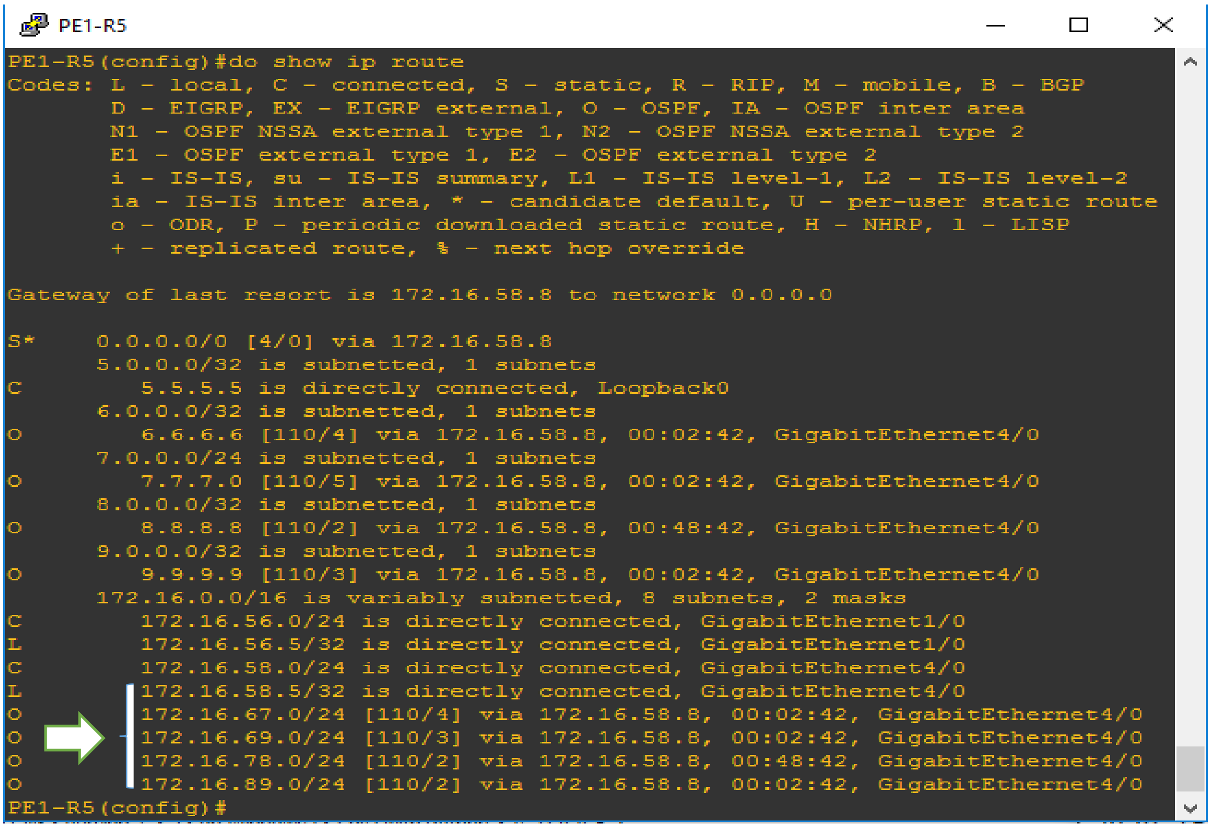
Figure 59 *– The Primary Link is DOWN.*



```
PE1-R5(config)#do show track
Track 1
  IP SLA 1 reachability
  Reachability is Down
    2 changes, last change 00:03:16
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
PE1-R5(config)#
```

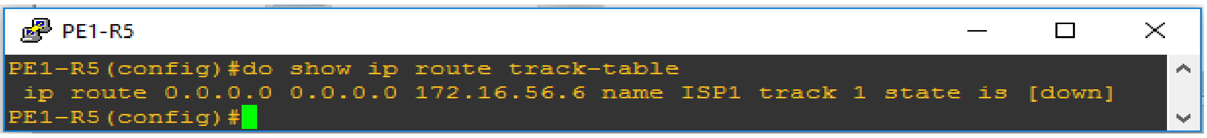
Figure 60 *- Reachability is Down*

In figures 61 and 62 we observe that Port g1/0 is *shutdown* and the IP address is removed from the ip route table and secondary route is up now.



```
PE1-R5(config)#do show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.58.8 to network 0.0.0.0

S*    0.0.0.0/0 [4/0] via 172.16.58.8
      5.0.0.0/32 is subnetted, 1 subnets
C        5.5.5.5 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/4] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/5] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/2] via 172.16.58.8, 00:48:42, GigabitEthernet4/0
      9.0.0.0/32 is subnetted, 1 subnets
O        9.9.9.9 [110/3] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.56.0/24 is directly connected, GigabitEthernet1/0
L        172.16.56.5/32 is directly connected, GigabitEthernet1/0
C        172.16.58.0/24 is directly connected, GigabitEthernet4/0
L        172.16.58.5/32 is directly connected, GigabitEthernet4/0
O        172.16.67.0/24 [110/4] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
O        172.16.69.0/24 [110/3] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
O        172.16.78.0/24 [110/2] via 172.16.58.8, 00:48:42, GigabitEthernet4/0
O        172.16.89.0/24 [110/2] via 172.16.58.8, 00:02:42, GigabitEthernet4/0
PE1-R5(config)#
```

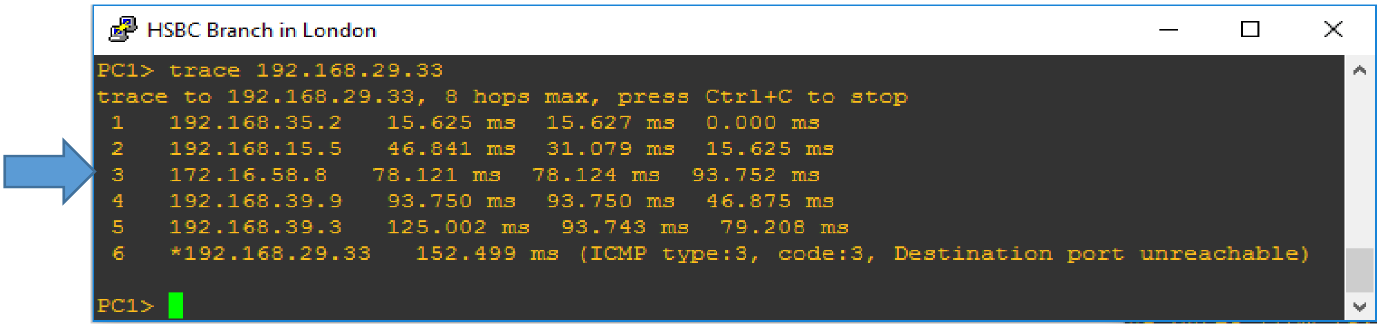
***Figure 61** – The ip address of the Primary Link is removed from the ip route table.*



```
PE1-R5(config)#do show ip route track-table
 ip route 0.0.0.0 0.0.0.0 172.16.56.6 name ISP1 track 1 state is [down]
PE1-R5(config)#
```

***Figure 62** – The Primary Link is DOWN.*

Link1 (Primary Link) is down now and the path is changed from P-R6 to P-R8 now. Figure 63 shows the route from "HSBC Branch in London", passing the traffic through the Line2 (Secondary Link) to reach the destination "HSBC Branch in Birmingham".



```
PC1> trace 192.168.29.33
trace to 192.168.29.33, 8 hops max, press Ctrl+C to stop
 1   192.168.35.2    15.625 ms  15.627 ms  0.000 ms
 2   192.168.15.5    46.841 ms  31.079 ms  15.625 ms
 3   172.16.58.8   78.121 ms  78.124 ms  93.752 ms
 4   192.168.39.9    93.750 ms  93.750 ms  46.875 ms
 5   192.168.39.3    125.002 ms  93.743 ms  79.208 ms
 6   *192.168.29.33   152.499 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

***Figure 63** – Traceroute from "HSBC Branch in London" to "HSBC Branch in Birmingham".*

HSBC Branch in London (PC1) ➔ CE1-R1 ➔ PE1-R5 ➔ P-R8 ➔ PE2-R9 ➔ CE1-R3 ➔ HSBC Branch in Birmingham (PC3)

3.8 Conclusions for the simulation scenario

The subject of Chapter 3 was the implementation and design of the MPLS Layer 3 and Layer 2 VPN which are the most significant applications of the MPLS with various protocols, for example, BGP, RIP and OSPF. In order to accomplish the implementation of a MPLS Layer 3 or Layer 2 VPN, some essential data is required from the PE routers.

In MPLS Layer 3 VPN, all packets are forwarded with the IGP label at the highest point of the label stack and the VPN label on the basis of the stack.

With Layer 3 VPN service you connect with your MPLS provider at layer 3. Consequently, you will have to run IP services with your provider. Subsequently you will peer up with your provider utilizing a Routing Protocol and participate in route exchange. The MPLS provider will then send these routes to their remote PE and then advertise these routes to your remote site at Layer 3. At the remote site you would also peer up with Layer 3 to your provider and have this routes advertised to you. So in this scenario, your two remote site routers will not show up as directly connected [2, 13].

In a MPLS Layer 2 VPN service, you do not run any routing or any IP services with your MPLS provider when you connect to it [9, 12].

CHAPTER FOUR

4. Result and Discussion:

4.1 Test the network with iperf and jperf tools

A network can be measured using various tools available on different operating systems. Bandwidth test software is used to determine the maximum bandwidth Internet connection or network. This usually happens by downloading or uploading the maximum amount of data in a given period of time, or a certain amount of data in a minimum amount of time. Because of this, bandwidth tests can delay data transfers over Internet connections that run tests, as well as load congestion. A more precise method is to use dedicated software (like iperf) to measure the maximum throughput of a network access link.

Here is a diagram that iperf and jperf installed on a two virtual machines. jperf is a graphical frontend for iperf written in Java. To test the network, one of the machine is used as the iperf client and the other machine as the iperf server.

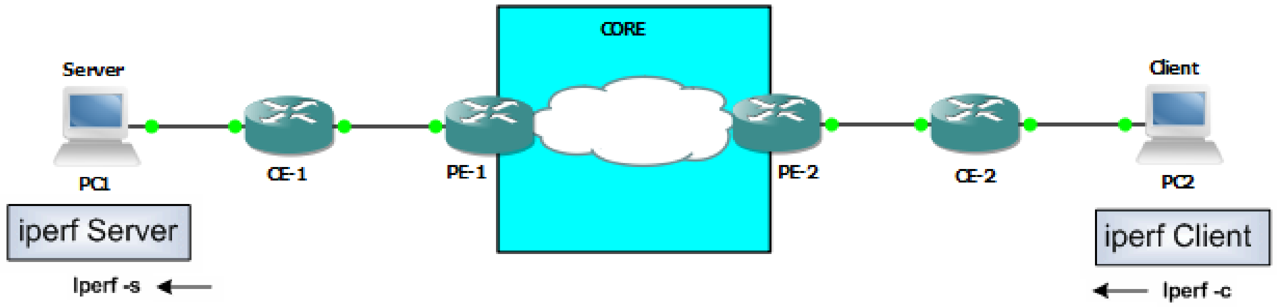
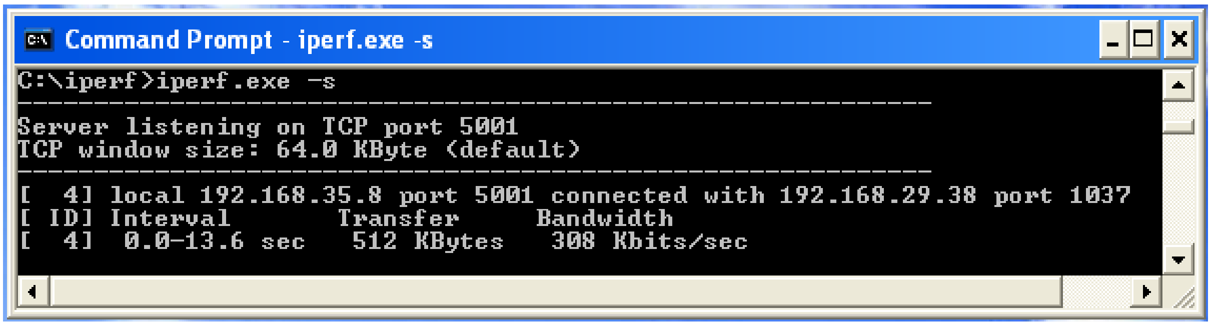


Figure 64 *- Diagram of performance of iperf in the network*

By default, the iperf client connects to the iperf server on the TCP port 5001 and the bandwidth displayed by iperf is the bandwidth from the client to the server.

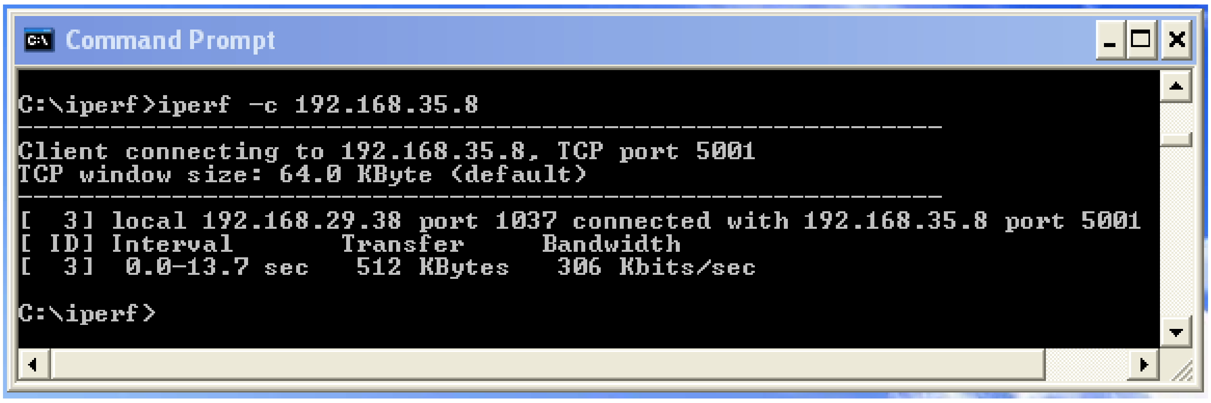
We have three Customers with three different protocols, a **BGP** in the top, **RIP** in the middle and **OSPF** at the bottom that I am going to use iperf and jperf softwares to measure the traffic and bandwidth in the network.

4.1.1 Customer 1 with BGP Protocol (Layer3):



```
C:\iperf>iperf.exe -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local 192.168.35.8 port 5001 connected with 192.168.29.38 port 1037
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-13.6 sec   512 KBytes   308 Kbits/sec
```

***Figure 65** - Bandwidth from the server to the client*

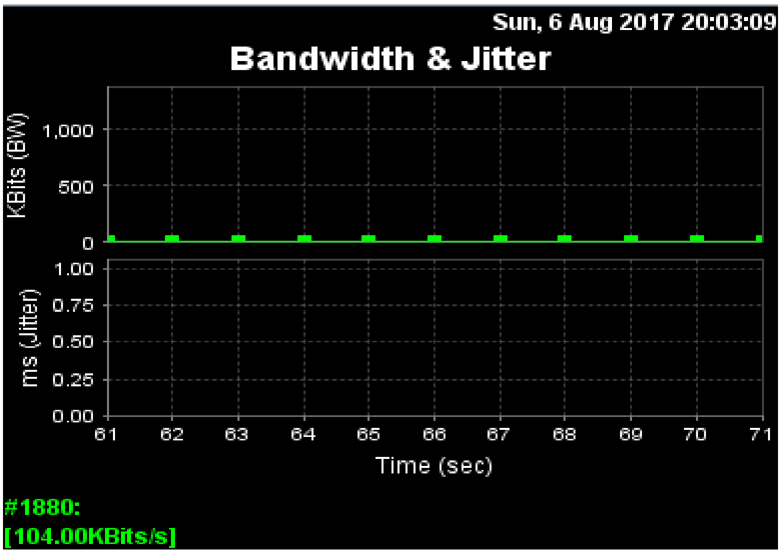


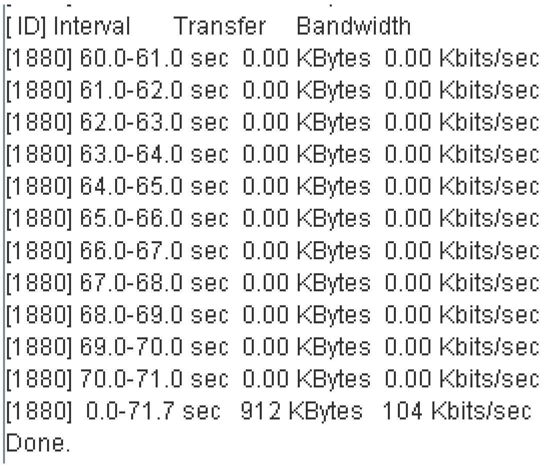
```
C:\iperf>iperf -c 192.168.35.8
------------------------------------------------------------
Client connecting to 192.168.35.8, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.29.38 port 1037 connected with 192.168.35.8 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-13.7 sec   512 KBytes   306 Kbits/sec

C:\iperf>
```

***Figure 66** - Bandwidth from the client to the server.*

As can be seen in figures 65 and 66, between two points A (PC1) and B (PC2), traffic was transferred at 512 KBytes and the actual bandwidth was between 306 Kbits/sec and all transaction was done within 13.7 seconds.

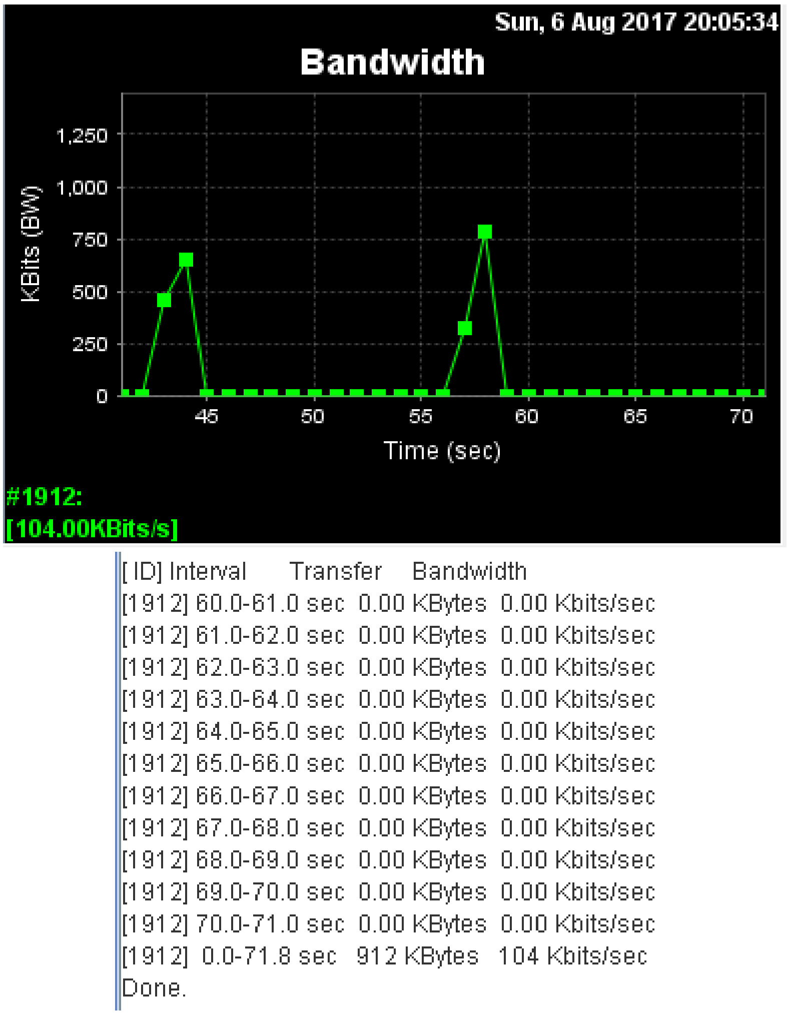
As can be seen in figures 67 and 68, jperf draws and updates the graph as each transmission is received within 60 seconds TCP test. The test will give you the average throughput on the last data string in the output file below. It will look like this.





```
[ ID] Interval       Transfer     Bandwidth
[1880] 60.0-61.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 61.0-62.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 62.0-63.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 63.0-64.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 64.0-65.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 65.0-66.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 66.0-67.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 67.0-68.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 68.0-69.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 69.0-70.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880] 70.0-71.0 sec  0.00 KBytes  0.00 Kbits/sec
[1880]  0.0-71.7 sec   912 KBytes   104 Kbits/sec
Done.
```

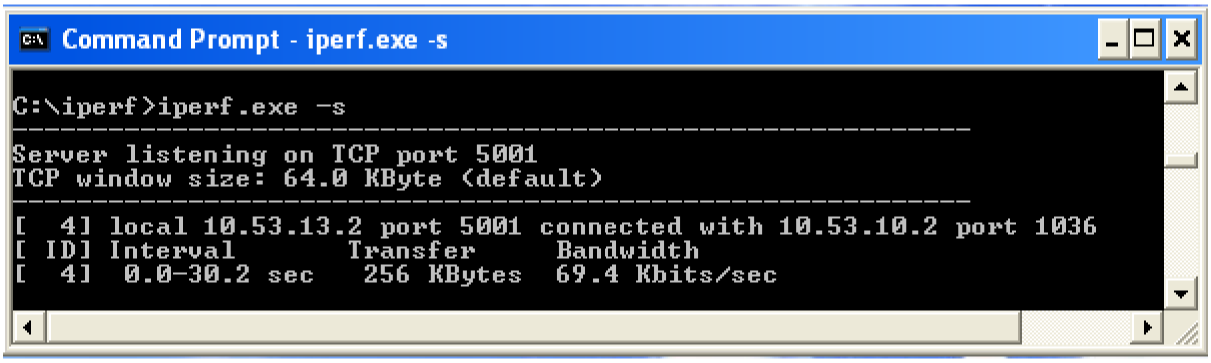
Figure 67 *- Result of running TCP parameters in server mode.*



```
[ ID] Interval       Transfer     Bandwidth
[1912] 60.0-61.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 61.0-62.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 62.0-63.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 63.0-64.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 64.0-65.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 65.0-66.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 66.0-67.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 67.0-68.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 68.0-69.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 69.0-70.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912] 70.0-71.0 sec  0.00 KBytes  0.00 Kbits/sec
[1912]  0.0-71.8 sec   912 KBytes   104 Kbits/sec
Done.
```

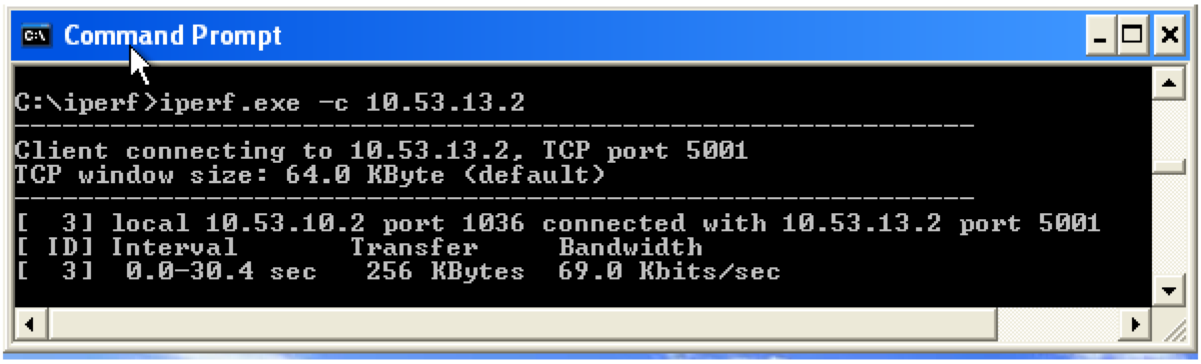
Figure 68 *- Result of running TCP parameters in client mode.*

4.1.2 Customer 2 with RIP Protocol (Layer 2)



```
C:\iperf>iperf.exe -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local 10.53.13.2 port 5001 connected with 10.53.10.2 port 1036
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-30.2 sec   256 KBytes  69.4 Kbits/sec
```

***Figure 69** - Bandwidth from the server to the client.*

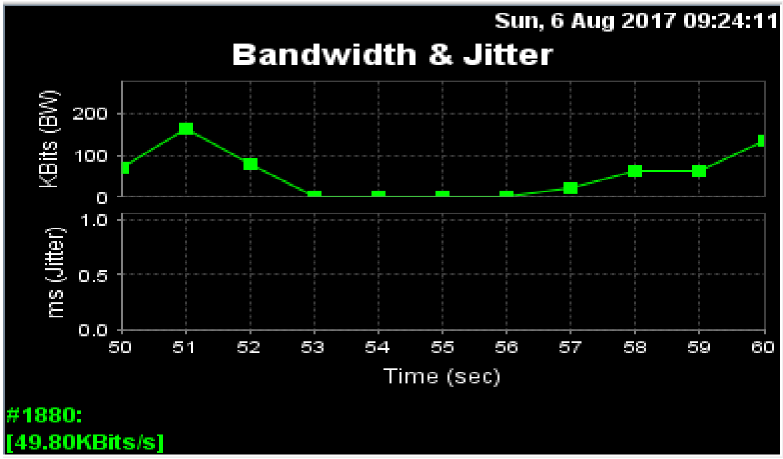


```
C:\iperf>iperf.exe -c 10.53.13.2
------------------------------------------------------------
Client connecting to 10.53.13.2, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 10.53.10.2 port 1036 connected with 10.53.13.2 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-30.4 sec   256 KBytes  69.0 Kbits/sec
```

***Figure 70** - Bandwidth from the client to the server.*

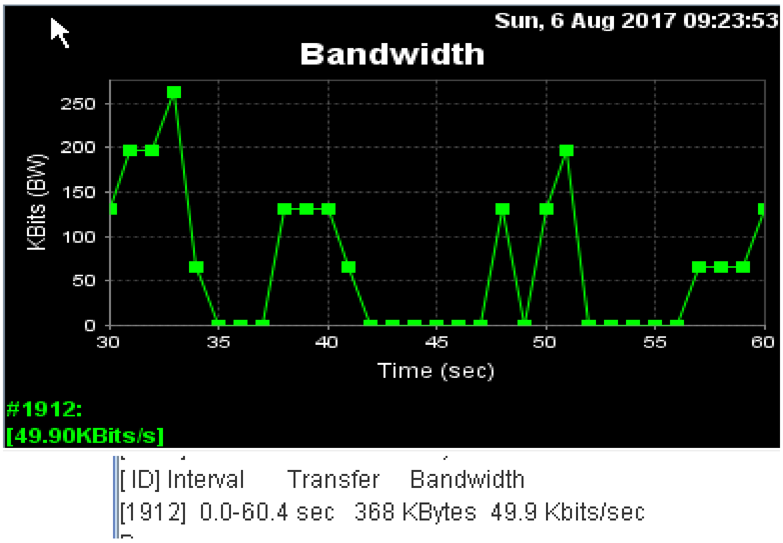
Between points A and B, traffic was transferred at 256 KBytes and the actual bandwidth was between 69.0 Kbits/sec and all transaction was done within 30.4 seconds.

As can be seen in the figures 71 and 72, jperf draws and updates the graph as each transmission is received within 60 seconds TCP test. The output window below the graph provides the numbers used to draw the graph.



```
[ ID] Interval      Transfer     Bandwidth
[1880]  0.0-60.5 sec   368 KBytes  49.8 Kbits/sec
```

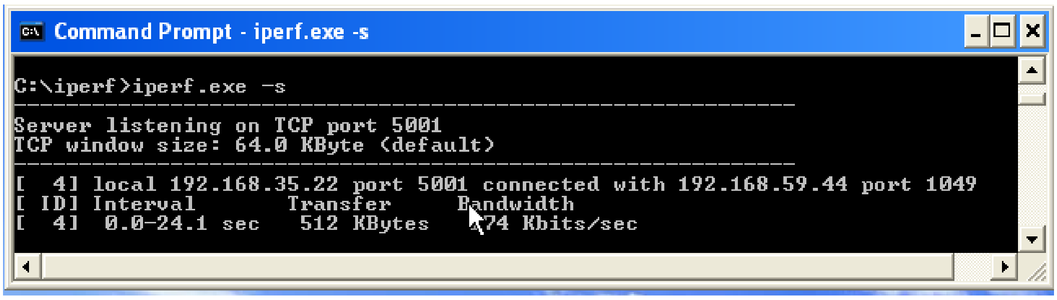
***Figure 71** - Result of running TCP parameters in server mode.*



```
[ ID] Interval      Transfer     Bandwidth
[1912]  0.0-60.4 sec   368 KBytes  49.9 Kbits/sec
```

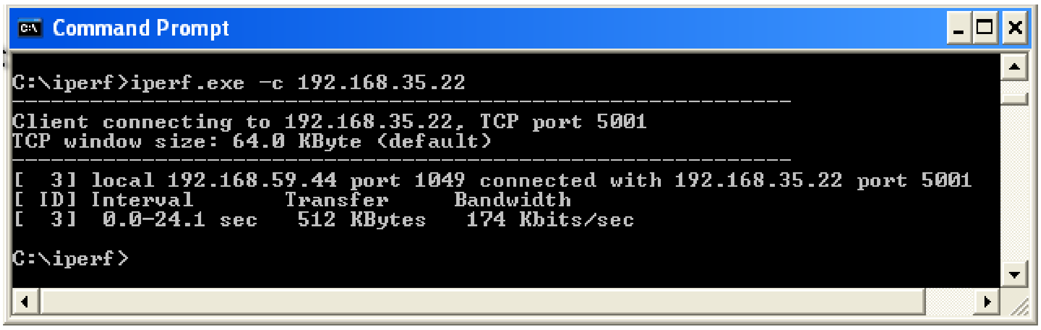
Figure 72 - *Result of running TCP parameters in client mode.*

4.1.3 Customer 3 with OSPF Protocol (Layer 3)



```
C:\iperf>iperf.exe -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local 192.168.35.22 port 5001 connected with 192.168.59.44 port 1049
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-24.1 sec   512 KBytes   174 Kbits/sec
```

Figure 73 - *Bandwidth from the server to the client.*



```
C:\iperf>iperf.exe -c 192.168.35.22
------------------------------------------------------------
Client connecting to 192.168.35.22, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.59.44 port 1049 connected with 192.168.35.22 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-24.1 sec   512 KBytes   174 Kbits/sec

C:\iperf>
```

Figure 74 - *Bandwidth from the client to the server.*

As you can see in the figures 73 and 74, between two points A and B, traffic was transferred at 512 KBytes and the actual bandwidth was between 174 Kbits/sec and all transaction was done within 24.1 seconds.

Figures 75 and 76 shows the bandwidth and jitter of each transmission when received within 60 seconds TCP test. The output window below the graph provides the numbers used to draw the graph.

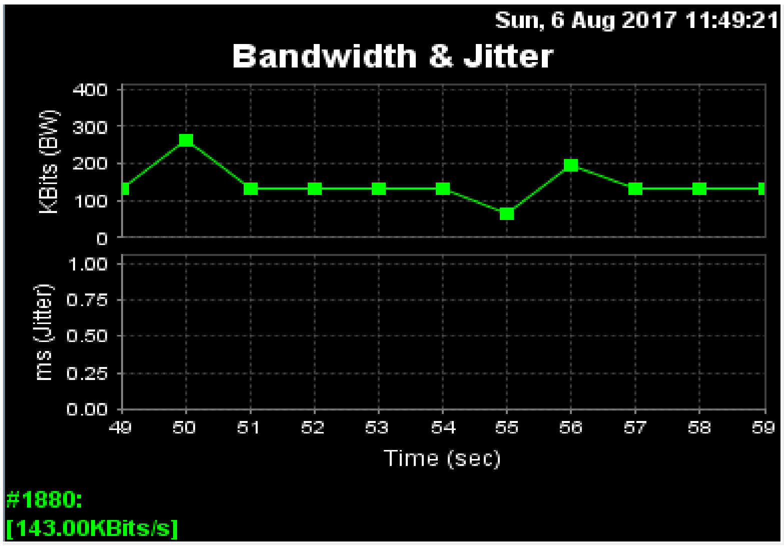
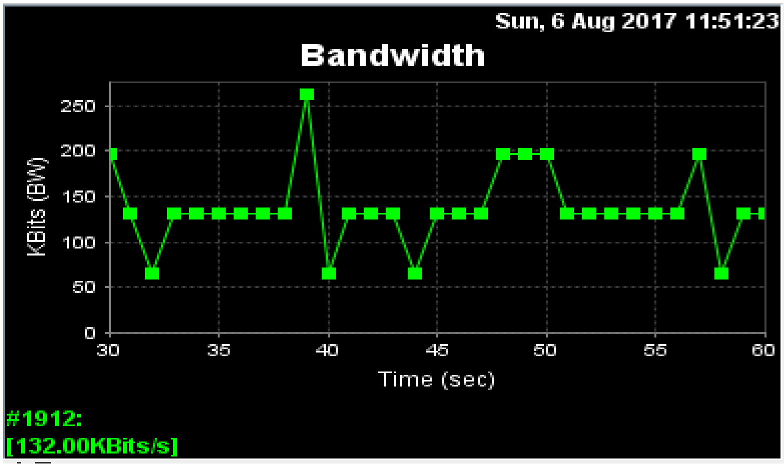
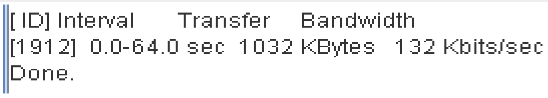


Figure 75 *- Result of running TCP parameters in server mode.*





```
[ ID] Interval       Transfer     Bandwidth
[1912]  0.0-64.0 sec  1032 KBytes   132 Kbits/sec
Done.
```

Figure 76 *- Result of running TCP parameters in client mode.*

After finishing the tests between customers with different protocols, the results show the following.

Customer	Interval	Transfer	Bandwidth
Customer 1 with BGP Protocol (Layer3):	13.7 sec	512 Kbytes	306 Kbits/sec
Customer 2 with RIP Protocol (Layer 2):	30.4 sec	256 Kbytes	69 Kbits/sec
Customer 3 with OSPF Protocol (Layer 3):	24.1 sec	512 Kbytes	174 Kbits/sec

Table 2 *- Results of Interval, Transfer and Bandwidth in iperf software.*

4.2 Comparing the Transfer and Bandwidth of throughput

As can be seen in the general diagram of performance of iperf in the network Figure 64 and throughput of a network Figure 77, considering the customer 1 with **BGP** protocol, the interval to send and receive is 13.7 second which is faster than the other two customers but the transfer is equal to Customer 3 and also has more bandwidth and it is faster than the other two customers. Customer 3 with **OSPF** protocol at the bottom has an average speed and bandwidth. Customer 2 with **RIP** protocol in the middle is very slow compared to the other two networks.

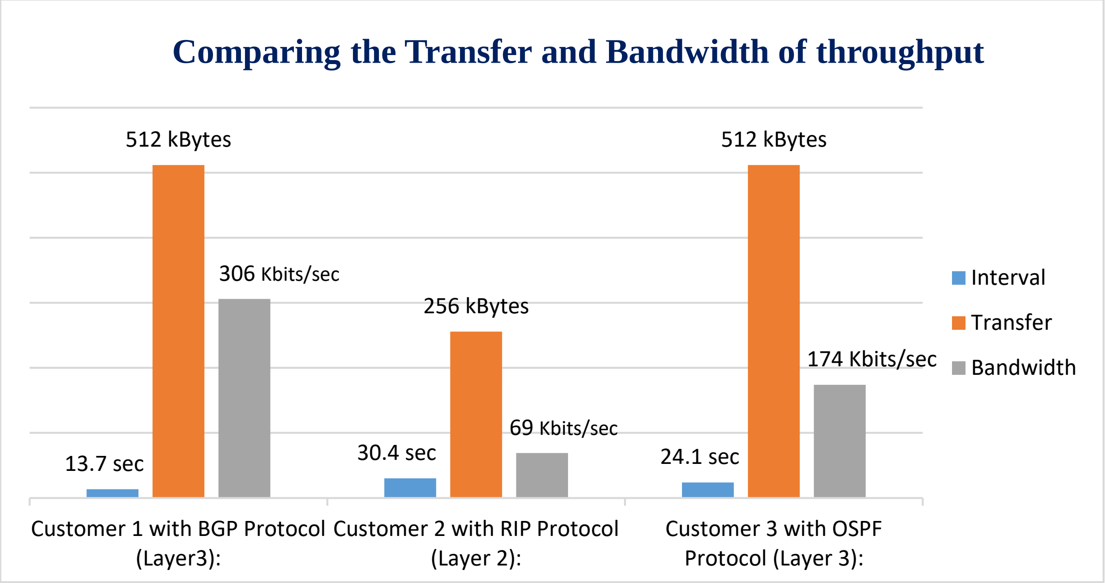


Figure 77 *- Comparing Interval, Transfer and Bandwidth of throuput.*

CHAPTER FIVE

5. Conclusions and Future Work

The objective of my thesis was to configure, to design, to implement and to verify Layer 3 and Layer 2 VPNs using MPLS. Both Layer 3 and Layer 2 topologies were compared to determine the main advantages and disadvantages such as bandwidth, traffic and speed between them.

MPLS is a standards-based technology used to speed up the delivery of network packets over multiple protocols and supplies great performance with its label switching technique. It likewise has the capability to make VPNs at both Layer 2 and Layer 3. In Layer 3 MPLS VPN, CE shares the routing table information with the PE router. However, in Layer 2 MPLS VPN, ISP acts similar to a Layer 2 Switch and is utilised just to forward the packets from one CE to another.

MPLS has benefits like, predictability, manageability and adaptability. MPLS enhances the versatility of routing and forwarding and gives traffic engineering abilities for better network provisioning. The MPLS infrastructure gives at any level of security as an equivalent ATM or Frame-Relay service. It would be a good decision for providing VPN [3].

This thesis did not include the security of the MPLS Layer 3 and Layer 2 VPNs, but from the Network Topology perspective (see Figure 5), is a site-to-site VPN that allows offices in multiple fixed locations to establish secure connections, provide a secure mechanism for encrypting and encapsulating private network traffic and moving it through an intermediate network with each other over a public network. And also the site-to-site VPN extends the secure private network traffic over an unsecured network and VPNs are an excellent way to maintain privacy and avoid transmitting sensitive data over public networks, which is in real life condition is one of the major important components in the VPNs.

The project was a skeleton of a bigger MPLS VPN network, and what was considered here was the designing, implementation, verification and the eventual troubleshooting of the MPLS Layer 3 and Layer 2 VPNs between the specified Cisco routers. After design and implementation of VPN MPLS technology, it helped me how to create a private network across a public network (e.g., the Internet). 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. A VPN is created by using dedicated connections, like virtual tunnelling protocols or traffic encryption.

The challenges that were accomplished or solved in the thesis were making of MPLS Layer 3 and Layer 2 VPNs and to further ensure the ability of routers and to ensure the eventual traversal of traffic from each side of the CE to the other. Although, the project covers simple details related to the Layer 3 and Layer 2 VPNs, which can verify significant to beginners who might want to better understand or expand their knowledge when it comes to understanding VPNs.

The VPNs made by the MPLS innovation and technology give an expanded level of protection of corporate information from the danger of spyware, as traffic between points belonging to the VPN is totally isolated from the traffic of different VPNs. With a specific end goal to achieve the objective of isolation, the MPLS standard demands each MPLS VPN having its own routing table and also the doors that are directly fixed to belong to it.

6. References

1) Networking Solutions: MPLS and VPNs - wseas.us, *www.wseas.us/e-library/conferences/2009/budapest/MIV-SSIP/MIV-SSIP30.pdf*

2) Layer 3 MPLS VPN Enterprise Consumer Guide Version 2 - Cisco, http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html

3) Multiprotocol Label Switching (MPLS), http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwj5u-j3ktnUAhWKL1AKHfOVBQQQFghUMAQ&url=http%3A%2F%2Ftele1.dee.fct.unl.pt%2Frit1_2016_2017%2Fpages%2FIEC_MPLS.pdf&usg=AFQjCNFtiKXAh3hcy0nKX-Fa5W8KqJr4ag

4) Leased Line vs VPN - Which Technology Is Right For YOUR Business ..., https://www.google.pt/search?q=VPN+based+on+leased+lines&sourceid=ie7&rls=com.microsoft:en-GB:IE-Address&ie=&oe=&gfe_rd=cr&ei=ZBhRWbioCa-C3gO4opXwCg

5) Network design with guaranteed End-to-End QoS, http://projekter.aau.dk/projekter/files/77301510/AAU_MPLS_Thesis_Final_060613.pdf

6) MPLS Overview, http://flylib.com/books/en/2.686.1.15/1/

7) Comparison between Traditional IP Networks/Routing and MPLS, http://www.ijser.in/archives/v3i3/IJSER1516.pdf

8) How VPN Works, https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx

9) MPLS Virtual Private Networks - Old Dog Consulting, *www.olddog.co.uk/mplsvpns.pdf*

10) MPLS Layer 2 VPNs Configuration Guide, Cisco IOS XE Everest, *http://www.cisco.com/c/en/us/td/docs/routers/ncs4200/configuration/guide/mpls/b-mp-l2-vpns-16-5-1-ncs4200.pdf*

11) Cisco - Implementing Managed IP Virtual Private Network Services, *http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/outso_wp.htm*

12) Implementing Point to Point Layer 2 Services - Cisco, https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-1/lxvpn/configuration/guide/lesc41/lesc41p2ps.pdf

13) Layer 2 vs. Layer 3 MPLS - The GCOMM Post, *http://www.thegcommpost.com.au/layer-2-vs-layer-3-mpls/*

14) Comparative Analysis of MPLS Layer 3vpn and MPLS Layer 2 ... - IJCST, http://www.ijcstjournal.org/volume-3/issue-3/IJCST-V3I3P37.pdf

15) MPLS WAN Technology Design Guide—December 2013 - Cisco, http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2013/CVD-

16) Technical Whitepaper on MPLS L3VPN - ZTE, http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjB29zt3dvUAhXSmLQKHWnCCNwQFghJMAQ&url=http%3A%2F%2Fwwwen.zte.com.cn%2Fen%2Fproducts%2Fbearer%2F201308%2FP020130828527155850511.pdf&usg=AFQjCNEsW1_n8TSG3YjZ39mqLVQMiGotIw

17) MPLS and VPLS Security - Black Hat, https://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rey-up.pdf

18) Implementing MPLS Layer 3 VPNs - Cisco, http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj2k-bZ39vUAhUGKFAKHZOfBrcQFggwMAE&url=http%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Frouters%2Fcrs%2Fsoftware%2Fcrs_r4-1%2Flxvpn%2Fconfiguration%2Fguide%2Fvc41crs%2Fvc41v3.pdf&usg=AFQjCNFNZ5sOGyTYl-WeNn_6JluTCFmmzg

19) Implementing Point to Point Layer 2 Services - Cisco, https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-1/lxvpn/configuration/guide/lesc41/lesc41p2ps.pdf

20) *Network design with guaranteed End-to-End QoS*, http://projekter.aau.dk/projekter/files/77301510/AAU_MPLS_Thesis_Final_060613.pdf

21) *Demystifying Layer2 and Layer3 VPNs*, http://marketclarity.com.au/wp-content/uploads/2013/07/DemystifyingLayer2andLayer3VPNs.pdf

22) https://en.wikipedia.org/wiki/Virtual_private_network

23) https://smallbiztrends.com/2013/09/osi-model-layer-networking.html

24) http://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-ex-series-vpn-layer2-layer3.html

7. Appendix

Configuration of each device

==

P-R6

==

```
P-R6#show run
hostname P-R6
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
!
mpls label range 600 699
mpls label protocol ldp
multilink bundle-name authenticated
!
ip tcp synwait-time 5
pseudowire-class PW-IAS1
 encapsulation mpls
!
interface Loopback0
 ip address 6.6.6.6 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet1/0
 ip address 172.16.56.6 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 172.16.67.6 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
```

```
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet5/0
 ip address 172.16.69.6 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet6/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 router-id 6.6.6.6
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

P-R6#
=====================================================================
```

P-R7

```
=====================================================================

P-R7#show run
hostname P-R7
!
boot-start-marker
boot-end-marker
```

```
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
!
mpls label range 700 799
mpls label protocol ldp
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 7.7.7.7 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 172.16.67.7 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet5/0
 ip address 172.16.78.7 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet6/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 router-id 7.7.7.7
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig
 mpls ldp autoconfig area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
P-R7#
```

==

P-R8

==

```
P-R8#show run
Building configuration...

Current configuration : 1568 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname P-R8
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
mpls label range 800 899
mpls label protocol ldp
```

```
multilink bundle-name authenticated
!
ip tcp synwait-time 5
pseudowire-class PW-IAS1
 encapsulation mpls
!
interface Loopback0
 ip address 8.8.8.8 255.255.255.0
 ip ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 ip address 172.16.78.8 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet4/0
 ip address 172.16.58.8 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
!
interface GigabitEthernet5/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet6/0
 ip address 172.16.89.8 255.255.255.0
 negotiation auto
!
router ospf 1
 router-id 8.8.8.8
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig
 mpls ldp autoconfig area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
```

```
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

P-R8#
```

===

PE1-R5

===

```
PE1-R5#show running-config
Building configuration...

Current configuration : 2895 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname PE1-R5
!
boot-start-marker
boot-end-marker
!
vrf definition CUST-A
 rd 15:39
 !
 address-family ipv4
  route-target export 15:39
  route-target import 15:39
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition CUST-B
 rd 200:2
 !
 address-family ipv4
  route-target export 200:2
  route-target import 200:2
 exit-address-family
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
mpls label range 500 599
mpls label protocol ldp
multilink bundle-name authenticated
!
ip tcp synwait-time 5
pseudowire-class PW-IAS1
 encapsulation mpls
!
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 vrf forwarding CUST-A
 ip address 192.168.15.5 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 vrf forwarding CUST-B
 ip address 192.168.25.5 255.255.255.0
 ip ospf 25 area 0
 speed auto
 duplex auto
!
interface GigabitEthernet1/0
 ip address 172.16.56.5 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 mpls ip
!
interface GigabitEthernet2/0
 no ip address
 negotiation auto
 no keepalive
 xconnect 9.9.9.9 101 encapsulation mpls
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 ip address 172.16.58.5 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 mpls ip
!
interface GigabitEthernet5/0
 no ip address
 shutdown
 negotiation auto
```

```
!
interface GigabitEthernet6/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 25 vrf CUST-B
 router-id 192.168.25.5
 domain-id 0.0.0.10
 ispf
 redistribute bgp 59 metric 9 subnets
!
router ospf 1
 router-id 5.5.5.5
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig area 0
!
router bgp 59
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 9.9.9.9 remote-as 59
 neighbor 9.9.9.9 update-source Loopback0
 !
 address-family ipv4
  neighbor 9.9.9.9 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 9.9.9.9 activate
  neighbor 9.9.9.9 send-community both
 exit-address-family
 !
 address-family ipv4 vrf CUST-A
  neighbor 192.168.15.1 remote-as 15
  neighbor 192.168.15.1 activate
 exit-address-family
 !
 address-family ipv4 vrf CUST-B
  redistribute ospf 25 match internal external 1 external 2 nssa-external 1 nssa-external 2
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 100 deny   udp any any eq 646
access-list 100 permit ip any any
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

PE1-R5#
==============================================================================
```

PE1-R9

```
==============================================================================

PE2-R9#show running-config
Building configuration...

Current configuration : 2819 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname PE2-R9
!
boot-start-marker
boot-end-marker
!
vrf definition CUST-A
 rd 15:39
 !
 address-family ipv4
  route-target export 15:39
  route-target import 15:39
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition CUST-B
 rd 200:2
 !
 address-family ipv4
  route-target export 200:2
  route-target import 200:2
 exit-address-family
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
```

```
!
mpls label range 900 999
mpls label protocol ldp
multilink bundle-name authenticated
!
ip tcp synwait-time 5
pseudowire-class PW-IAS1
 encapsulation mpls
!
interface Loopback0
 ip address 9.9.9.9 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 vrf forwarding CUST-A
 ip address 192.168.39.9 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 vrf forwarding CUST-B
 ip address 192.168.49.9 255.255.255.0
 ip ospf 49 area 0
 speed auto
 duplex auto
!
interface GigabitEthernet1/0
 no ip address
 negotiation auto
 no keepalive
 xconnect 5.5.5.5 101 encapsulation mpls
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet5/0
 ip address 172.16.69.9 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 mpls ip
!
interface GigabitEthernet6/0
 ip address 172.16.89.9 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 mpls ip
```

```
!
router ospf 49 vrf CUST-B
 router-id 192.168.49.9
 domain-id 0.0.0.10
 ispf
 redistribute bgp 59 metric 9 subnets
!
router ospf 1
 router-id 9.9.9.9
 network 0.0.0.0 255.255.255.255 area 0
 mpls ldp sync
 mpls ldp autoconfig area 0
!
router bgp 59
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 5.5.5.5 remote-as 59
 neighbor 5.5.5.5 update-source Loopback0
 !
 address-family ipv4
  neighbor 5.5.5.5 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community both
 exit-address-family
 !
 address-family ipv4 vrf CUST-A
  neighbor 192.168.39.3 remote-as 39
  neighbor 192.168.39.3 activate
 exit-address-family
 !
 address-family ipv4 vrf CUST-B
  redistribute ospf 49 match internal external 1 external 2 nssa-external 1 nssa-external 2
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
```

```
!
end

PE2-R9#
==========================================================================
```

CUST1-R1

```
==========================================================================

CUST1-R1#show run
hostname CUST1-R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.15.1 255.255.255.0
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.35.2 255.255.255.0
 duplex full
!
router bgp 15
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 192.168.15.5 remote-as 59
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.15.5 activate
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
```

```
end

CUST1-R1#
```

===

CUST2-R2

===

```
CUST2-R2#show run
Building configuration...

Current configuration : 792 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CUST2-R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
 ip ospf 25 area 0
!
interface FastEthernet0/0
 ip address 192.168.35.3 255.255.255.0
 ip ospf 25 area 0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.25.2 255.255.255.0
 ip ospf 25 area 0
 speed auto
 duplex auto
!
router ospf 25
 router-id 10.1.1.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
```

```
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end

CUST2-R2#
```

===

CUST2-R3

===

```
CUST1-R3#show run
hostname CUST1-R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.39.3 255.255.255.0
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.29.4 255.255.255.0
 duplex full
!
router bgp 39
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 192.168.39.9 remote-as 59
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.39.9 activate
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
```

```
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end

CUST1-R3#
================================================================
```

CUST1-R4

```
================================================================

CUST2-R4#show run
Building configuration...

Current configuration : 992 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CUST2-R4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 10.3.3.3 255.255.255.255
 ip ospf 49 area 0
!
interface FastEthernet0/0
 ip address 192.168.59.4 255.255.255.0
 ip ospf 49 area 0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.49.4 255.255.255.0
 ip ospf 49 area 0
 speed auto
 duplex auto
!
```

```
router ospf 49
 router-id 10.3.3.3
 ispf
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

CUST2-R4#
===========================================================================
```

CUST3-R5

```
===========================================================================

CUST3-R5#show running-config
Building configuration...

Current configuration : 931 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CUST3-R5
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
```

```
interface Loopback0
 ip address 10.52.11.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.53.13.1 255.255.255.0
 duplex full
!
interface GigabitEthernet1/0
 ip address 10.53.12.1 255.255.255.0
 negotiation auto
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

CUST3-R5#
===============================================================
```

CUST3-R6

```
===============================================================

CUST3-R6#show running-config
Building configuration...

Current configuration : 931 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CUST3-R6
!
boot-start-marker
boot-end-marker
```

```
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 10.53.22.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.53.10.1 255.255.255.0
 duplex full
!
interface GigabitEthernet1/0
 ip address 10.53.12.2 255.255.255.0
 negotiation auto
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

CUST3-R6#
```