ABSTRACT

Information technology and telecommunications have converged along with each other for creating an absolutely positive contribution in global economy and social development. The connection of information systems with business efficiency and effectiveness, production activities as well as their development roadmap becomes almost indispensable to several corporations. The needs of data accessing at a long distance from corporations and customer relationship developing, this project will solve those demands through deploying available resources of companies with high security. Traditional VPN technology based on ATM, Frame Relay and IP suffered many drawbacks such as manageability, security and quality of service. Recently, the technology of multi-protocol label switching - MPLS is concerned by service providers particularly with its outstanding capabilities in delivering high quality services over IP networks, the simplicity, the efficiency and the ability to deploy on VPN. Its advantages include fast forwarding traffic, flexibility, and streamlined control and flexible service routing services, utilizing the transmission to help to reduce costs, MPLS technology is replacing traditional technologies such as IP and ATM. MPLS VPN also addresses the limitations of traditional network-based VPN technology ATM, Frame Relay and IP, such as saving time, reducing installation costs and high security for businesses. Therefore, understanding the application-based MPLS VPN is considered as an urgent topic to help businesses easily approach new technologies. By doing that, enterprises can catch the pace of technology development which is developing day by day on over the World.

Keywords: MPLS, VPN, Mega Wan, Routing Technology, IPsec.

ACKNOWLEDGMENT

The following people did their best to facilitate to me to complete this thesis with the best result, so I wish to thank them.

Firstly, I thank MSc. Nguyen Hoang Sy, my supervisor, for helping me whenever I needed with clear and enthusiastic explanations. MSc. Nguyen Hoang Sy also helps me keep the thesis correct during this course. I wish to thank Mr. Dang Thai Doan as well for allowing me to use lab room and many network equipment. He also taught me necessary information to be able to configure the devices.

My family, for supporting me during my university years; this year in particular.

And finally, I wish to thank my friends for helping me relax and supporting me when I needed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

AAA	Authentication, Authorization and Accounting
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
ATM	Asynchronous Transfer Mode
AS	Autonomous System
BGP	Border Gateway Protocol
B-ISDN	Broadband Integrated Services Digital Network
CE	Customer edge
FR	Frame Relay
HDLC	High Level Data Link Control
ICMP	Internet Control Message Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPsec	Internet protocol security
ISP	Internet Service Providers
LDP	Label Distribute Protocol
LERs	Label Edge Router
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LSP	Label Switched Path
LSRs	Label Switch Router
MP-BGP	Multiprotocol BGP
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
PE	Provider edge
PPP	Point to Point Protocol

PVC	Permanent virtual circuit
QoS	Quality of Service
RD	Route Distinguisher
RT	Route Targets
SP	Service Provider
SVC	Switch virtual circuit
TCP	Transport Control Protocol
TE	Traffic Engineering
TTL	Time To Live
UDP	User Datagram Protocol
VC	Virtual channel
VCI	Virtual Channel Identifier
VOIP	Voice Over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

Chapter 1: Introduction

1.1 Problem definition

Internet is widened and developed day by day, along with the adaption of using requirement and services about quality and delaying. Traditional IP router through Router equalizer is not responsible for requirements like trust, speed and delaying anymore. IP package analyzing will be complex and waste a lot of time while searching in router board or updating and also cost more resources.

To overcome those previous weaknesses, Multiple Protocol Label Switching (MPLS) technology was born to adapt to requirements of speed and quick routing of the Internet. MPLS is a technique combining benefits of layer three routing and layer two switching which allows extremely fast package transferring in Core Network and good routing in Edge Network base on labels. MPLS was build and normalize by staffs of IETF.

1.2 Motivation

The definition of Label Switching is from the research process of the two basic devices in IP networks such as PBX switches and GPS devices. Based on the factors of switching speed, flow control modes and the ratio between price and quality, PBX witches are much better than GPD devices. However, there is no denying of the flexible routing function of the GPS devices which none of PBX switches can compare to. Therefore, there is no evidence to prove that there will have a device which can control the flow, the speed level of PBX switches and the flexible routing functions of GPS devices. Such this primary motivation leads to the development of label switching.

One of the outstanding applications of MPLS technique is MPLS-VNP. With MPLS, the delaying in the network is kept in the lowest point because data packages in the network do not need to be packaged or encrypted. MPLS-VNP is proved to be unique and secured, have a flexible way to name address and the data analyzing of MPLS-VNP is in the isolating core with customers. The remarking point is customer network does not need MPLS supporting devices; moreover, it is easy to widen and develop. MPLS-VNP is also the main target in this research.

1.3 Objectives

The first objective of this thesis is to research in Multiple Protocol Label Switching (MPLS) on VPN to install the experiment by applying MPLS/VPN.

Secondly is to research in Mega WAN.

Finally, this thesis is to make reader have awareness of the fundamental MPLS VPN and be able to build a Mega WAN based on the foundation of MPLS/VPN.

1.4 Organization of the thesis

There are five chapters including in thesis "MPLS VPN Routing Technology and Its Applications On Mega Wan for Enterprise"

Chapter 1: Introduction: In this chapter, I write about MPLS status at present, the motivation and my target in this thesis.

Chapter 2: Literature Review: Basics understanding about MPLS VPN, Control techniques flow TE (Traffic Engineering), and the routing protocols based on MPLS.

Chapter 3: MPLS VPN application on MEGAWAN: In this section, I will present an overview and some applications of Mega WAN.

Chapter 4: Installation and experiment: I will guide the steps to configure and test the configuration steps are correct.

Chapter 5: Conclusion: Some reviews and future work are illustrated in this chapter.

Chapter 2: Literature Review

2.1 Introduction to VPN technology

2.1.1 What is VPN?

VPN technology allows connecting the components of a private network through a public network infrastructure (Internet). Activity-based VPN tunneling technique: packet before being transmitted to VPN will be encrypted and placed in a different packet that can be transmitted over public network. The packet is transmitted to the other end of the VPN connection. At the point of connection to the other side of the VPN, the packet has been encrypted will be "removed" from the public packet network and decoded.

The development phase of the VPN:

- The first generation of VPN is developed by AT&T called SDN.
- The second generation is ISND and X25.
- The third generation are Frame Relay and ATM.
- And the current generation, 4th generation is IP-based VPN.
- The next generation will be based on VPN MPLS network.

VPN includes the following areas:

- Network customer comprises routers at various customer sites. The router connects to the network's personal site provider edge router called the CE client side.
- Network provider is used to provide great connections via point-to-point network infrastructure of service providers. The equipment of service providers that connects directly to the CE router called the provider edge router PE. Network providers may also use the devices to relay data in the backbone (SP backbone) called the provider router (P-provider).

2.1.2 Pros and Cons of VPN

Pros and cons of particular types of VPN

a) VPN based on customer's premise equipment

- Satisfy customer's safety needs.

- Suitable for low need.

- High cost of installment, necessary devices as well as further management of operation.

- No guarantee for the quality of supplied service depending on external factors.

- Be difficult to manage in adding or removing regular users and usually is interrupted during implementation.

- No compatibility.

- Suitable for a single type of equipment, particularly affecting the link with other networks or change in software use.

- Difficulties in the management of service providers because each customer will use different types of equipment, as well as using different management software.

- Low revenue and no long-term relationship with customers.

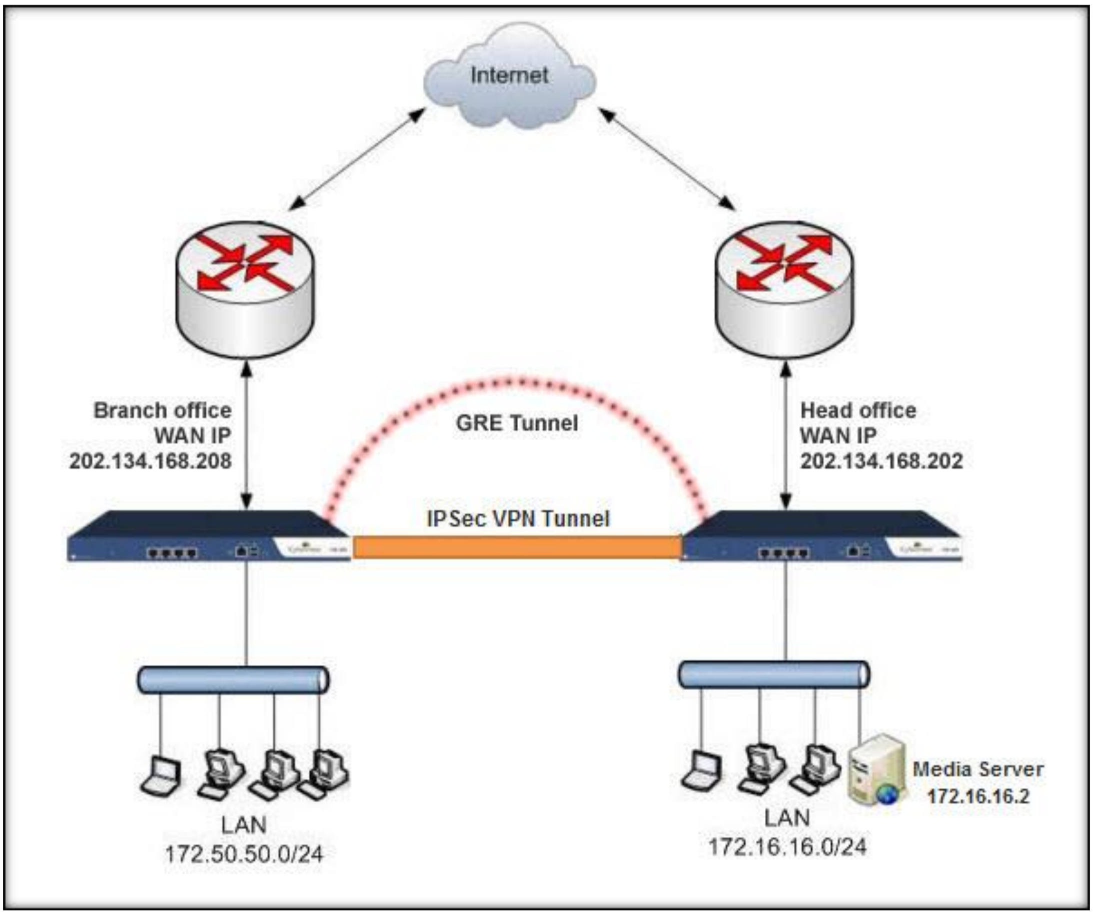


Figure 2. 1 VPN Network

b) Network-based VPN

Provides services and utilities like CPE Based VPN solutions

Reduces device and installation costs

Quickly responds to consumers' enquiries when expanding operation scope

- Responds to customer network monitoring capabilities. They can also keep track and manage separate parts in their network systems. Also, it makes network system easy to monitor

- Quality of services is guaranteed

- Increase the effectiveness in using network

VPN classification

c) VPN for businesses

There are two common types of enterprises today are remote access VPN (Remote - Access) and point-to-point VPN (site-to-site).

Remote access VPN is also known as virtual private dial-up network (VPDN - Virtual Private Dial-up Network), this is the type of connection User-to-Lan apply to companies, whose employees may need to connected to a private network from remote locations and using different devices.

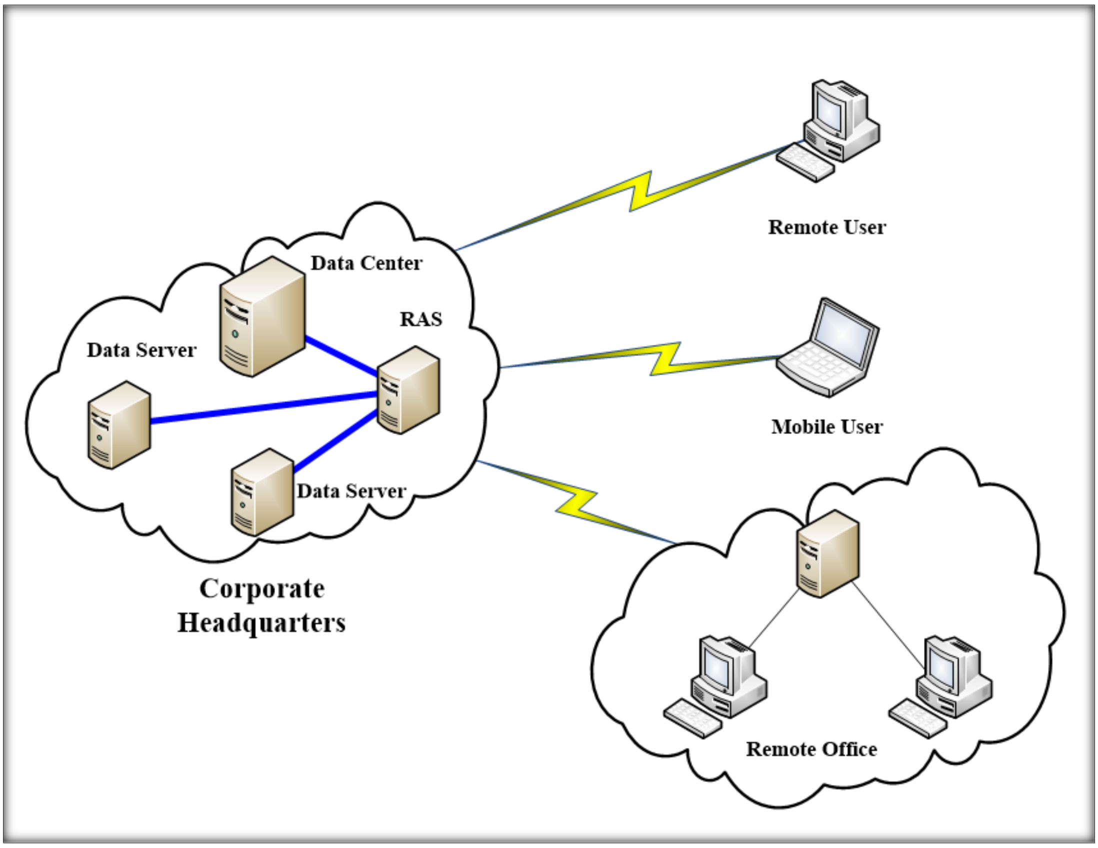


Figure 2. 2 Remote Access VPN

Key components:

- Remote Access Server (RAS) is placed in the center taking responsibility for validation and certification requests sent.
- Dial connection to the center, which will reduce costs for some requirements in far center.
- Support for those who have the task configuration, maintenance and management of RAS, and support remote access by users.

d) Advantage:

- The connection with distance will be replaced by the local connection.
- Cost reduction costs for connecting to a distance.
- Since this is a localized connection, so connection speed will be higher than direct connections to the long distance.
- VPNs provide access to the center better because it supports access services at the most minimal level despite the rapid rise of simultaneous connections to the network.

e) Disadvantages:

- Remote Access VPN does not guarantee the quality of service.
- The possibility of data loss is very high, adding that the segments of data packets can go out and be lost.
- Due to the complexity of encryption algorithms, protocol overhead significantly increase, this makes it difficult for the validation process. In addition, data compression IP and PPP-based place extremely slow and bad.
- Due to data transmission via the Internet, so the exchange of data such as media packets, films, sound will be very slow.

VPN point-to-point is the use of passwords for multiple people to connect multiple fixed together via a public network such as the Internet. This type can be based on Intranet or Extranet.

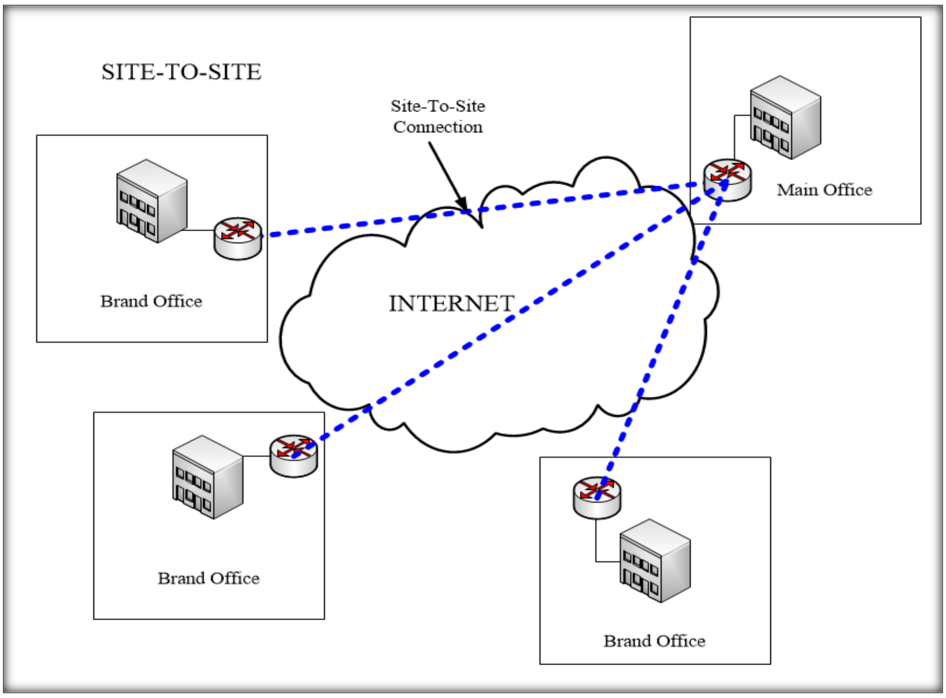


Figure 2. 3 VPN Point to Point

Intranet VPN

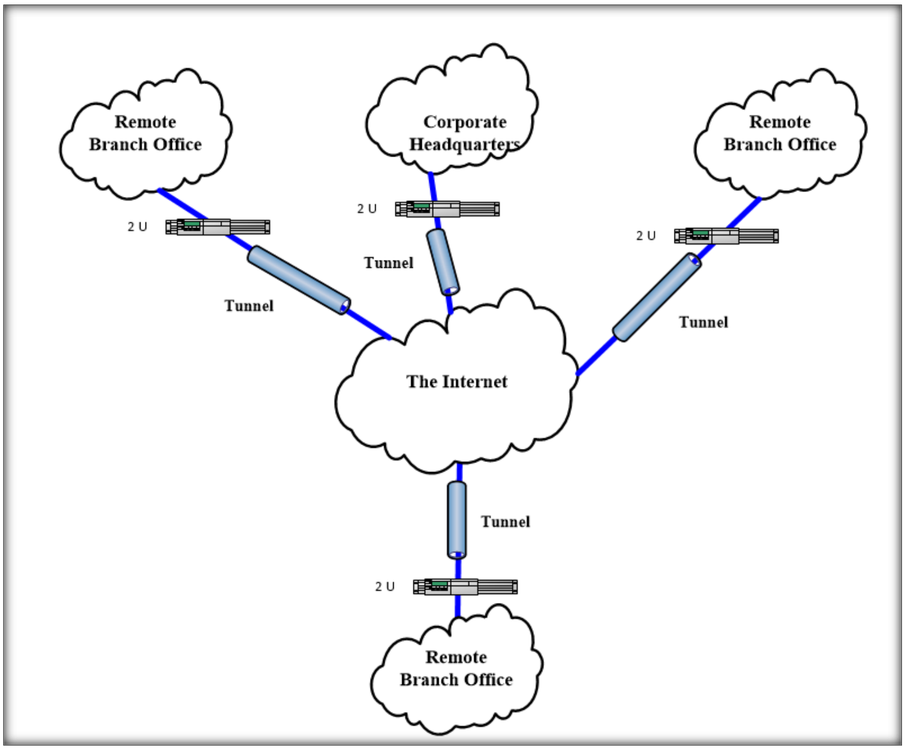


Figure 2. 4 Intranet VPN

Apply in cases where the company has one or more remote locations, each location has had a LAN. Then, they can build a virtual private network to connect to the local network into private network unification.

f) Advantages:

- Significantly reduce support required individual users across the globe, in some remote stations different site
- Because the Internet acts as an intermediary connection, it can easily provide new peer connections.
- Connect faster and better because of the nature connected to the service provider, eliminating the problem of distance and more help organizations lower the costs of implementing Intranet.

g) Disadvantages:

- Because the data is still tunnel during sharing on public networks-the Internet- and the risk of attacks, such as attacks by denial of service, is still a threat of safety information.
- The possibility of data loss during transfer of information also remained very high.
- In some cases, especially when the data is high-end, as the files multimedia, the exchange of data will be very slow due to be transmitted via the Internet.
- Because of the Internet-based connections, so the efficiency is not continuous, regular, and QoS is not guaranteed.

Extranet VPN

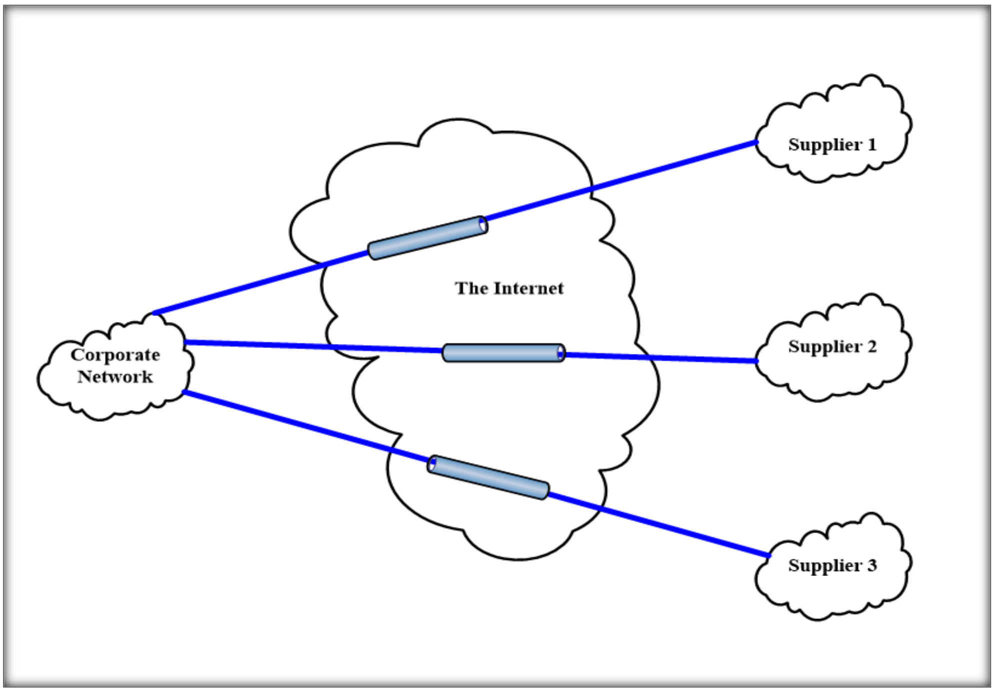


Figure 2. 5 Extranet VPN

When a company has an intimate relationship with another company (e.g. Figure 1.5, a partner, supplier or customer), they can build an extranet VPN that connects LAN to network LAN and allows companies to work in an environment of shared resources.

h) Advantages:

- Because of activities on the Internet, you can choose when selecting a distributor and provides a method of settlement according to the needs of organizations.
- Because Internet-connectivity part is maintained by the supplier (ISP) which should also reduce maintenance costs when hiring maintenance staff.
- Easy deployment, management, and editing information.

i) Disadvantages:

- The threat to security, such as being attacked by a denial of service still exists.
- Increased penetration is dangerous for organizations on Extranet.
- As it is based on the Internet, so when the data is all kinds of high-end data, the exchange takes place slowly.
- As it is based on the Internet, QoS (Quality of Service) is not guaranteed regular.

j) VPN for service providers

Based on the participation of service providers in customer routing, VPN can be divided into two types of models:

- **Overlay VPN Model**

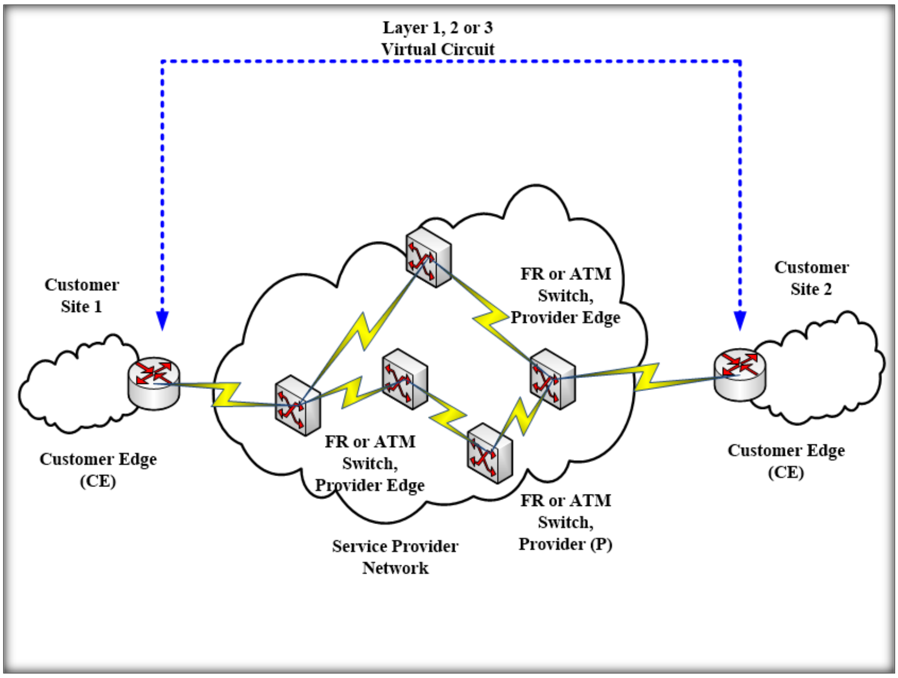


Figure 2. 6 Overlay VPN

When Frame Relay and ATM provide customers with a private network, providers cannot participate in customer routing. The service provider only transports data through virtual connections. Thus, providers only provide customers with virtual connections in layer 2. That is the pattern overlay. If the virtual circuit is fixed, ready for customers to use all the time, it is called virtual fixed PVC circuit. If the virtual circuit is set up on request (on-demand), it is called a virtual circuit switch SVC.

The main drawback of the model is the virtual circuit overlay of customer sites full mesh connectivity. If there are N customer sites total number of virtual circuits required N(N-1)/2.

Overlay VPN is implemented by the SP to provide the connectivity layer 1 (physical) or transport layer circuit 2 (Data link - data frame or cell types) between customer sites using Frame Relay devices or ATM Switch. Thus, the SP could not identify the router at the customer.

Overlay VPN services are implemented through Layer 3 protocols such as GRE tunnels, IPsec and so on. However, in either case, whether the provider's network remains transparent to the customer, and the routing protocol runs directly between the customer's routers.

- **Peer-to-peer VPN Model**

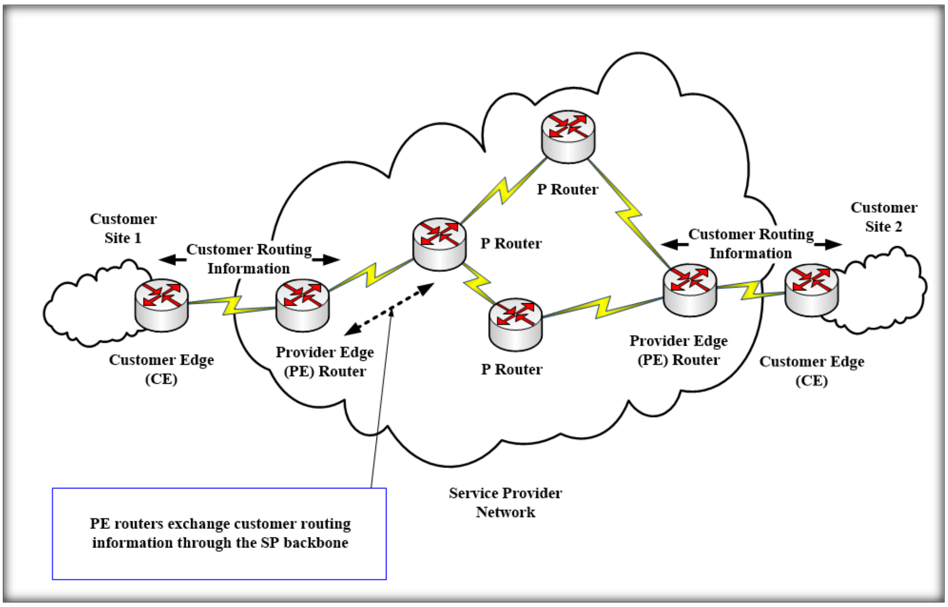

P Router
Customer Site 1
Customer Routing Information
P Router
Customer Routing Information
Customer Site 2
Customer Edge (CE)
Provider Edge (PE) Router
P Router
Provider Edge (PE) Router
Customer Edge (CE)
Service Provider Network
PE routers exchange customer routing information through the SP backbone

Figure 2. 7 Peer to Peer VPN

Peer-to-peer models overcome the disadvantages of the Overlay model and provide customers optimal transport mechanisms across the SP backbone, because service providers know the customer network model and thereby could set up routing optimization for their routers.

Service providers involving in the routing of customer. Routing information of customers is promoted through the network of service providers. Network service providers determine the optimal path from one customer site to another site.

The discovery of the own routes information with customers by performing packet, filtering (packet) in the router connected to the customer network.

Peer-to-peer VPN is divided into two categories:

k) Shared-router

Sharing Router, VPN client that is shared with the network edge router PE provider. In this method, multiple clients can connect to the same PE router. On the PE router, it must be configured for each interface access-list PE-CE to ensure the separation between the VPN clients, to prevent this VPN client perform denial-of-service attack on the VPN DoS other customers. Service providers divide each part in its address space for customers and manage packet filters on the PE router.

l) Dedicated-router

A method that VPN clients have dedicated PE router. In this method, each VPN client must have a dedicated PE router, and thus access to the router's routing table that PE router. Dedicated-router models use routing protocols to create the routing table on a VPN on PE router. The routing table routing only marketed by VPN client to connect to them, the result is to create separation between the VPNs.

2.1.3 Service provider offers VPN service to customers

At the present, all ISP offered VPN service for customers, some service providers have deployed VPN network including:

- Vietnam Posts and Telecommunications Group
- Viettel Group
- FPT Telecom

2.2 Introducing multi-protocol label switching - MPLS VPN

2.2.1 The concept of MPLS

Multiprotocol Label Switching (MPLS - Multiprotocol Label Switching) is a hybrid technology combining the best features between Layer 3 routing (Layer 3 routing) and Layer 2 switching (Layer 2 switching). It allows transfer of very fast packet core network (core) routers and good at the edge network (edge) by relying on the label (label).

2.2.2 Functions and benefits of MPLS

a) Functions

- The process of managing the traffic the flow of the various networks, such as flow between machines, different hardware or even flow between various applications.
- Maintain the independence of the protocol layer 2 and layer 3.
- Provides a way to map IP addresses into a simple label with constant length is used by the packet forwarding technology and various packet switching.
- The interface used in conjunction with routing protocols OSPF or RSVP.
- Support for IP, ATM, Frame Relay.

b) Benefits

- Working with most of the data link technology.
- Compatible with most of routing protocols and other technologies related to the Internet.
- Operating independently of the routing protocol (routing protocol).
- Finding flexible way based on the label (label) to advance.
- Supporting for configuration management and system maintenance (OAM).
- Operating in a decentralized network.
- High compatibility.

2.2.3 MPLS Features

No MPLS API nor the host protocol components.

MPLS stays on the router.

MPLS is an independent protocol, so it can work with different network protocols such as IPX IP, ATM, Frame-Relay, PPP, or direct to the Data Link layer.

Routers in the MPLS are used to create the flow of fixed bandwidth similar virtual channels of ATM or Frame Relay.

MPLS simplifies the routing process, and increases flexibility in the intermediate layer.

2.2.4 MPLS architecture

One of MPLS nodes has two functions: MPLS forwarding plane and MPLS control plane. MPLS nodes can perform routing or switch the third grade class two. The basic architecture of a MPLS node as follows:

Forwarding plane

Forwarding plane uses a forwarding information base label (LFIB - Label Forwarding Information Base) to forward the packet. There are two tables in each MPLS node relating to the transition: the basis of information labels (LIB - Label Information Base) and LFIB. LIB contains all the local label MPLS node marking and mapping of these labels to the label received from its neighbors (MPLS neighbor). LFIB uses a subset of the labels contained in LIB to perform packet forwarding.

Control Plane

MPLS control plane takes responsibility for creating and storing LFIB. All MPLS nodes run an IP routing protocol to exchange routing information for other MPLS nodes in the network. ATM MPLS enabled nodes will use a manual controller (LSC -

Label Switch Controller) as routers 7200, 7500 or use a route processor module (RPM - Route Processor Module) to participate handle IP routing.

The routing protocol OSPF and link-state as IS-IS protocol is selected because it provides information for each node of the entire network MPLS. In the conventional router, the IP routing is used to build the storage switch (Fast switching cache) or FIB (used by CEF - Cisco Express Forwarding). However, with MPLS, IP routers provide the information of destination network and subnet prefix. The routing protocols link-state routing information sent (flood) between a set of routers directly connected (adjacent), information associated with labels are distributed between the routers, only. They are directly connected to each other by using a protocol distributor (LDP - Label Distribution Protocol) or TDP (Cisco's proprietary Tag Distribution Protocol).

The labels are exchanged between adjacent MPLS nodes to build LFIB. They use a sample MPLS forwarding based on labels swapping to connect with various control modules. Each control module takes responsibility for marking and distributing a set of labels as well as retaining information related controls. The interior gateway protocol (IGP - Interior Gateway Protocols) is used to confirm the ability, the links, and the mapping between the FEC and next station addressing (next-hop address).

The control module includes MPLS:

- Unicast Routing
- Multicast Routing
- Traffic engineering
- VPN – Virtual private Network
- QoS – Quality of service

2.2.5 Comparing OSPF and EIGRP in MPLS

EIGRP and OSPF are the good routing protocols. Each protocol has particular strengths in the design and the deployment of a network infrastructure which is flexible and easy to expand. It is difficult to compare which protocol is better than the other). The followings are to interpret all aspects of them to have a better look for your network model to select the most appropriate protocol:

- Ease of use: it is easier to configure EIGRP than OSPF. OSPF with more complex concepts such as LSA, divides Area to make the configuration more complicated. However, if it is configured correctly, OSPF works very well on a large network model.

- Broadcast network: In EIGRP, each router directly exchanges information with each other on the network model therefore causing bandwidth consumption. Meanwhile, OSPF uses DR (Designated Router) and BDR (Backup Designated Router), and the other routers will exchange routing information with the DR and DR which will distribute routing information to each router. As a result, this will save a lot of bandwidth.
- Route Filtering and Aggregation: EIGRP supports very well than OSFP.
- Convergence (Convergence): Depends on many factors such as topology, metric, type of failure and so on. In some cases, EIGRP is proved that it is faster, but in other cases, OSPF is better.
- Memory and CPU: OSPF generally requires more CPU and memory than EIGRP to serve in the best way.
- Support multi-protocol: EIGRP can use for IP, IPX, and AppleTalk while OSPF is only used for IP.
- Metric: EIGRP selects the best path based on Bandwidth, Delay, Reliability, Load, MTU Size while OSPF Cost based on synthetic indices to destination (100,000,000/interface speed). [1]
- Bandwidth consumption: EIGRP generally consumes less bandwidth. Also, EIGRP allows the limited bandwidth that it uses while OSPF uses bandwidth without caring about other factors.
- Hierarchy network: EIGRP is not a good choice for large network model because it does not support split rank while OSPF is supported by split 'area'.
- Dial on Demand: To maintain EIGRP neighbor relationship, it requires the router to send packets to each other after each paragraph HELLO appearing in a specific time. Meanwhile, OSPF supports Dial on Demand.
- Copyright: EIGRP is a proprietary protocol, developed by Cisco, it does not run on other devices. Meanwhile, OSPF is an open standard from the Internet Engineering Task Force (IETF) and is most manufacturers’ support, so this protocol is growing more rapid.

2. 3 MPLS VPN

2.3.1 What's MPLS VPN?

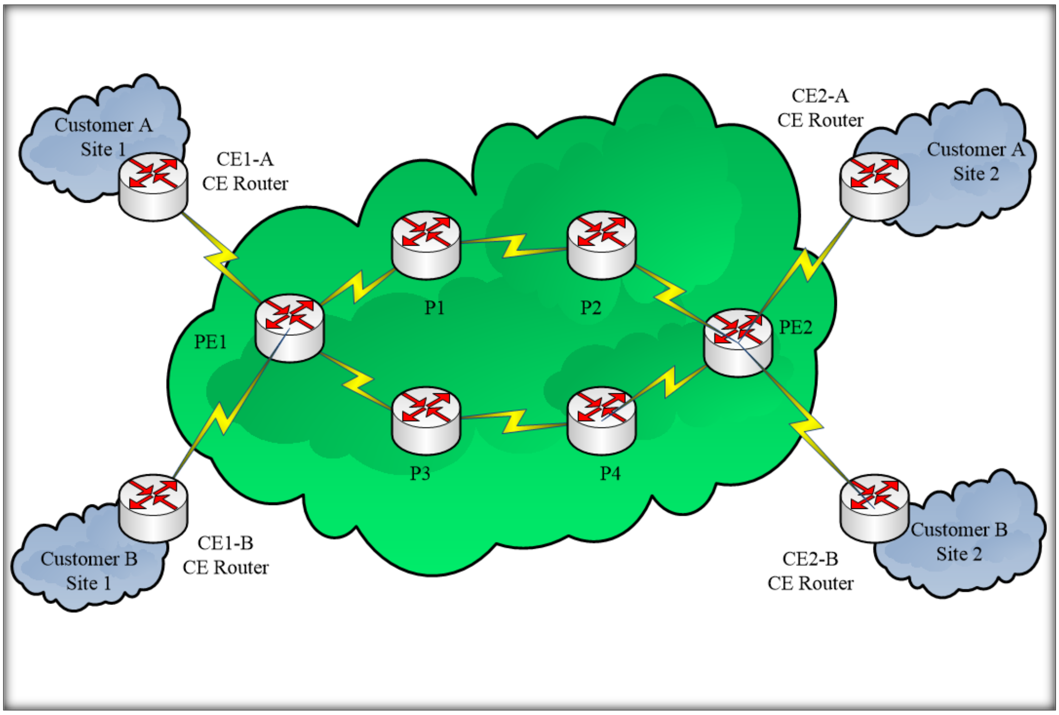


Figure 2. 8 MPLS VPN

MPLS VPN combines the best characteristics of overlay VPN and peer-to-peer VPN:

- The PE router involved in the routing of customer and optimal routing between customer sites.
- The PE router uses virtual routing tables for each client to provide the connection to the network of suppliers to many customers.
- The customer can use identical IP addresses (addresses overlap) MPLS VPN backbone and customer sites exchange information Layer 3 routing.

MPLS VPN includes the following regions:

- Customer Network: usually the domain controller client devices including routers, or spread over much of the same customer site. The CE router is the router in the customer network to communicate with the network of suppliers.
- Networking vendor: domain is under the control of the provider edge routers include and core to connect the subject to the customer site in a shared network infrastructure. The PE router is the router in the provider's network to

communicate with the customer edge router. P routers in the core of the network's router communicate with other core or edge router vendor.

- In MPLS VPNs, routers provide core label switching between the edge routers of the supplier and unknown to the VPN route. The CE router in the customer network is not aware of the core router, so that the structure of the network intranet provider becomes transparent to the customer.

2.3.2 Benefits of MPLS VPN

Low cost and speed stability meet the requirements for information security, support to effectively manage and convert easier.

Reduce in costs compared with similar technologies in the management, construction and deployment of a wide area network.

Stability and scalability: meets the need to expand rapidly, can faster connect to other networks.

Adapting to different types of technology and maintain the current network of customers. Thanking to the support of many different types of technology, MPLS can support different types of access, such as Frame Relay, IP and so on, reduce costs for clients or can take advantage of existing network equipment.

Secure Networking: with the ability to encrypt and tunnel of MPLS VPN technology to help achieve high safety level as in private network environment.

Quality of service: ensuring to distinguish priorities for different types of data such as data, images and sound.

2.3.3 The components of MPLS VPN

a) Virtual Routing and Forwarding Table (VRF)

Customers are differentiated on the PE router with routing tables virtualization (virtual routing tables) or instances, known as VRF (virtual routing and forwarding tables / instances).

Functions of a VRF routing, like wikis, except that it contains all the routes involved a specific VPN.

VRF IP routing table contains a corresponding global IP routing table, CEF table, listing the interfaces involved in the VRF, and a set of principles for determining routing protocol exchange with the router CE (routing protocol contexts). VRF also contains the VPN identifier as membership information VPN (RD and RT).

b) Multiprotocol BGP (MP-BGP)

MP-BGP runs between the edge router vendor for information exchange VPNv4 routes. MP-BGP is an extension of the current protocol BGP. Address VPNv4 client is a 12-byte address, a combination of IPv4 and RD. 8 bytes are RD; 4-byte IPv4 address followed.

An MP-BGP session between BGP AS PE in an MP- iBGP called session and accompanying the implementation of iBGP principles concerning the attributes of BGP (BGP attributes). If VPN extends beyond the scope of an AS, the VPNv4 will exchange between AS in the minutes by MP eBGP session.

c) Route Distinguisher (RD)

RD is a 64-bit identifier unique. Resolving the IP address of the polymerization customers by inserting into the IPv4 64-bit address form VPNv4 (96 bit). Therefore, only one RD be configured for a VRF on the PE router. VPNv4 addresses are exchanged between PE routers via BGP.

RD can be in two formats: the IP address format and indicators AS:

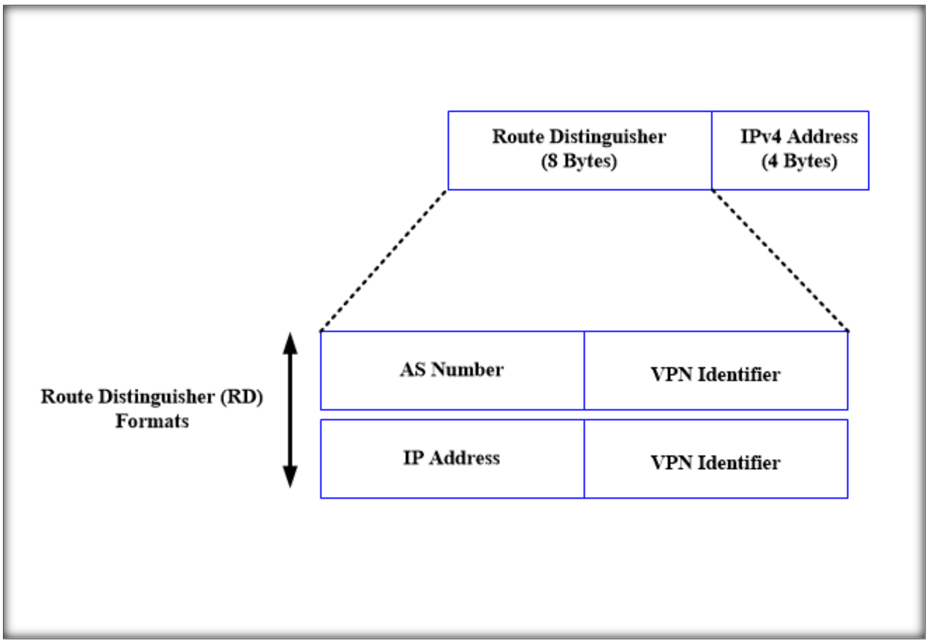


Figure 2. 9 Route Distinguisher(RD)

The first router PE-1 inserting 64bit RD in IPv4 packets and VPNv4 address form through MP-BGP protocol to transfer packet router PE-2

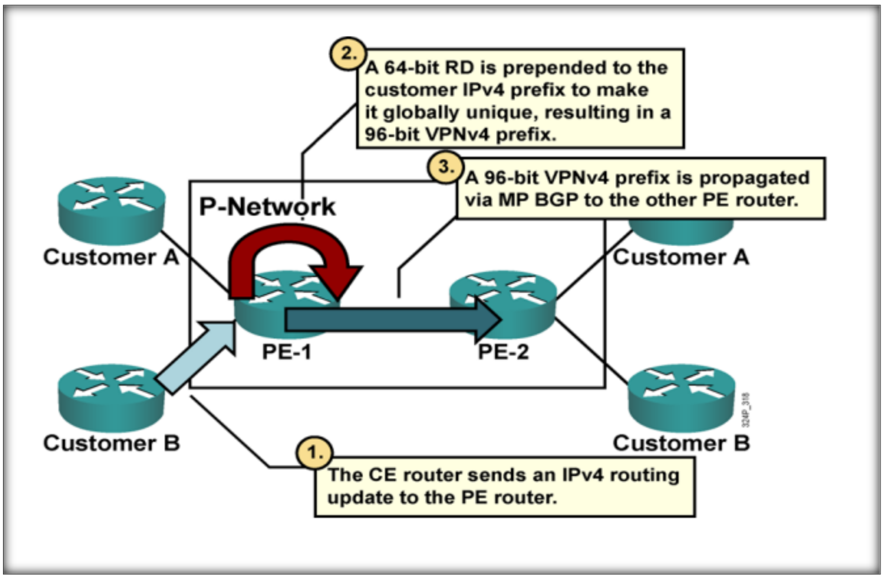

2.
A 64-bit RD is prepended to the customer IPv4 prefix to make it globally unique, resulting in a 96-bit VPNv4 prefix.
3.
A 96-bit VPNv4 prefix is propagated via MP BGP to the other PE router.
P-Network
Customer A
Customer A
PE-1
PE-2
Customer B
Customer B
324P_318
1.
The CE router sends an IPv4 routing update to the PE router.

Figure 2. 10 The process of assigning RD

At router PE-2, the packet VPNv4, RD was removed and replaced by IPv4.

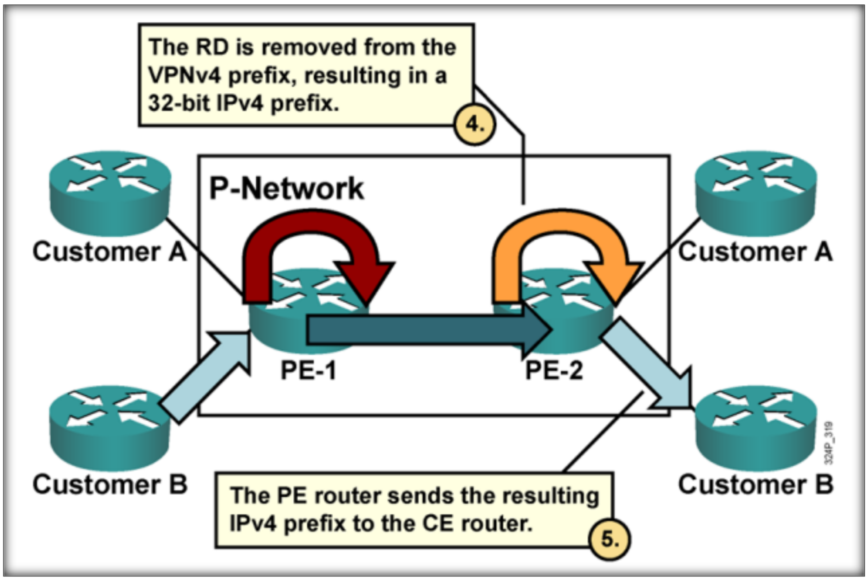

The RD is removed from the VPNv4 prefix, resulting in a 32-bit IPv4 prefix.
4.
P-Network
Customer A
Customer A
PE-1
PE-2
Customer B
Customer B
324P_319
The PE router sends the resulting IPv4 prefix to the CE router.
5.

Figure 2. 11 The process of removing the RD

d) Route Targets (RT)

Route targets (RT) are identifiers used in domain MPLS VPN MPLS VPN deployment to identify members of the VPN routes learned from specific sites. RT is implemented by BGP extended community use 16 bits of BGP extended community high (64-bit) encryption with a value corresponding to the members of the site-specific

VPN. When a VPN route learned from a CE inserted VPNv4 BGP, a list of attributes for the VPN router community expansion target is associated with it.

- RT is attached routers called export RT and is configured separately for each VRF in the PE router. Export RT members used to define VPN and is associated with each VRF. Export RT is appended to the customer's address when converted into VPNv4 address by PE and promotions in MP-BGP updates. [2]

- Import RT associated with each VRF and define VRF routing VPNv4 added for specific customers. The format of the RT like value RD. [2]

When implementing complex VPN network structure (For example, extranet VPN, Internet access VPNs, network management VPN and so on) and using MPLS VPN technology, the RT core role. A network address can be associated with one or more RT when promoting the export MPLS VPN network.

Thus, RT can be combined with many members of multiple VPN sites.

2.3.4 Operation of the control plane

Control plane in MPLS VPN routing information containing any layer 3 and the information exchange process of the IP prefix is assigned and distributed by LDP label.

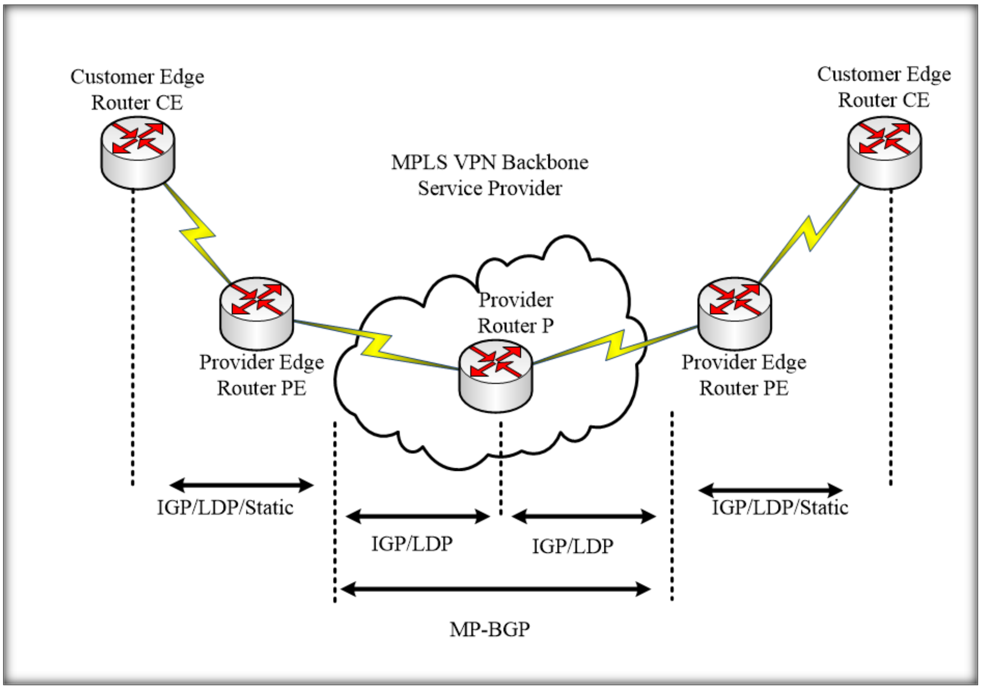


Figure 2. 12 MPLS VPN Control plane

The operational steps of the control plane MPLS VPN: Each PE router advertising its loopback address: PE1 and PE2 advertisement ad 1.1.1.1/32 2.2.2.2/32. LDP is used to distribute label information between routers running MPLS. On each PE router, LFIB contains a label attached to the loopback address of the other PE router. When forwarding packets from PE1 PE2 2.2.2.2 on, it will add label 20 to the package label and the PE2 forwards a packet from 1.1.1.1, it will put the label 10 for the package. VPN routing and forwarding PE1 and PE2 created on, called VPNA. PE1 user interface S0 / 0 in this VPN and PE2 user interface S0 / 1. OSPF runs between CE1 PE1va; PE2 and CE2. When PE1 gets to network 10.1.1.0 route from CE1, the router put it in the router's routing table VPNA. At this point, it labeled (5) for the prefix. When PE2 gets to network 10.1.2.0 route from CE2, it puts into the routing table of VPNA. Now the label (6) is assigned to the prefix. PE1 then sends updated multi-protocol MP-iBGP to PE2 advertising network 10.1.1.0. Update also contains labels (5), which tied for prefix 10.1.1.0 PE1, and PE2 embedded in any packet network to 10.1.1.0 before it forwards the packet. When PE1 online ads, it puts the address is 1.1.1.1/32 BGP next stage, as its loopback address. PE2 then sends updates iBGP multi-protocol for ad PE1 10.1.2.0 network. Update also contains labels (6), which assigns prefix 10.1.2.0 PE2 and PE1 to add additional network packets to 10.1.2.0 before forwarding it. When PE2 routes advertisement, it sets the next leg BGP address 2.2.2.2/32 as its loopback address. PE1 puts prefix 10.1.2.0 in the routing table of PE2 VPNA and puts prefix 10.1.1.0 in the routing table of VPNA.

2.3.5 Activity data of MPLS VPN

Perform data plane forwarding IP packets are labeled successor to the destination station.

The forwarding of MPLS VPN requires the husband to use labels (label stack).

Labels on assigned and swaps to forward data packets go in the MPLS core. Second label (label VPN) is associated with VRF in the PE router to forward the packet to the CE. Figure 2.13 shows the steps in the data forwarding plane customer data from a customer site to CE1 CE2-A-A in the SP network infrastructure.

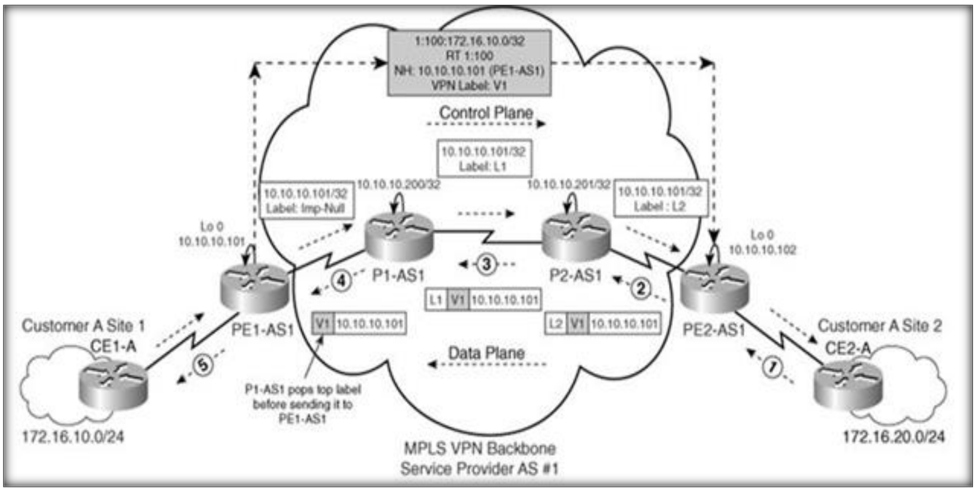


Figure 2. 13 MPLS VPN Data plane

Figure 2.13 shows the process in which CE2-A sends a packet to CE1-A. At first, the data is forwarded to PE2-AS1 from CE2-A. At PE2-AS1, it is labelled “VI” and appended the LDP L2 and then forwarded to P2-AS1. Then P2-AS1 receives the data packet which is transmitted to 172.16.10.1 and swaps LDP label L2 with L1. After that, P1-AS1 receives the data packet that is forwarded to 172.16.10.1 and drops the first label L1. That packet (Labelled VPN V1) is forwarded to PE1-AS1. Finally, PE1-AS1 drops the VPN label and forwards the packet to CE1-A where the 172.16.10.0 network is determined. *[3]*

SUMMARY CHAPTER 2:

This chapter presents an overview of VPN technology, which VPN includes for enterprise VPN and VPN for the service provider. Based on the participation of service providers in the routing for the customer, there are two basic models: overlay VPN and peer-to-peer VPN, each model has its own advantages and disadvantages. MPLS VPN combines the benefits of overlay VPN and peer-to-peer VPN, the legacy from MPLS technology advantages with the benefits of security, deployment flexibility, quality of transmission lines and the competiveness of price. The next is Chapter 2 Mega WAN with its applications can be achieved.

Chapter 3: Applications of MPLS - VPN on Mega Wan

3.1 Introduction

Nowadays, information technology and telecommunications are converging along deep and very positive contribution in economic development and global society. There is no denying that information systems have increasingly supported for the growth of business and organizations both in production activities and the development roadmap. Each day, they invest more to both value the information content and network infrastructure equipment and services. A series of new solutions is launched to bring major changes in the structure of the business network infrastructure users and organizations. The popular structure now no longer appears in the form of internal LAN, but switched to WAN (Wide Area Network) thanking to WAN, enterprises, organizations gradually spread across the country and beyond borders, and frequently connect with its branches, customers, suppliers and distribution centers.

3.2 The general concept of Mega WAN

Allows link between corporate computer networks such as the office, branch, remote collaborator, etc., in different geographic locations to form a single network and trust through using xDSL broadband links.

Mega WAN uses methods such as multi-protocol label switching (Multiprotocol Label Switching) network protocol next generation.

As service provider for the private network connection IP-based client / MPLS, Services VPN/MPLS allow deployment of strong connection, simplicity, convenience and cost improvement.

Virtual private network access has Internet access (when customer needs).

3.3 The requirement to network design Mega WAN

There are four key requirements:

WAN is flexible and be able to change the business management activities in an enterprise as open offices, changing suppliers of raw materials, changes distributors, sales channels, etc. and if there is a network architecture, a number of network nodes will also be changed accordingly.

The quick recovery function, serving when problems occurred, causes a rocket in capacity requirements reroute traffic. This function will perform when an intermediate point on the network/on the Internet or a transmission line goes dead. Normally, it will take 50 milliseconds to recover the transmission line and have less than 50 milliseconds to recover voice traffic.

Network infrastructure Convergence (Convergence of Network Infrastructure): merges many types of technologies (ATM and Frame Relay), protocols (IP, IPX and SNA) and the type of traffic (data, voice and videos) on a single network infrastructure. However, when it costs to support network infrastructure greatly reduce compared to support multiple networks as before.

Isolate traffic or in other words, Traffic Isolation, aims to increase security (only accesses to the information flow of their data) and stability (the activities of an entity only affect that entity).

3.4 Application of Mega WAN

Networking (LAN / WAN to LAN / WAN).

Watching movies on demand (Video on Demand).

Video Conferencing (Video Conferencing).

Game on the network (Network Game; Game online).

Working remotely, at home (home office, Telecommuting).

Training / learning remote network (Tele learning).

Diagnostic / treatment remotely (Tele medicine).

Purchase / Sales Online (Online Shopping).

Radio / TV (Broadcast Audio & TV).

Serving for the Security Service (home security, traffic management ...)

Services virtual private network (VPN).

3.5 Mega WAN actual model

Allowing networking businesses together (such as offices, branches, remote users and so on in different geographical locations access into a single network and reliability through the use the xDSL bandwidth links. Allows users to access the private network and Internet access, ensuring the circulation of work

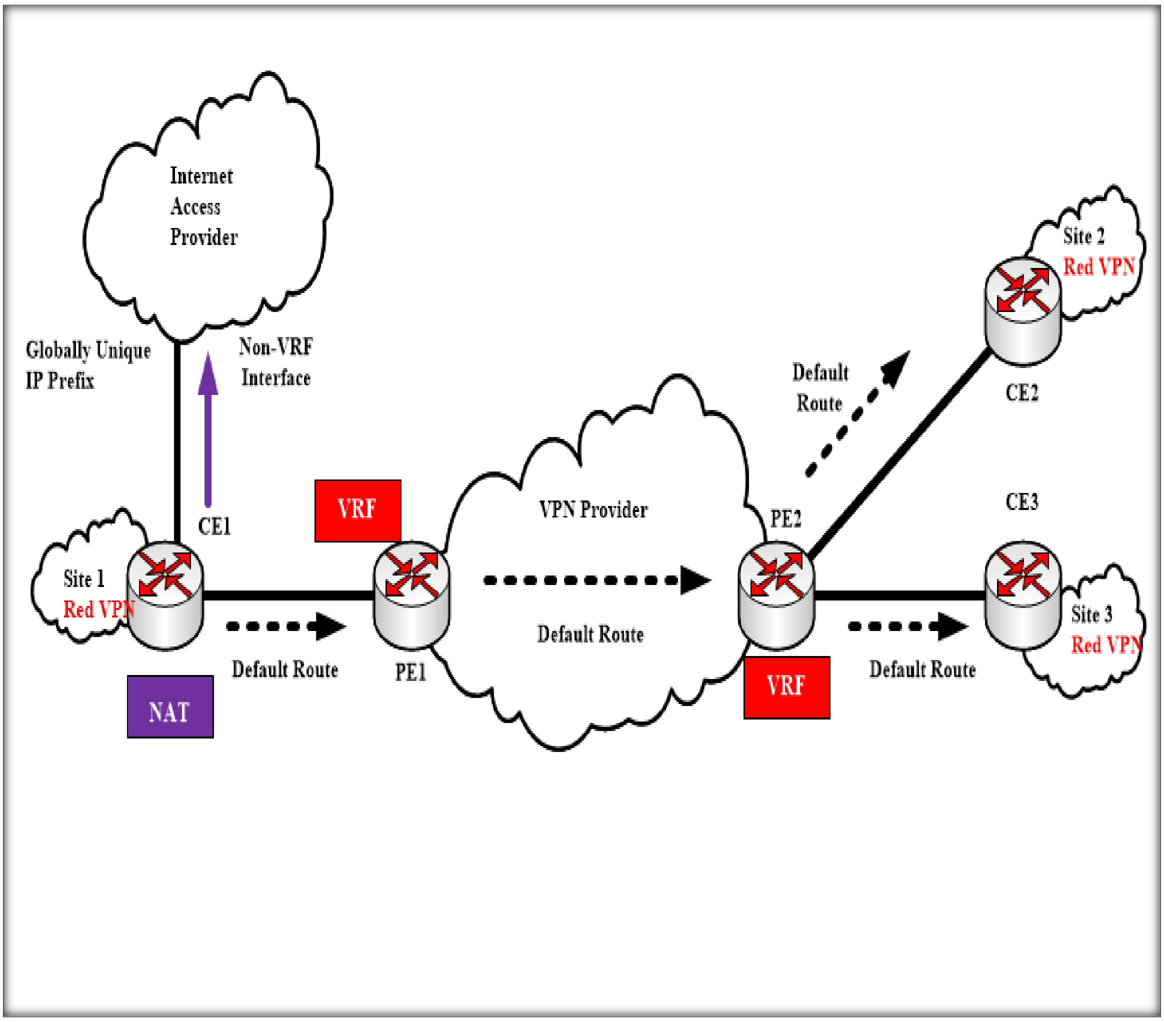


Figure 3. 1 Mega WAN access virtual private network and Internet access

3.5.1 VOIP

With the PBX systems available plus VOIP solutions without the need to pay for long distance calls charge is a great turning point in communication process, as following:

- Call quality is as good as when having a face-to-face talk.
- Number dialing is simple and easy to use.
- Low construction cost for VOIP.

As so, calling VOIP via Mega WAN will pay no cost.

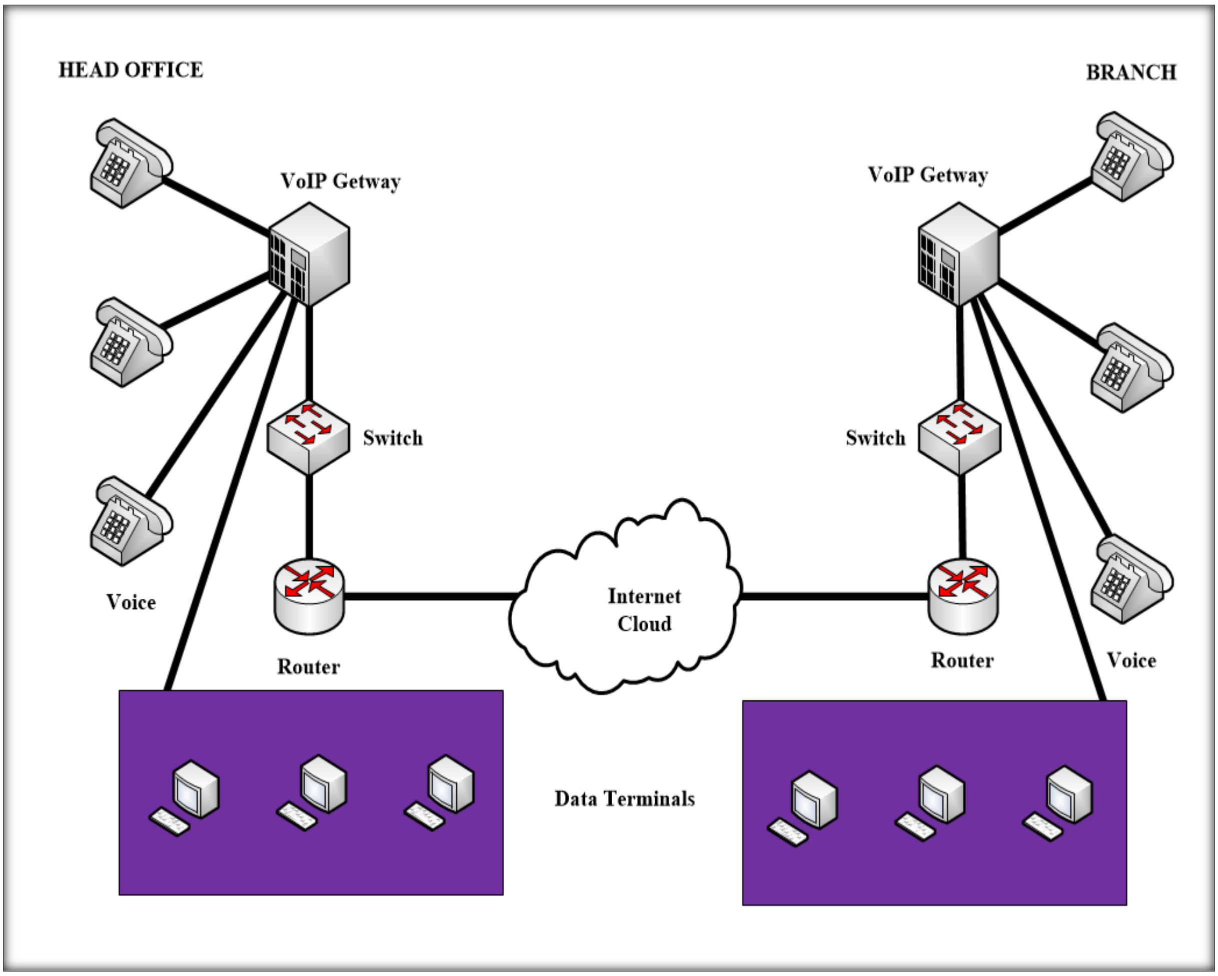


Figure 3. 2 VoIP via Mega WAN

3.5.2 Video Conferencing

Video Conferencing Solution saves travel costs between branches through direct meetings on television head placed in the branch.

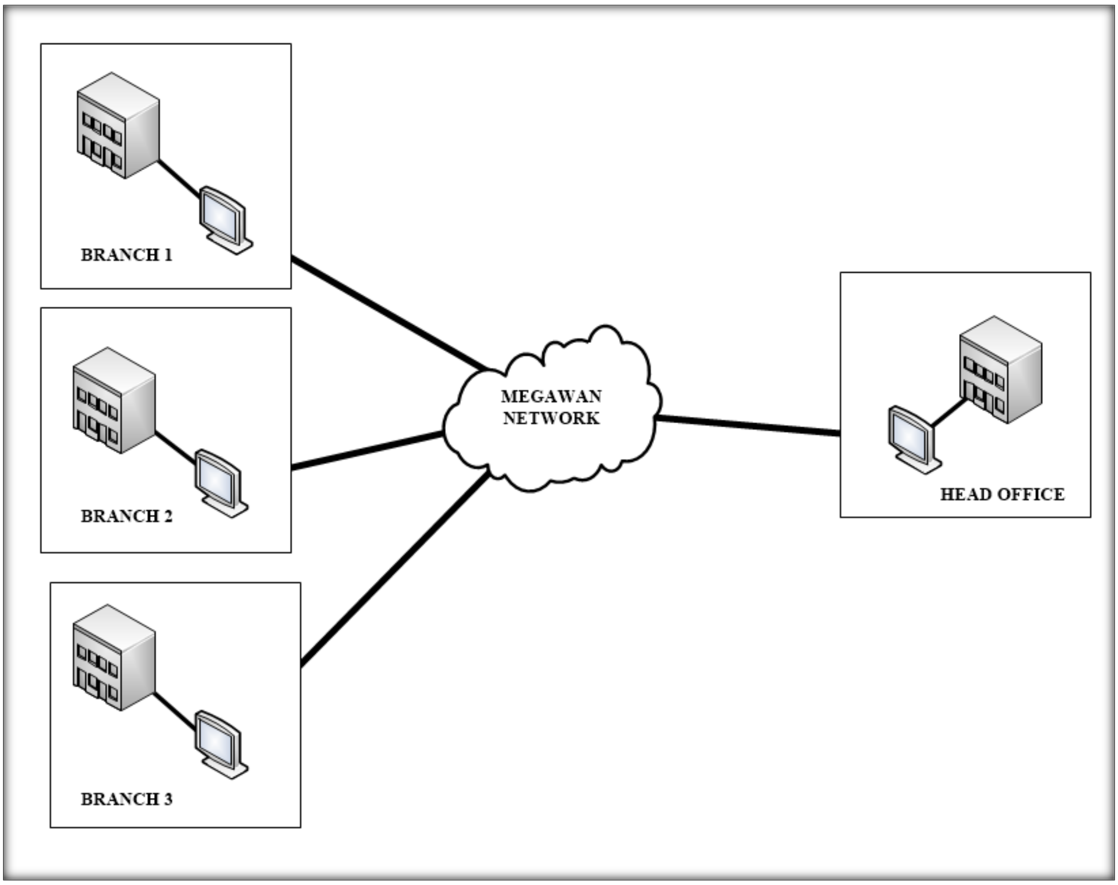


Figure 3. 3 Video Conferencing via Mega Wan

3.5.3 Cameras monitoring via Mega Wan

Through Mega WAN network, the companies can monitor the camera system at the branches. It assists to follow the current situation, current status at the branches through camera system installed under the types of analog or IP.

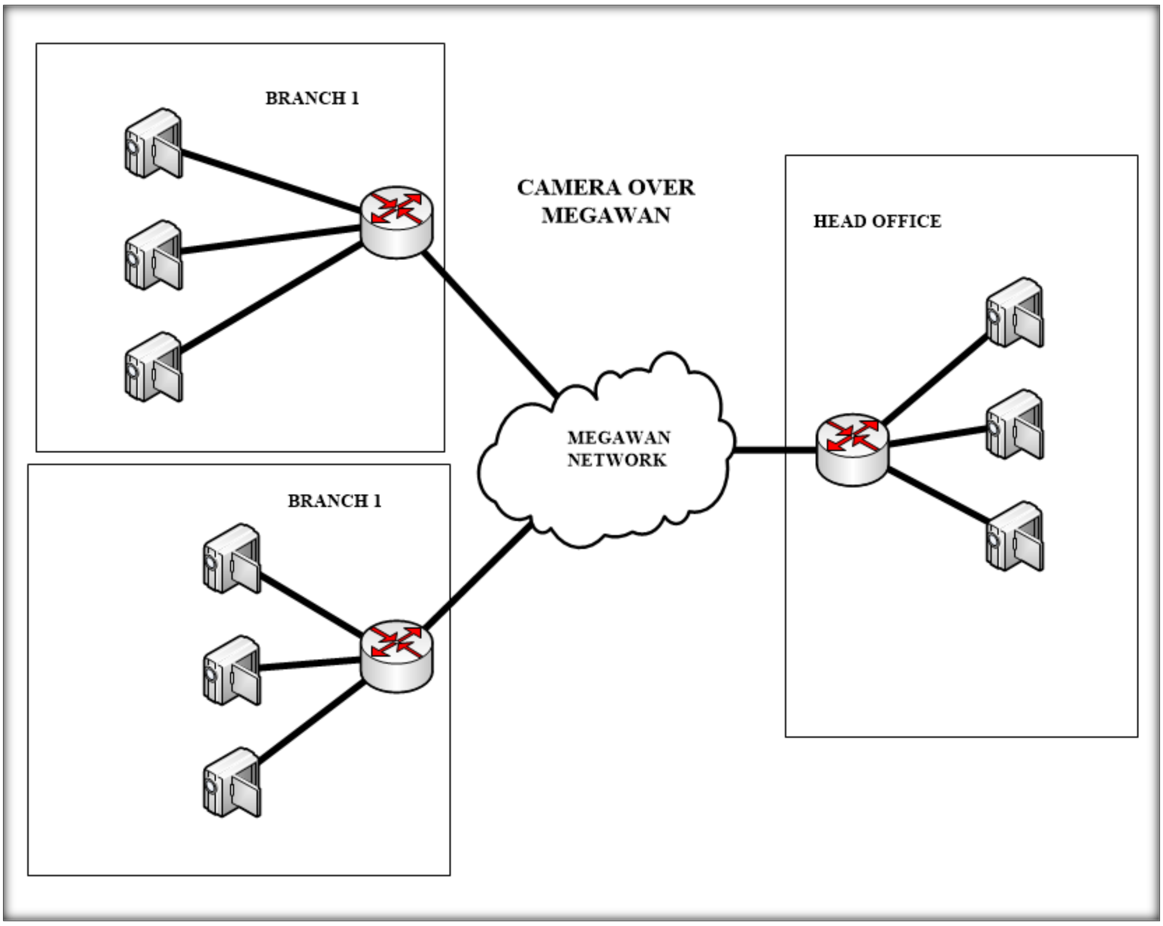


Figure 3. 4 Camera Over Mega Wan

SUMMARY CHAPTER 3:

Mega WAN is an application based on VPN MPLS. So, when the businesses and organizations use this application, they can achieve its criteria for practical applications such as video conferencing, surveillance cameras, VoIP and more. It also ensures greater control over network infrastructure, which results a better and proper service performance. It provides multiple classes of service to users, improves safety and guarantees responsiveness for the requirements of the application, supporting converged multi-technology and multi-type of traffic over the same network applications. I will realize some demo to learn more about the application of Mega WAN.

Chapter 4: Demo and Experimental Setup

4.1 Topology MPLS/VPN

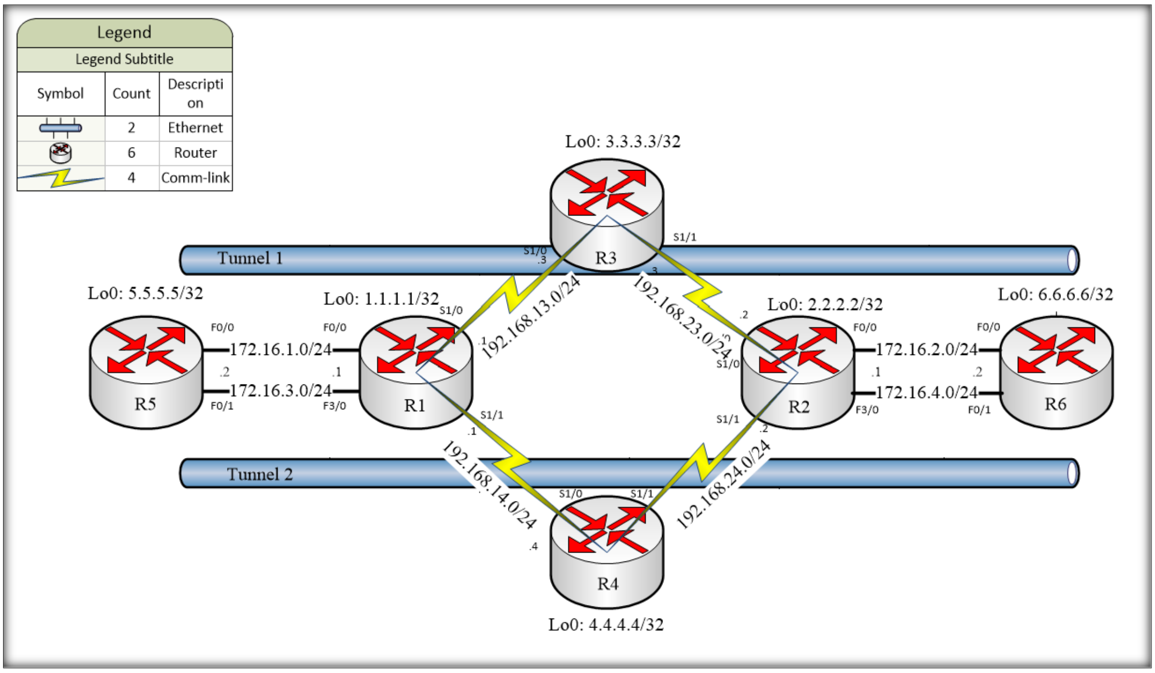


Figure 4. 1 Topology MPLS VPN IPsec

Router function in the network:

R1, R2: is PE router that connects with the router by MPLS core bearing crabs in ISP and connects with the CE of customer sites.

R3, R4: is P router that performs MPLS switching, and routes IGP core ISP network.

R5, R6: is CE router is on the client side, connects with the PE of the service provider.

The below framework illustrates the process:

OSPF process 1: Perform core routing IGP in bringing ISP.

OSPF process 100: OSPF routing with CE of CUS_A.

OSPF process 200: OSPF routing with CE of CUS_B.

BGP AS 1: MP-iBGP route runs counted among the PE together.

Traffic Engineering:

TUNNEL1 (Customer A): R1->R3->R2 CUS_A (172.16.1.0/24, 172.16.2.0/24).

TUNNEL2 (Customer B): R1->R4->R2 CUS_B (172.16.3.0/24, 172.16.4.0/24).

IPsec is configured on the CE (R5 and R6) at terminal 2 of the client to ensure that data is encrypted when transmitted over the network backbone ISP.

MPLS-VPN Routing

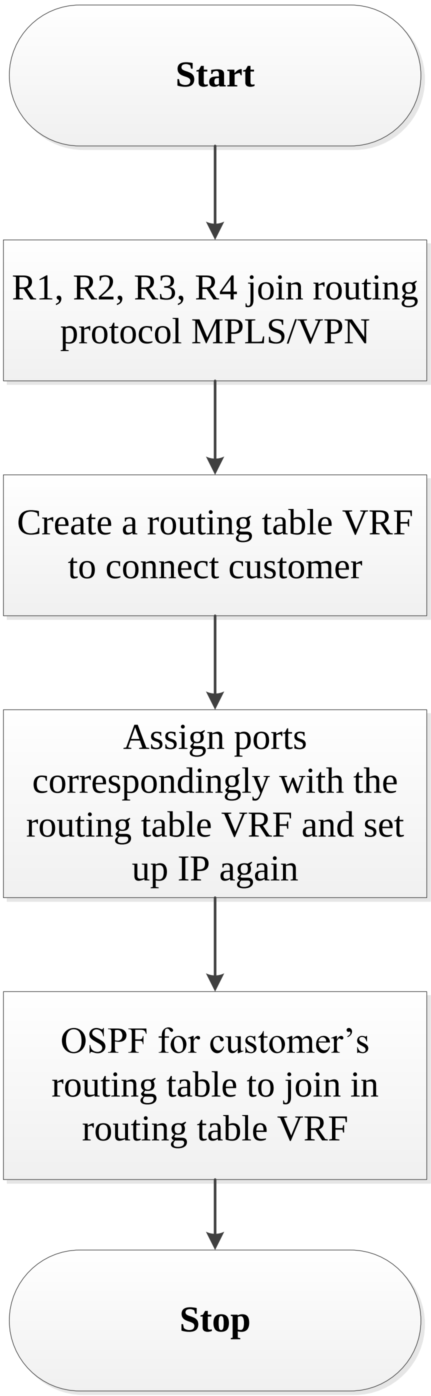

Start
R1, R2, R3, R4 join routing protocol MPLS/VPN
Create a routing table VRF to connect customer
Assign ports correspondingly with the routing table VRF and set up IP again
OSPF for customer's routing table to join in routing table VRF
Stop

Figure 4. 2 Configure MPLS/VPN Routing

Flow chart explanation:

Step 1: In the model of the router R1, R2, R3, R4 will join routing protocol MPLS / VPN network core of the service provider, for example on the R1.

Step 2: This step is to create a routing table to connect customers with service provider through edge router. Then, configuring more than two edge routers R1 and R2, known as router R1 is similar to R2.

Step 3: After creating the routing table to connect customers is completed, this step is to assign ports correspondingly with the routing table VRF and set up IP again. Since when they are in the routing table, all of the data of the old IP will be erased.

Step 4: The final step is to run the protocol OSPF for customers' routing table to join in routing table VRF.

Traffic Engineering

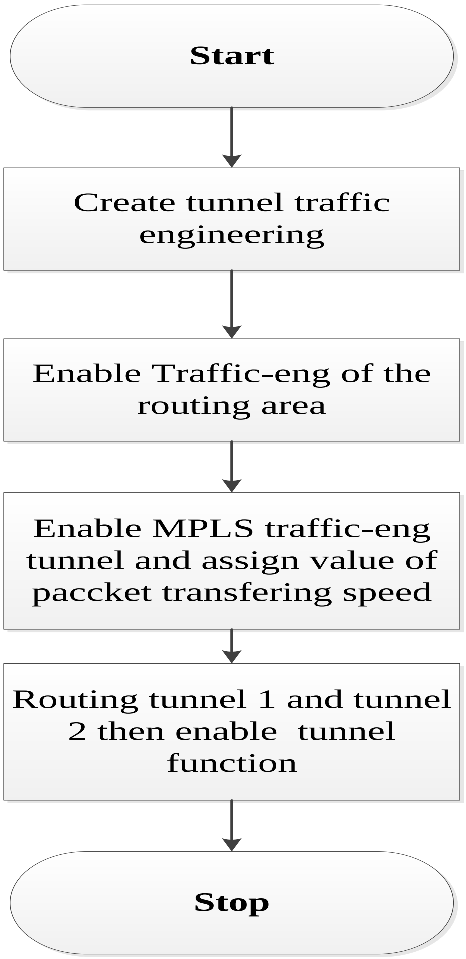

Start
Create tunnel traffic engineering
Enable Traffic-eng of the routing area
Enable MPLS traffic-eng tunnel and assign value of paccket transfering speed
Routing tunnel 1 and tunnel 2 then enable tunnel function
Stop

Figure 4. 3 Configure Traffic Engineering

Flow chart explanation:

Step 1: Create tunnel traffic engineering beside using command IP unnumbered to allow processing operations IP in interface serial without assigning IP. It can borrow another interface's IP that was configured. This method is used to save address space.

Step 2: Enable Traffic-eng of the routing area so that they could see each other through traffic-eng tunnel.

Step 3: Shows router the ways through creating tunnel and assigning value of the packet transferring speed (mb/s), for example, 2mb/s corresponds to the other router in ISP network.

Step 4: Shows the packet the way in tunnel 1 and 2 and show what tunnels to go through and enable tunnel function.

IPsec VPN

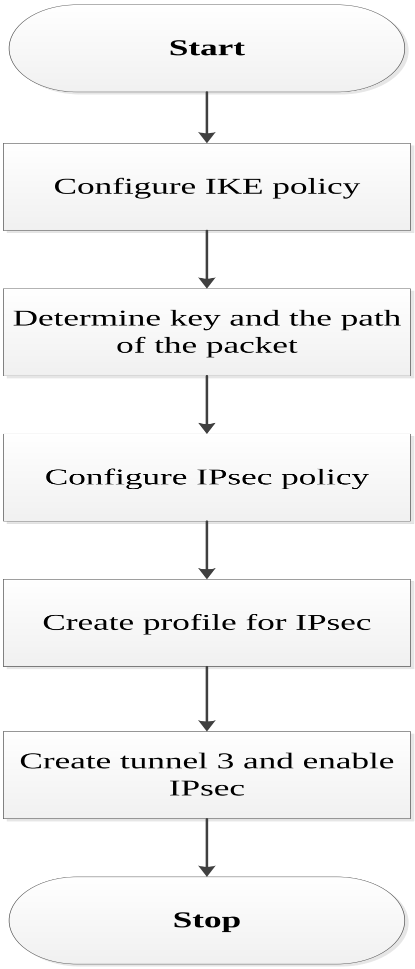


Figure 4. 4 Configure IPsec VPN

Flow chart explanation:

Step 1: Configure IKE policy.

Step 2: Determine key information and the path of the packet.

Step 3: Configure IPSEC policy.

Step 4: Create a profile for IPsec.

Step 5: Create tunnel 3, shows the address from the start and finish line and enable IPsec ipv4 then enable created profile protection mode then rout the packet destination.

4.2 Topology HSRP-DHCP

Model of installing a company network and provide redundant IP via DHCP Server for LAN

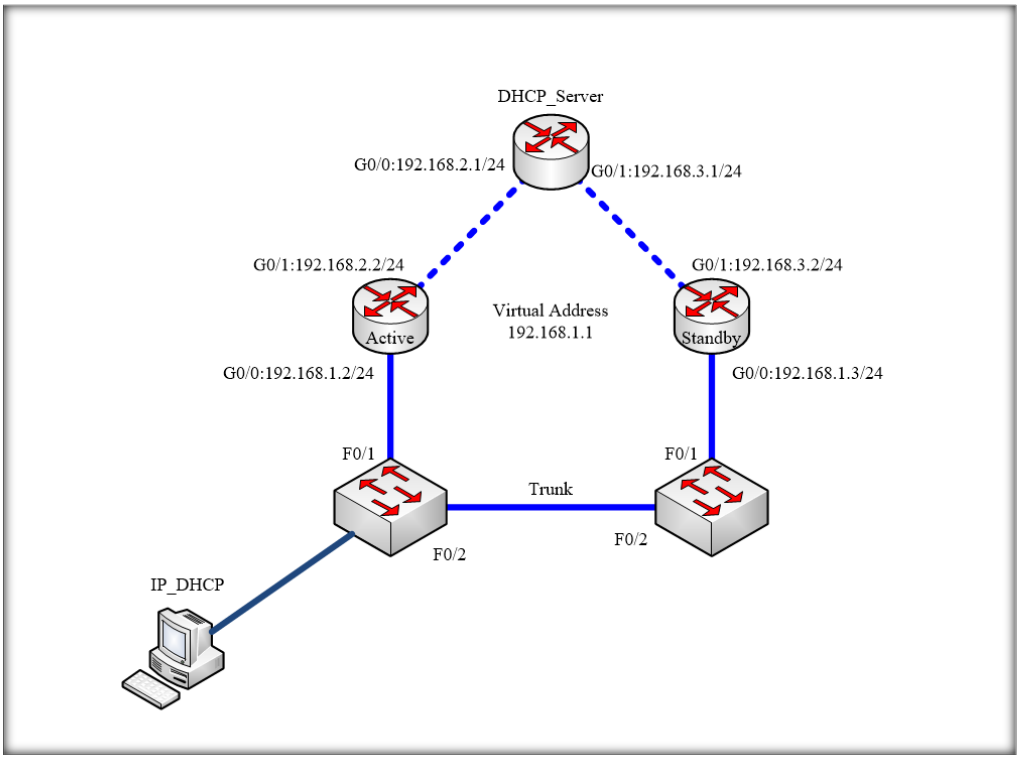


Figure 4. 5 Topology HSRP-DHCP

The functions of the routers and switches in the model:

DHCP_Server plays a role in providing the IP address for network in the LAN.

Active_Router and Standby_Router are two components of the HSRP.

SW1 and SW2 are connected together allowing other components to connect to SW1 or SW2 can see each other.

PC gets IP address from DHCP_Server.

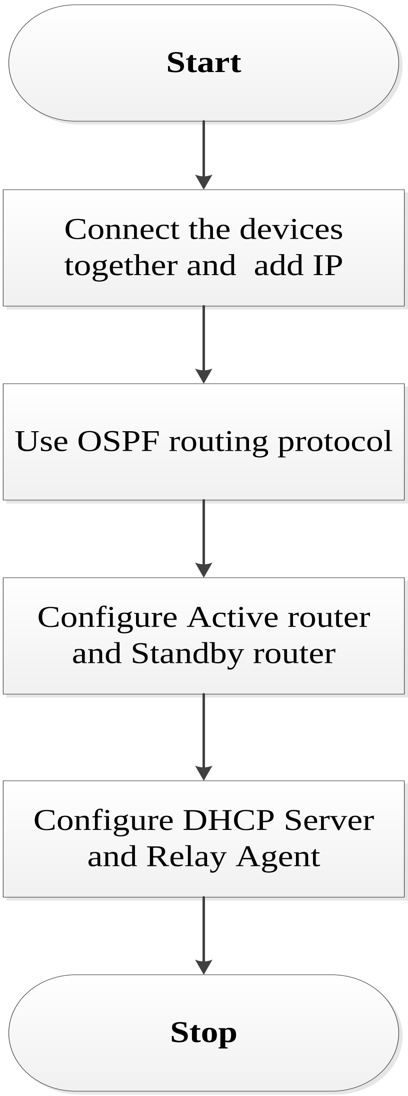

Start
Connect the devices together and add IP
Use OSPF routing protocol
Configure Active router and Standby router
Configure DHCP Server and Relay Agent
Stop

Figure 4. 6 Configure HSRP and DHCP

Flow chart explanation:

Step 1: The first step is to connect the devices together and planning of IP as shown.

Step 2: When step 1 is done, using OSPF routing protocol is a suggestion to ensure that all addresses on the LAN can see each other.

Step 3: Active router and Standby Router likely become the Active router if it has higher priority (configured preempt).

- If you do not configure the "preempt" for the Routers when Active_Router dead and Standby_Router become Active, then Active_Router resurrection cannot be active again despite Active_Router has the higher priority than Standby_Router.

- By default, HSRP router is running on the "non-preempt" means not to seize. Therefore, we need to configure "preempt" if the road network and internet needs is the highest priority.

- Standby Router is the default standby router priority = 100 < Active Router therefore it is no need to be fixed.

Step 4: Configuring DHCP Server and Relay Agent to issue dynamic IP for LAN.

4.3 Topology PPPoE ADSL

Network model of a service provider offers user ADSL to rent through DSLAM

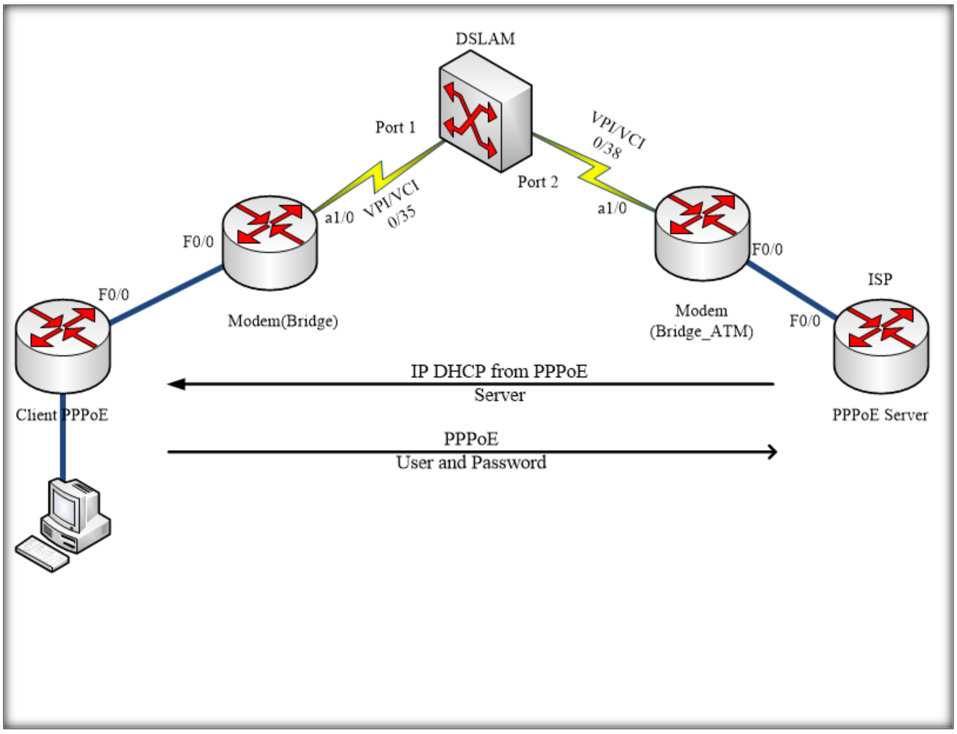


Figure 4. 7 Topology PPPoE ADSL

ISP deploying service delivery to subscribers, the address provided to the subscribers will be located within 192.168.1.10 192.168.1.254, using technology PPPoE and user authentication CHAP.

The subscriber terminal will use the DHCP to give our users while performing NAT overload mechanism for users to be able to get the Internet.

Configuring router Client_PPPoE

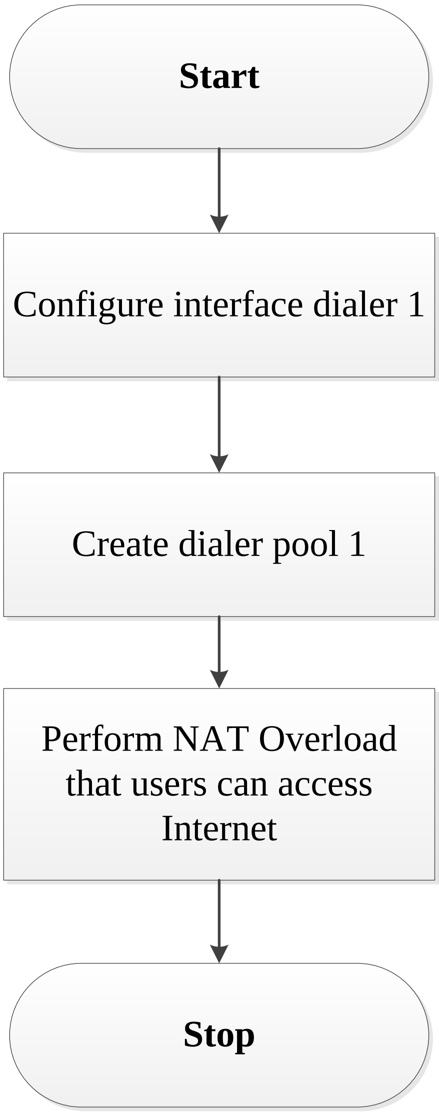

Start
Configure interface dialer 1
Create dialer pool 1
Perform NAT Overload that users can access Internet
Stop

Figure 4. 8 Configure Client_ADSL

Flow chart explanation:

Step 1: Build interface dialer 1 used to create configuration templates.

Step 2: Create a dialer pool 1 for authentication chap and enter Username and Password information from service providers.

Step 3: Perform NAT Overload mechanism so that users can access the Internet.

Configure two Bridge routers of the customers and service provider

Configuring the VPI / VCI with value 0/35 on router Brigde_Customer and the same value for VPI / VCI 0/38 on Brigde_Provider to mapped to the uplink port on the DSLAM.

Configure router PPPoE_Server of ISP service provider

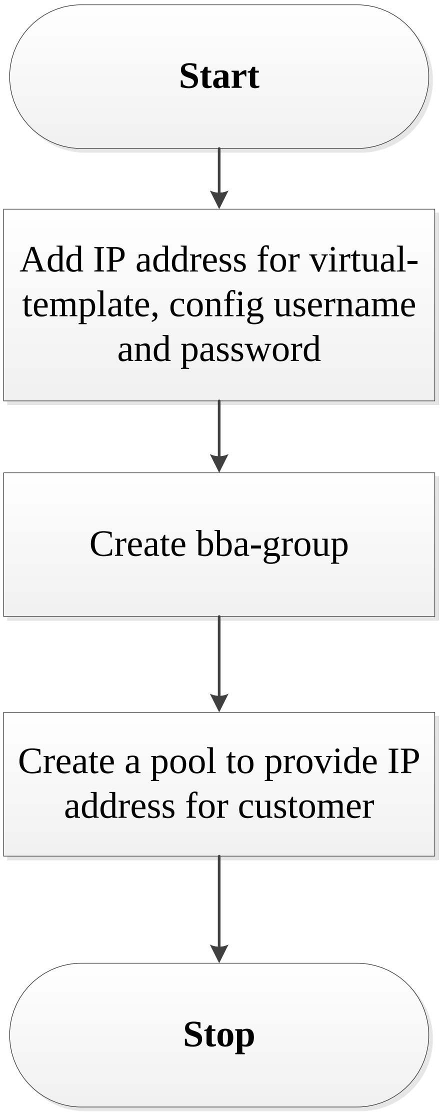

Start
Add IP address for virtual-template, config username and password
Create bba-group
Create a pool to provide IP address for customer
Stop

Figure 4. 9 Configure PPPoE_ADSL Server

Flow chart explanation:

Step 1: Assign IP address for virtual-template then configure username, password and protocol for user authentication from the service provider.

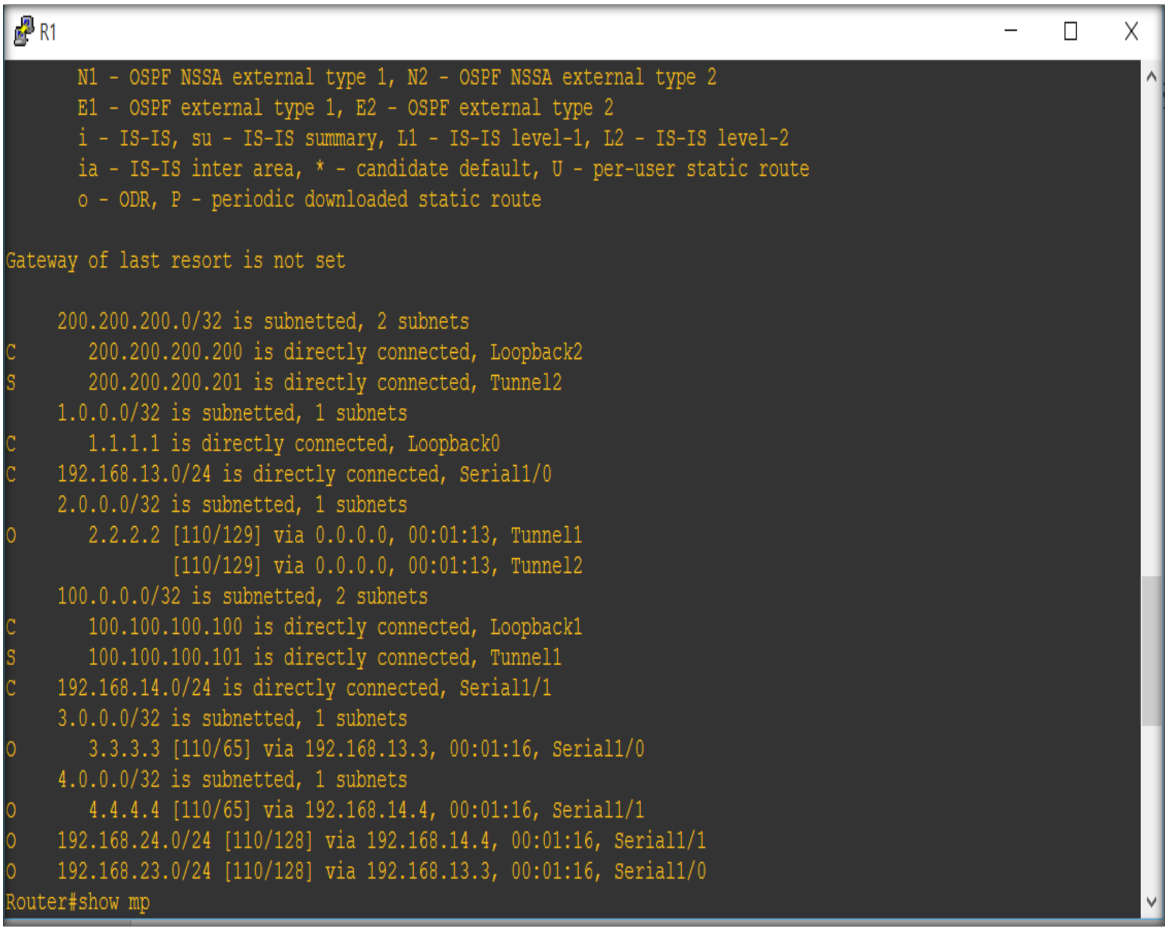
Step 2: create bba-group pppoe then let it connect to router Brigde_Provider to enable them and join in pppoe.

Step 3: Create a pool to provide IP for customer when they require to hire ADSL Internet connection.

4.4 Testing

MPLS VPN

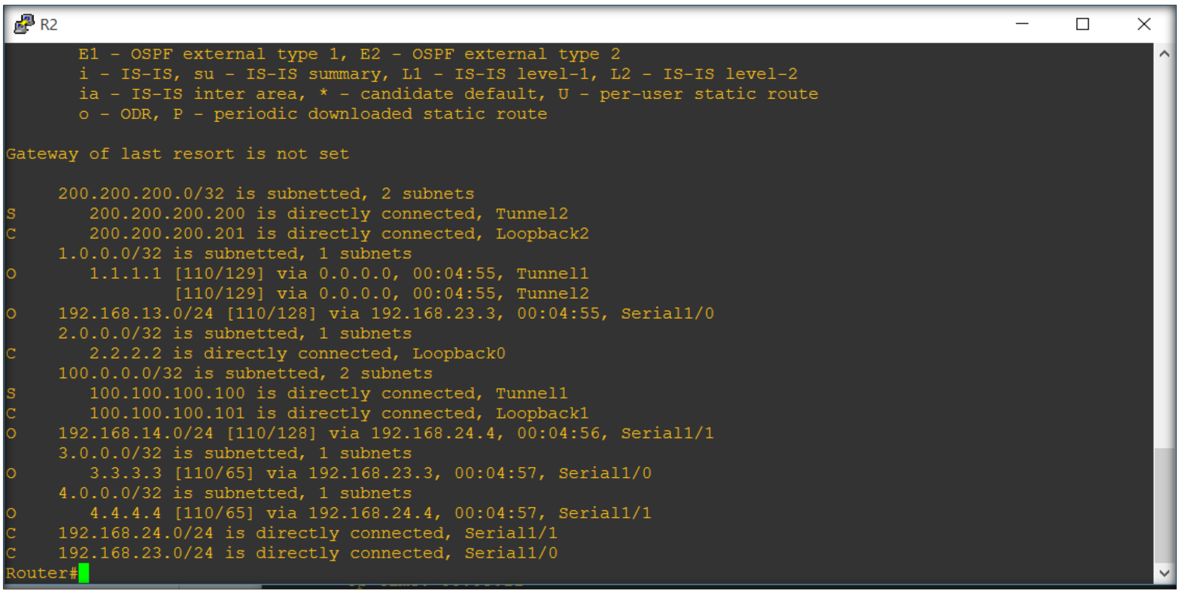
Information routing in the core network service provider.



```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     200.200.200.0/32 is subnetted, 2 subnets
C       200.200.200.200 is directly connected, Loopback2
S       200.200.200.201 is directly connected, Tunnel2
     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
C    192.168.13.0/24 is directly connected, Serial1/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/129] via 0.0.0.0, 00:01:13, Tunnel1
                [110/129] via 0.0.0.0, 00:01:13, Tunnel2
     100.0.0.0/32 is subnetted, 2 subnets
C       100.100.100.100 is directly connected, Loopback1
S       100.100.100.101 is directly connected, Tunnel1
C    192.168.14.0/24 is directly connected, Serial1/1
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/65] via 192.168.13.3, 00:01:16, Serial1/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/65] via 192.168.14.4, 00:01:16, Serial1/1
O    192.168.24.0/24 [110/128] via 192.168.14.4, 00:01:16, Serial1/1
O    192.168.23.0/24 [110/128] via 192.168.13.3, 00:01:16, Serial1/0
Router#show mp
```

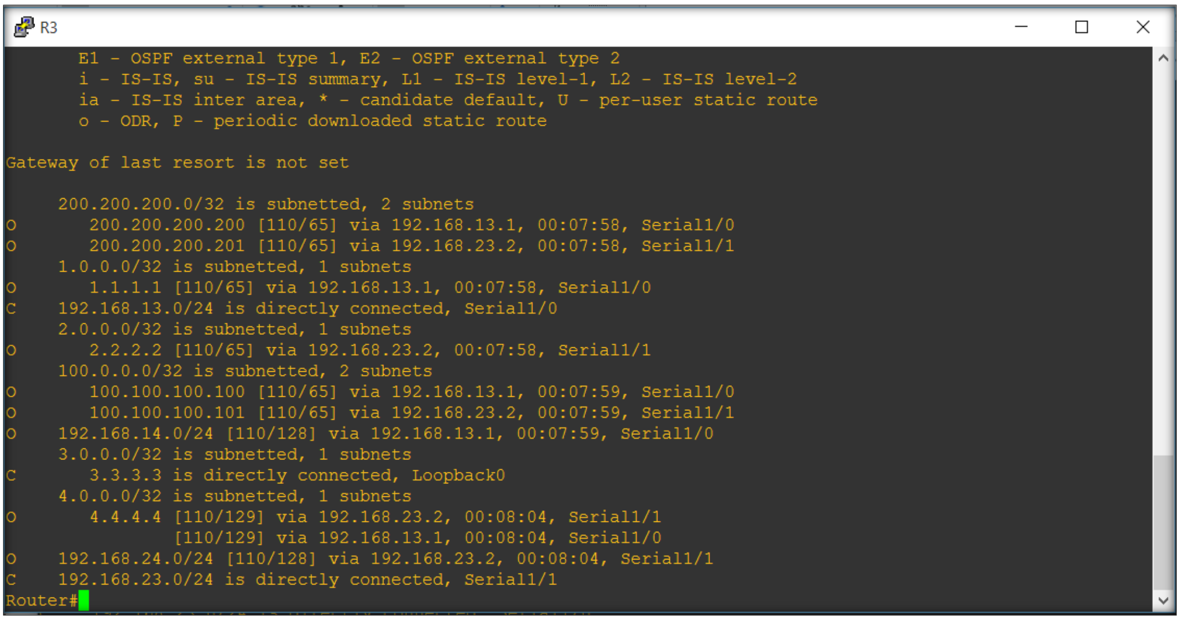
Figure 4. 10 Routing on R1

Figure 4.10 shows routing information on R1, you see all subnets can see each other. Its means on R1 will go to the address through the port as serial, tunnel or specific addresses connected directly to the port on the R1, similar to figure 4.11, 4:12, 4:13, 4:14, 4:15



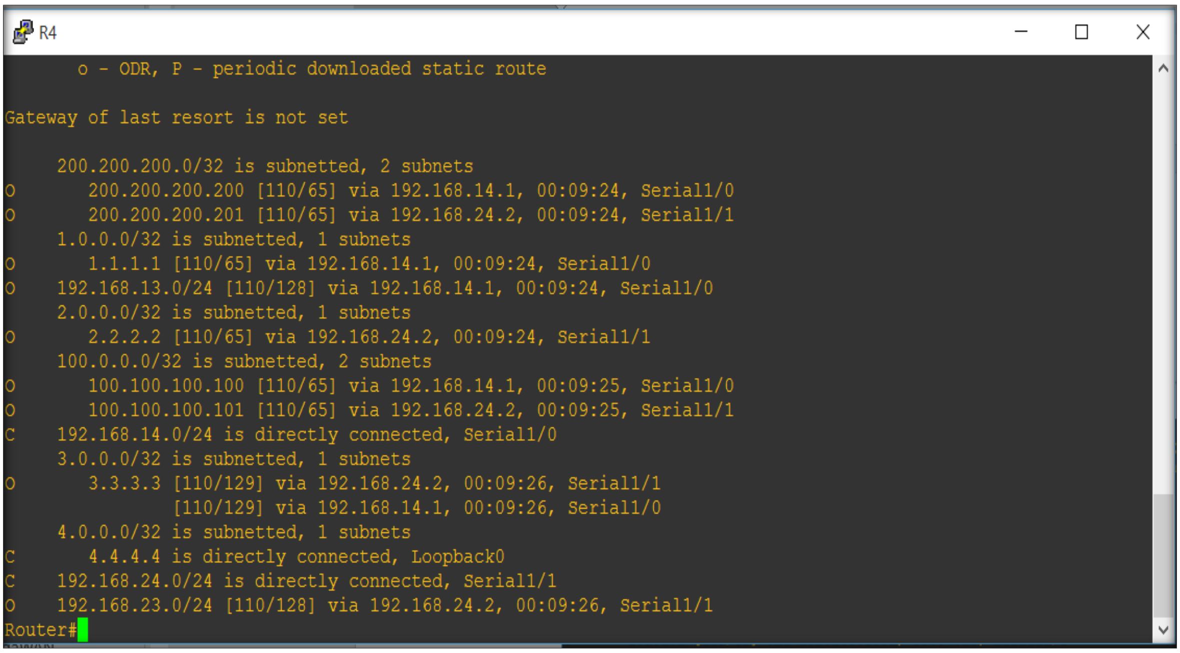
```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     200.200.200.0/32 is subnetted, 2 subnets
S       200.200.200.200 is directly connected, Tunnel2
C       200.200.200.201 is directly connected, Loopback2
     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/129] via 0.0.0.0, 00:04:55, Tunnel1
                [110/129] via 0.0.0.0, 00:04:55, Tunnel2
O    192.168.13.0/24 [110/128] via 192.168.23.3, 00:04:55, Serial1/0
     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
     100.0.0.0/32 is subnetted, 2 subnets
S       100.100.100.100 is directly connected, Tunnel1
C       100.100.100.101 is directly connected, Loopback1
O    192.168.14.0/24 [110/128] via 192.168.24.4, 00:04:56, Serial1/1
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/65] via 192.168.23.3, 00:04:57, Serial1/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/65] via 192.168.24.4, 00:04:57, Serial1/1
C    192.168.24.0/24 is directly connected, Serial1/1
C    192.168.23.0/24 is directly connected, Serial1/0
Router#
```

Figure 4. 11 Routing on R2



```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     200.200.200.0/32 is subnetted, 2 subnets
O       200.200.200.200 [110/65] via 192.168.13.1, 00:07:58, Serial1/0
O       200.200.200.201 [110/65] via 192.168.23.2, 00:07:58, Serial1/1
     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/65] via 192.168.13.1, 00:07:58, Serial1/0
C    192.168.13.0/24 is directly connected, Serial1/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/65] via 192.168.23.2, 00:07:58, Serial1/1
     100.0.0.0/32 is subnetted, 2 subnets
O       100.100.100.100 [110/65] via 192.168.13.1, 00:07:59, Serial1/0
O       100.100.100.101 [110/65] via 192.168.23.2, 00:07:59, Serial1/1
O    192.168.14.0/24 [110/128] via 192.168.13.1, 00:07:59, Serial1/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/129] via 192.168.23.2, 00:08:04, Serial1/1
                [110/129] via 192.168.13.1, 00:08:04, Serial1/0
O    192.168.24.0/24 [110/128] via 192.168.23.2, 00:08:04, Serial1/1
C    192.168.23.0/24 is directly connected, Serial1/1
Router#
```

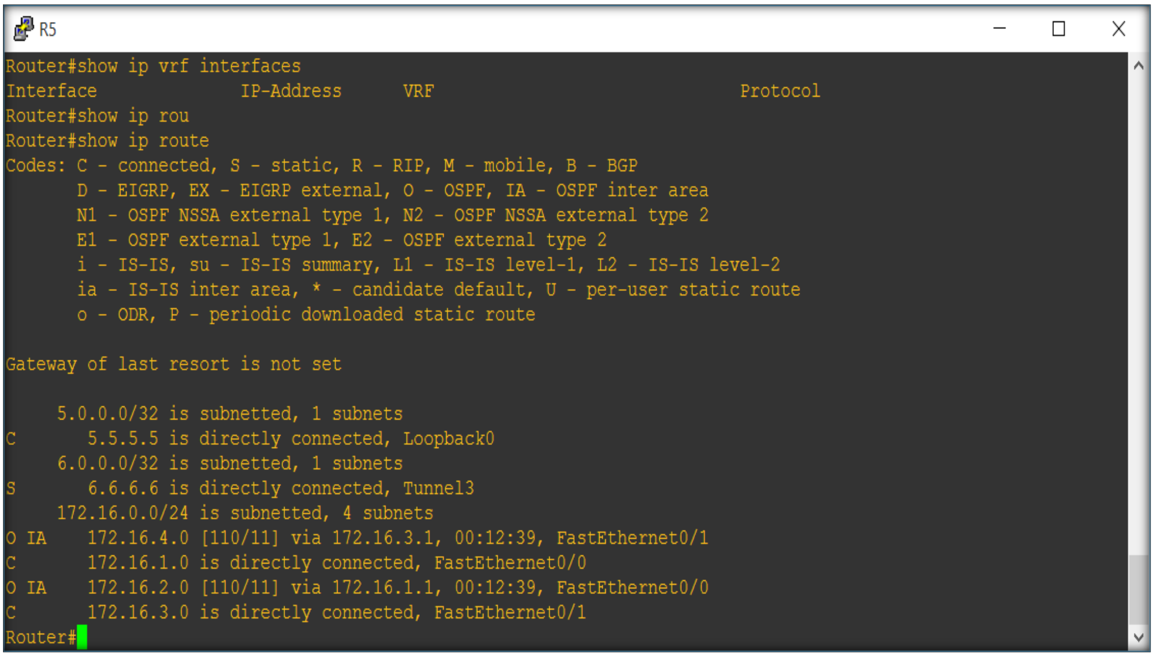
Figure 4. 12 Routing on R3



```
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     200.200.200.0/32 is subnetted, 2 subnets
O       200.200.200.200 [110/65] via 192.168.14.1, 00:09:24, Serial1/0
O       200.200.200.201 [110/65] via 192.168.24.2, 00:09:24, Serial1/1
     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/65] via 192.168.14.1, 00:09:24, Serial1/0
O    192.168.13.0/24 [110/128] via 192.168.14.1, 00:09:24, Serial1/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/65] via 192.168.24.2, 00:09:24, Serial1/1
     100.0.0.0/32 is subnetted, 2 subnets
O       100.100.100.100 [110/65] via 192.168.14.1, 00:09:25, Serial1/0
O       100.100.100.101 [110/65] via 192.168.24.2, 00:09:25, Serial1/1
C    192.168.14.0/24 is directly connected, Serial1/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/129] via 192.168.24.2, 00:09:26, Serial1/1
                [110/129] via 192.168.14.1, 00:09:26, Serial1/0
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
C    192.168.24.0/24 is directly connected, Serial1/1
O    192.168.23.0/24 [110/128] via 192.168.24.2, 00:09:26, Serial1/1
Router#
```

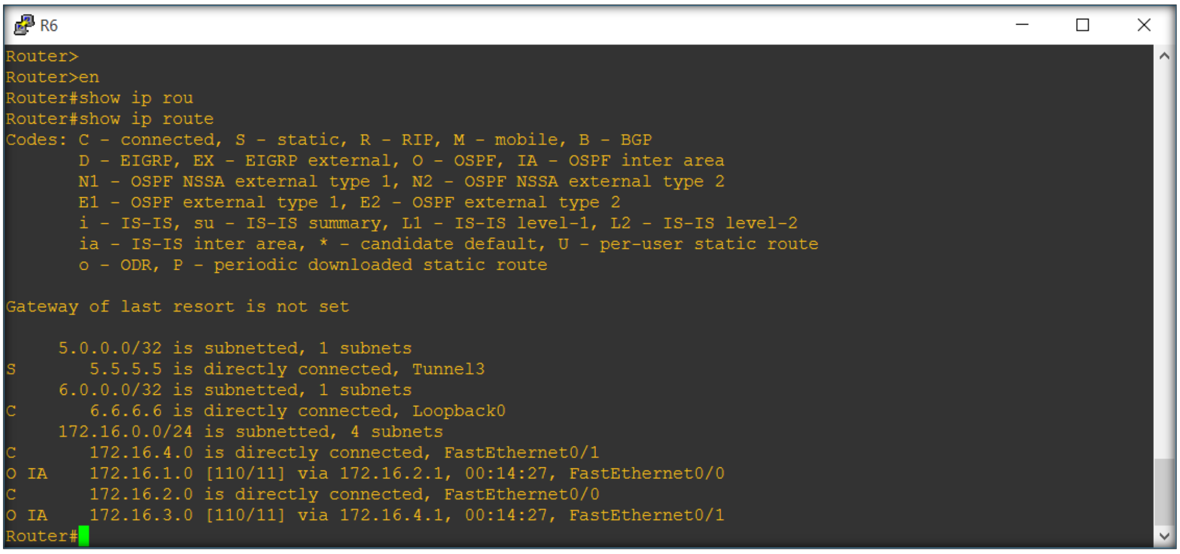
Figure 4. 13 Routing on R4

Routing information of client



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

Gateway of last resort is not set

     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
S       6.6.6.6 is directly connected, Tunnel3
     172.16.0.0/24 is subnetted, 4 subnets
O IA    172.16.4.0 [110/11] via 172.16.3.1, 00:12:39, FastEthernet0/1
C       172.16.1.0 is directly connected, FastEthernet0/0
O IA    172.16.2.0 [110/11] via 172.16.1.1, 00:12:39, FastEthernet0/0
C       172.16.3.0 is directly connected, FastEthernet0/1
Router#
```

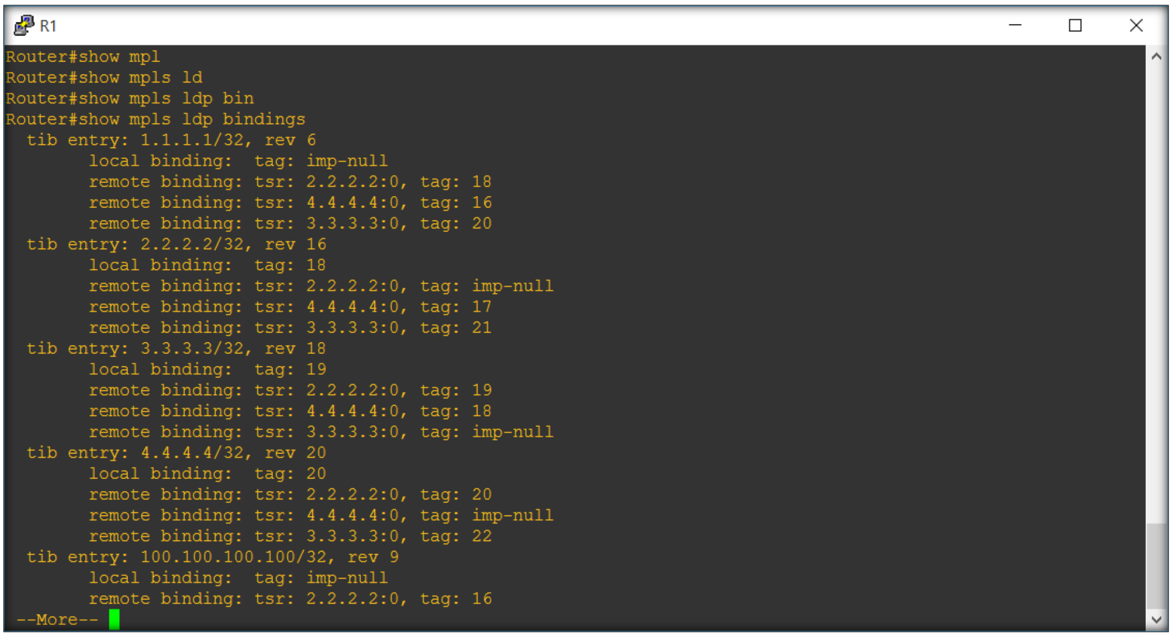
Figure 4. 14 Routing on R5



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

Gateway of last resort is not set

     5.0.0.0/32 is subnetted, 1 subnets
S       5.5.5.5 is directly connected, Tunnel3
     6.0.0.0/32 is subnetted, 1 subnets
C       6.6.6.6 is directly connected, Loopback0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.4.0 is directly connected, FastEthernet0/1
O IA    172.16.1.0 [110/11] via 172.16.2.1, 00:14:27, FastEthernet0/0
C       172.16.2.0 is directly connected, FastEthernet0/0
O IA    172.16.3.0 [110/11] via 172.16.4.1, 00:14:27, FastEthernet0/1
Router#
```

Figure 4. 15 Routing on R6

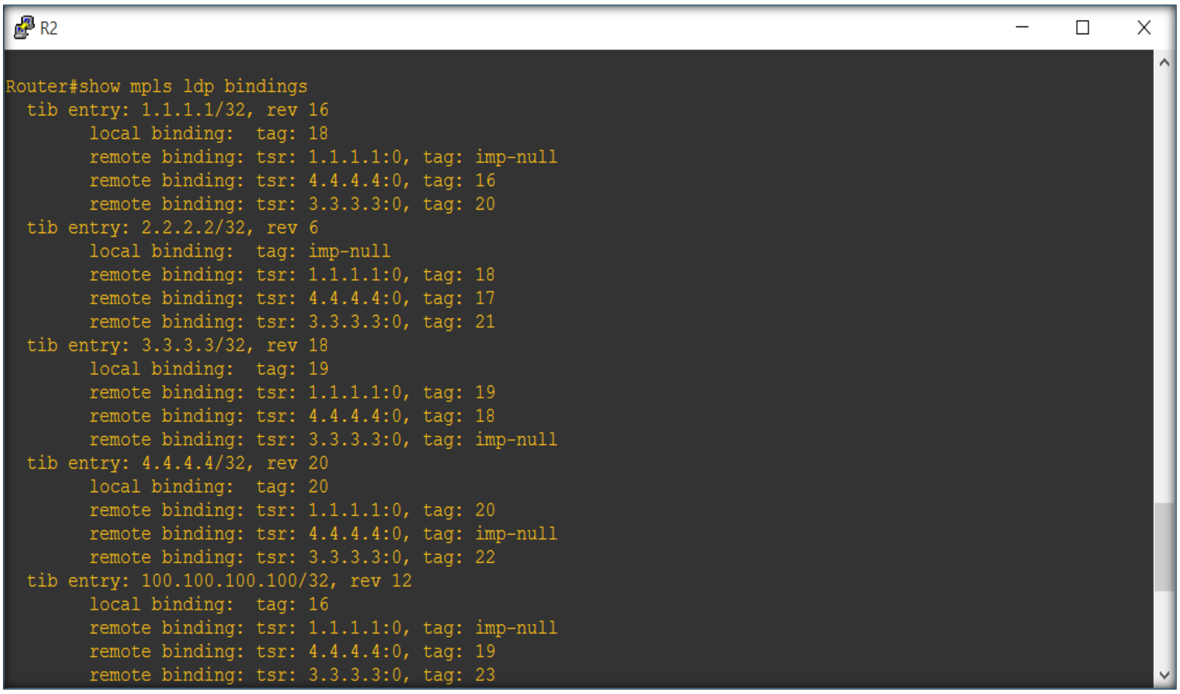
Check the LDP on the router



```
Router#show mpl
Router#show mpls ld
Router#show mpls ldp bin
Router#show mpls ldp bindings
  tib entry: 1.1.1.1/32, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 18
        remote binding: tsr: 4.4.4.4:0, tag: 16
        remote binding: tsr: 3.3.3.3:0, tag: 20
  tib entry: 2.2.2.2/32, rev 16
        local binding:  tag: 18
        remote binding: tsr: 2.2.2.2:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 17
        remote binding: tsr: 3.3.3.3:0, tag: 21
  tib entry: 3.3.3.3/32, rev 18
        local binding:  tag: 19
        remote binding: tsr: 2.2.2.2:0, tag: 19
        remote binding: tsr: 4.4.4.4:0, tag: 18
        remote binding: tsr: 3.3.3.3:0, tag: imp-null
  tib entry: 4.4.4.4/32, rev 20
        local binding:  tag: 20
        remote binding: tsr: 2.2.2.2:0, tag: 20
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
        remote binding: tsr: 3.3.3.3:0, tag: 22
  tib entry: 100.100.100.100/32, rev 9
        local binding:  tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 16
 --More--
```

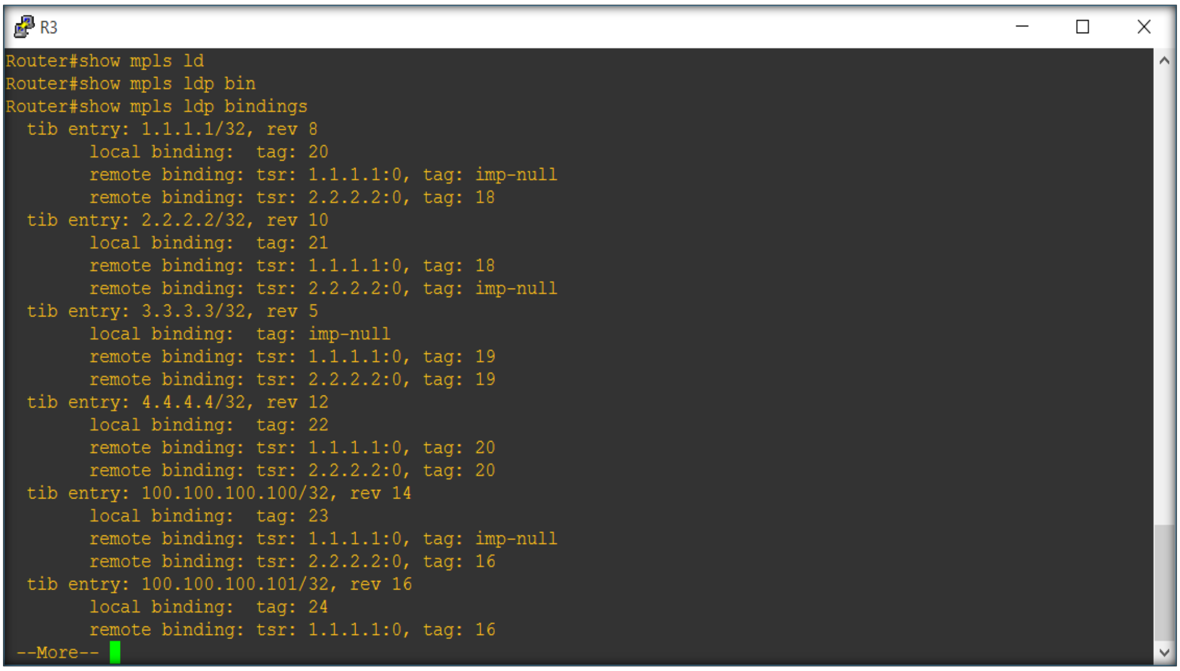
Figure 4. 16 MPLS LDP on R1

We see that the packets are labeled LDP on R1. At here, it will take responsibility for packaging and labeling 16, 17, 18, 19 and 20. Then they will be moved to the neighboring routers. The receiving router will continue to package and send to other router, which has already been routed, similar to figure 4.17, 4.18, 4.19, 4.20.



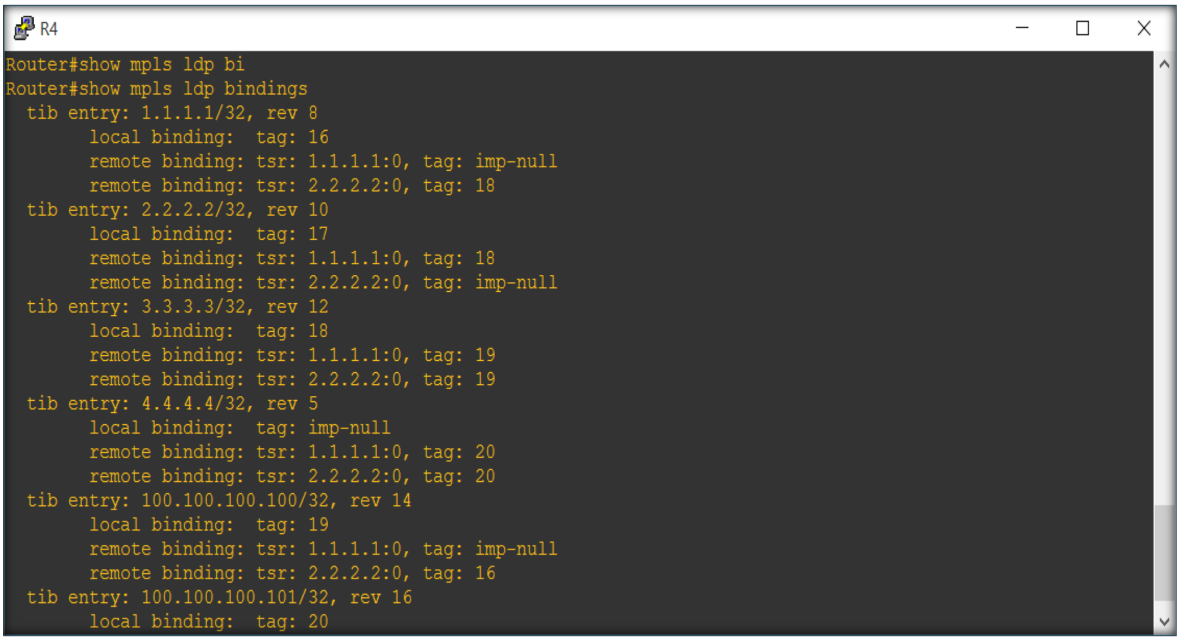
```
Router#show mpls ldp bindings
  tib entry: 1.1.1.1/32, rev 16
        local binding:  tag: 18
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 16
        remote binding: tsr: 3.3.3.3:0, tag: 20
  tib entry: 2.2.2.2/32, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: 18
        remote binding: tsr: 4.4.4.4:0, tag: 17
        remote binding: tsr: 3.3.3.3:0, tag: 21
  tib entry: 3.3.3.3/32, rev 18
        local binding:  tag: 19
        remote binding: tsr: 1.1.1.1:0, tag: 19
        remote binding: tsr: 4.4.4.4:0, tag: 18
        remote binding: tsr: 3.3.3.3:0, tag: imp-null
  tib entry: 4.4.4.4/32, rev 20
        local binding:  tag: 20
        remote binding: tsr: 1.1.1.1:0, tag: 20
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
        remote binding: tsr: 3.3.3.3:0, tag: 22
  tib entry: 100.100.100.100/32, rev 12
        local binding:  tag: 16
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 19
        remote binding: tsr: 3.3.3.3:0, tag: 23
```

Figure 4. 17 MPLS LDP on R2



```
Router#show mpls ld
Router#show mpls ldp bin
Router#show mpls ldp bindings
  tib entry: 1.1.1.1/32, rev 8
        local binding:  tag: 20
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 18
  tib entry: 2.2.2.2/32, rev 10
        local binding:  tag: 21
        remote binding: tsr: 1.1.1.1:0, tag: 18
        remote binding: tsr: 2.2.2.2:0, tag: imp-null
  tib entry: 3.3.3.3/32, rev 5
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: 19
        remote binding: tsr: 2.2.2.2:0, tag: 19
  tib entry: 4.4.4.4/32, rev 12
        local binding:  tag: 22
        remote binding: tsr: 1.1.1.1:0, tag: 20
        remote binding: tsr: 2.2.2.2:0, tag: 20
  tib entry: 100.100.100.100/32, rev 14
        local binding:  tag: 23
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 16
  tib entry: 100.100.100.101/32, rev 16
        local binding:  tag: 24
        remote binding: tsr: 1.1.1.1:0, tag: 16
 --More--
```

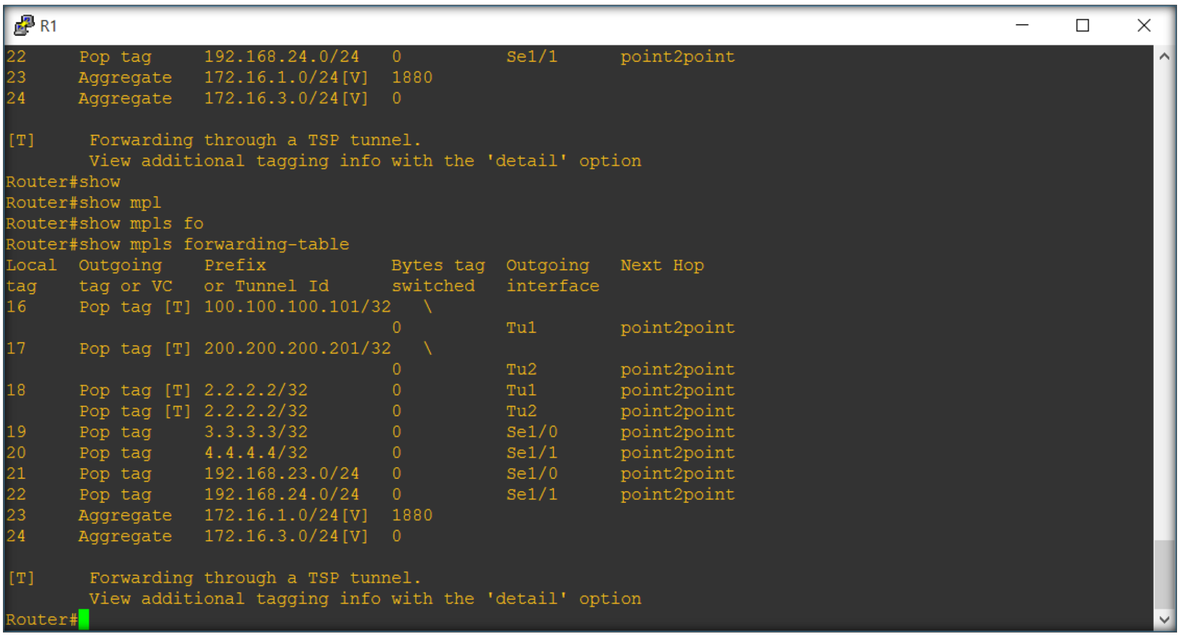
Figure 4. 18 MPLS LDP on R3



```
Router#show mpls ldp bi
Router#show mpls ldp bindings
  tib entry: 1.1.1.1/32, rev 8
        local binding:  tag: 16
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 18
  tib entry: 2.2.2.2/32, rev 10
        local binding:  tag: 17
        remote binding: tsr: 1.1.1.1:0, tag: 18
        remote binding: tsr: 2.2.2.2:0, tag: imp-null
  tib entry: 3.3.3.3/32, rev 12
        local binding:  tag: 18
        remote binding: tsr: 1.1.1.1:0, tag: 19
        remote binding: tsr: 2.2.2.2:0, tag: 19
  tib entry: 4.4.4.4/32, rev 5
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: 20
        remote binding: tsr: 2.2.2.2:0, tag: 20
  tib entry: 100.100.100.100/32, rev 14
        local binding:  tag: 19
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 2.2.2.2:0, tag: 16
  tib entry: 100.100.100.101/32, rev 16
        local binding:  tag: 20
```

Figure 4. 19 MPLS LDP on R4

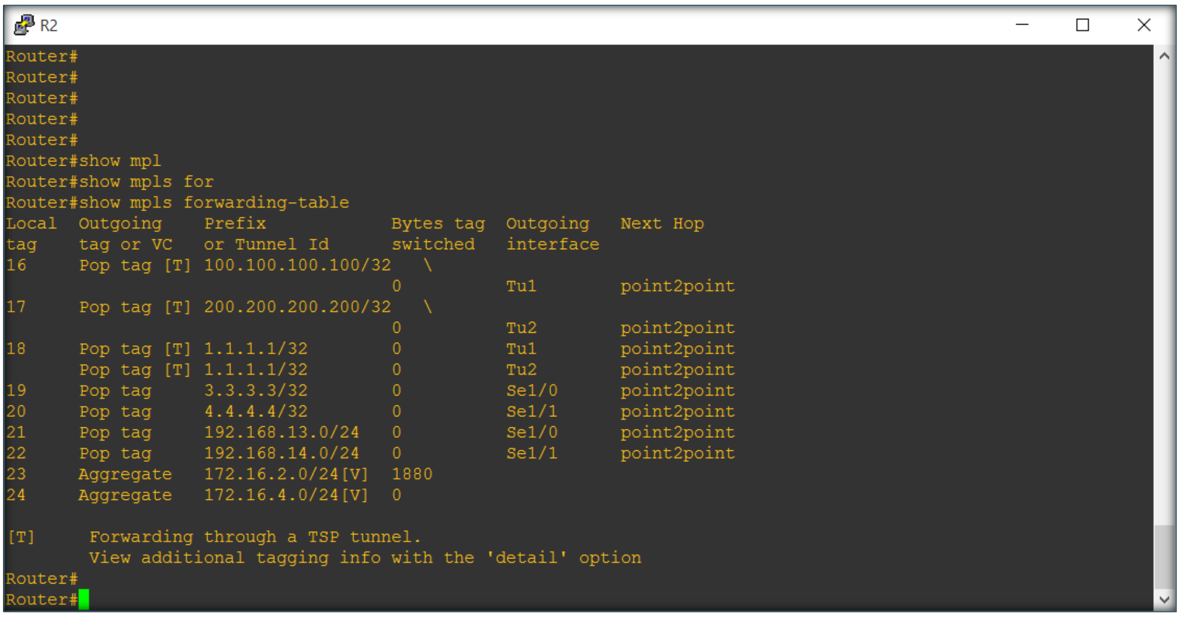
Table LFIB



```
22     Pop tag      192.168.24.0/24   0          Se1/1      point2point
23     Aggregate    172.16.1.0/24[V]  1880
24     Aggregate    172.16.3.0/24[V]  0

[T]     Forwarding through a TSP tunnel.
        View additional tagging info with the 'detail' option
Router#show
Router#show mpl
Router#show mpls fo
Router#show mpls forwarding-table
Local  Outgoing     Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC    or Tunnel Id      switched   interface
16     Pop tag [T]  100.100.100.101/32   \
                                      0          Tu1        point2point
17     Pop tag [T]  200.200.200.201/32   \
                                      0          Tu2        point2point
18     Pop tag [T]  2.2.2.2/32        0          Tu1        point2point
       Pop tag [T]  2.2.2.2/32        0          Tu2        point2point
19     Pop tag      3.3.3.3/32        0          Se1/0      point2point
20     Pop tag      4.4.4.4/32        0          Se1/1      point2point
21     Pop tag      192.168.23.0/24   0          Se1/0      point2point
22     Pop tag      192.168.24.0/24   0          Se1/1      point2point
23     Aggregate    172.16.1.0/24[V]  1880
24     Aggregate    172.16.3.0/24[V]  0

[T]     Forwarding through a TSP tunnel.
        View additional tagging info with the 'detail' option
Router#
```

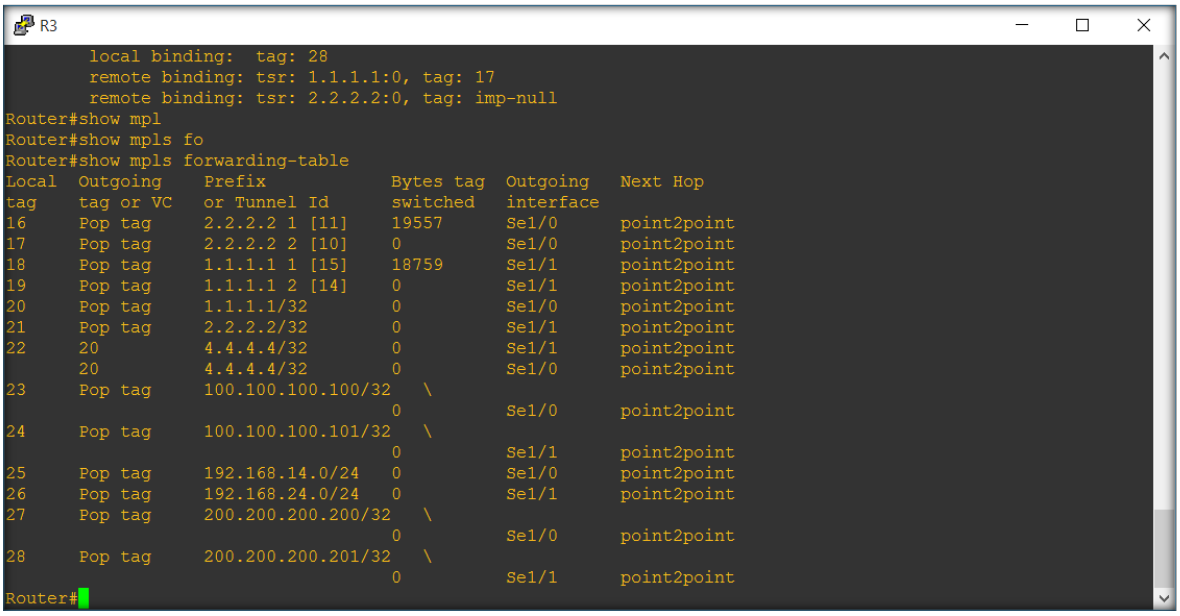
Figure 4. 20 MPLS Forwarding-table on R1

Checking forwarding-table information. We can see that the labels, which serve the switching process, have been transferred between routers for every IP subnet and then they have appeared on the label-switching board together. We have completed the core MPLS building, similar to figure 4.21, 4.22, 4.23.



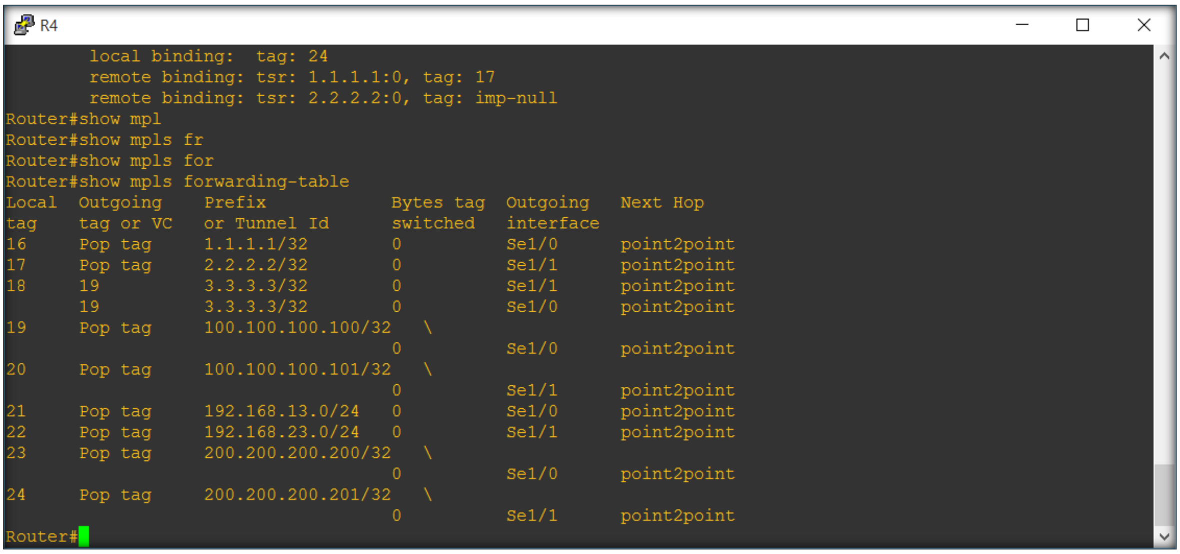
```
Router#
Router#
Router#
Router#
Router#
Router#show mpl
Router#show mpls for
Router#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag [T] 100.100.100.100/32   \
                                     0          Tu1        point2point
17     Pop tag [T] 200.200.200.200/32   \
                                     0          Tu2        point2point
18     Pop tag [T] 1.1.1.1/32        0          Tu1        point2point
       Pop tag [T] 1.1.1.1/32        0          Tu2        point2point
19     Pop tag     3.3.3.3/32        0          Se1/0      point2point
20     Pop tag     4.4.4.4/32        0          Se1/1      point2point
21     Pop tag     192.168.13.0/24   0          Se1/0      point2point
22     Pop tag     192.168.14.0/24   0          Se1/1      point2point
23     Aggregate   172.16.2.0/24[V]  1880
24     Aggregate   172.16.4.0/24[V]  0

[T]     Forwarding through a TSP tunnel.
        View additional tagging info with the 'detail' option
Router#
Router#
```

Figure 4. 21 MPLS Forwarding-table on R2



```
        local binding:  tag: 28
        remote binding: tsr: 1.1.1.1:0, tag: 17
        remote binding: tsr: 2.2.2.2:0, tag: imp-null
Router#show mpl
Router#show mpls fo
Router#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     2.2.2.2 1 [11]    19557      Se1/0      point2point
17     Pop tag     2.2.2.2 2 [10]    0          Se1/0      point2point
18     Pop tag     1.1.1.1 1 [15]    18759      Se1/1      point2point
19     Pop tag     1.1.1.1 2 [14]    0          Se1/1      point2point
20     Pop tag     1.1.1.1/32        0          Se1/0      point2point
21     Pop tag     2.2.2.2/32        0          Se1/1      point2point
22     20          4.4.4.4/32        0          Se1/1      point2point
       20          4.4.4.4/32        0          Se1/0      point2point
23     Pop tag     100.100.100.100/32   \
                                     0          Se1/0      point2point
24     Pop tag     100.100.100.101/32   \
                                     0          Se1/1      point2point
25     Pop tag     192.168.14.0/24   0          Se1/0      point2point
26     Pop tag     192.168.24.0/24   0          Se1/1      point2point
27     Pop tag     200.200.200.200/32   \
                                     0          Se1/0      point2point
28     Pop tag     200.200.200.201/32   \
                                     0          Se1/1      point2point
Router#
```

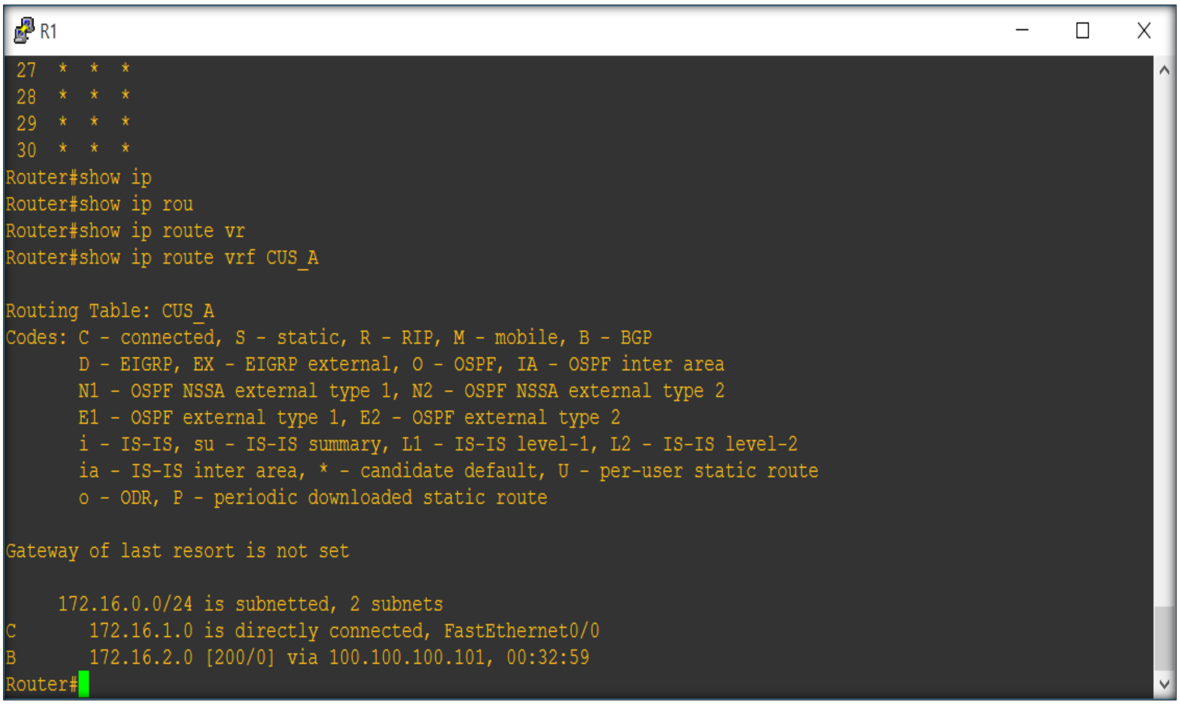
Figure 4. 22 MPLS Forwarding-table on R3



```
        local binding:  tag: 24
        remote binding: tsr: 1.1.1.1:0, tag: 17
        remote binding: tsr: 2.2.2.2:0, tag: imp-null
Router#show mpl
Router#show mpls fr
Router#show mpls for
Router#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     1.1.1.1/32        0          Se1/0      point2point
17     Pop tag     2.2.2.2/32        0          Se1/1      point2point
18     19          3.3.3.3/32        0          Se1/1      point2point
       19          3.3.3.3/32        0          Se1/0      point2point
19     Pop tag     100.100.100.100/32   \
                                     0          Se1/0      point2point
20     Pop tag     100.100.100.101/32   \
                                     0          Se1/1      point2point
21     Pop tag     192.168.13.0/24   0          Se1/0      point2point
22     Pop tag     192.168.23.0/24   0          Se1/1      point2point
23     Pop tag     200.200.200.200/32   \
                                     0          Se1/0      point2point
24     Pop tag     200.200.200.201/32   \
                                     0          Se1/1      point2point
Router#
```

Figure 4. 23 MPLS Forwarding-table on R4

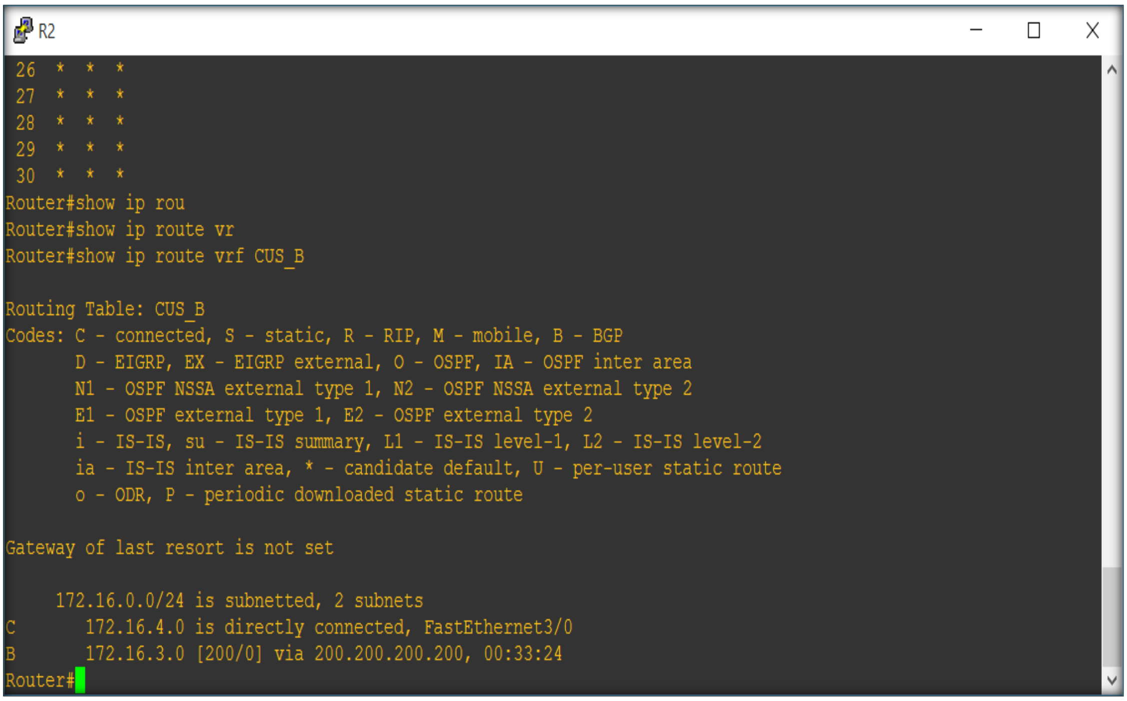
Routing table vrf of customer



```
 27  *  *  *
 28  *  *  *
 29  *  *  *
 30  *  *  *
Router#show ip
Router#show ip rou
Router#show ip route vr
Router#show ip route vrf CUS_A

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
B       172.16.2.0 [200/0] via 100.100.100.101, 00:32:59
Router#
```

Figure 4. 24 Routing table vrf on CUS_A

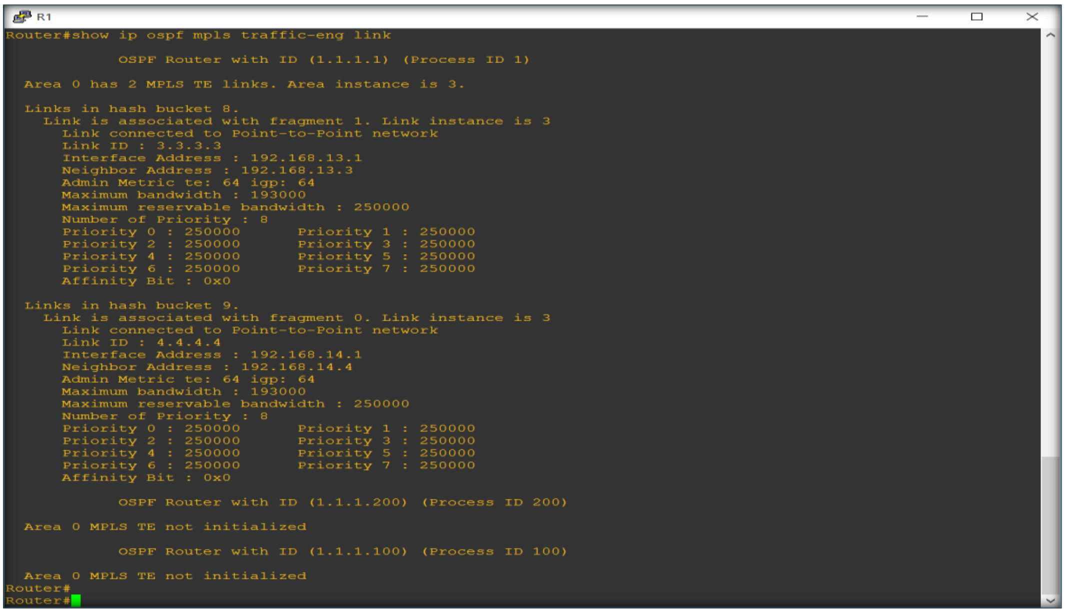
Figure 4.24 shows vrf routing table of CUS_A on R1. Its means only IP addresses which are saved in this VRF board can communicate with the nearby router, similar to figure 4.25.



```
26  *  *  *
27  *  *  *
28  *  *  *
29  *  *  *
30  *  *  *
Router#show ip rou
Router#show ip route vr
Router#show ip route vrf CUS_B

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.4.0 is directly connected, FastEthernet3/0
B       172.16.3.0 [200/0] via 200.200.200.200, 00:33:24
Router#
```

Figure 4. 25 Routing table vrf on CUS_B

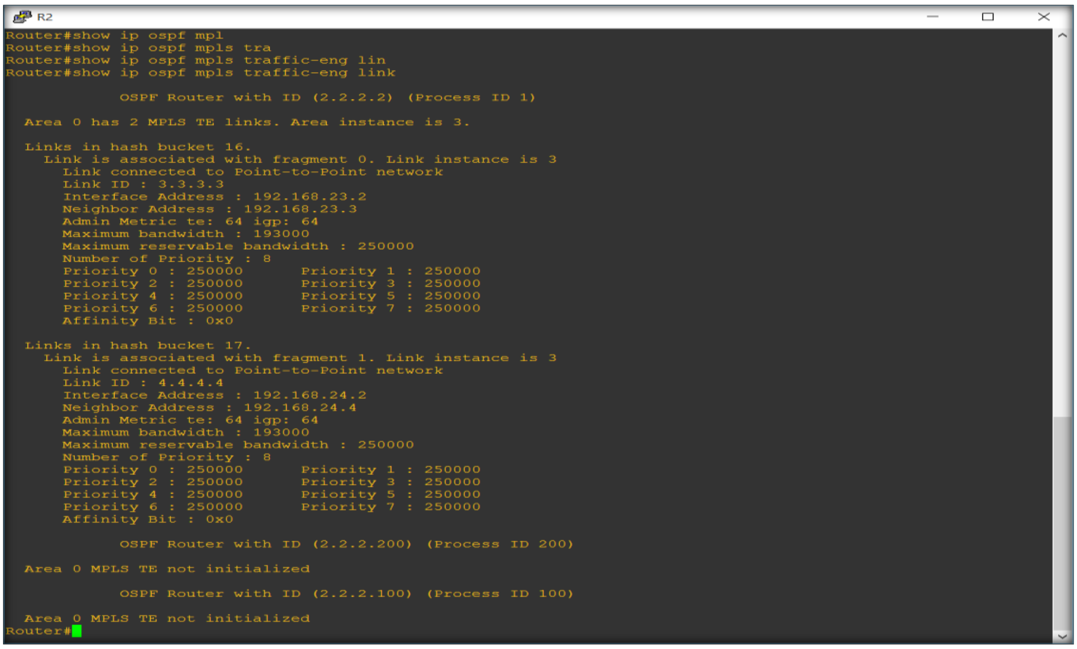
Information OSPF MPLS traffic-eng



```
Router#show ip ospf mpls traffic-eng link

            OSPF Router with ID (1.1.1.1) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 3.

  Links in hash bucket 8.
    Link is associated with fragment 1. Link instance is 3
      Link connected to Point-to-Point network
      Link ID : 3.3.3.3
      Interface Address : 192.168.13.1
      Neighbor Address : 192.168.13.3
      Admin Metric te: 64 igp: 64
      Maximum bandwidth : 193000
      Maximum reservable bandwidth : 250000
      Number of Priority : 8
      Priority 0 : 250000       Priority 1 : 250000
      Priority 2 : 250000       Priority 3 : 250000
      Priority 4 : 250000       Priority 5 : 250000
      Priority 6 : 250000       Priority 7 : 250000
      Affinity Bit : 0x0

  Links in hash bucket 9.
    Link is associated with fragment 0. Link instance is 3
      Link connected to Point-to-Point network
      Link ID : 4.4.4.4
      Interface Address : 192.168.14.1
      Neighbor Address : 192.168.14.4
      Admin Metric te: 64 igp: 64
      Maximum bandwidth : 193000
      Maximum reservable bandwidth : 250000
      Number of Priority : 8
      Priority 0 : 250000       Priority 1 : 250000
      Priority 2 : 250000       Priority 3 : 250000
      Priority 4 : 250000       Priority 5 : 250000
      Priority 6 : 250000       Priority 7 : 250000
      Affinity Bit : 0x0

            OSPF Router with ID (1.1.1.200) (Process ID 200)

  Area 0 MPLS TE not initialized

            OSPF Router with ID (1.1.1.100) (Process ID 100)

  Area 0 MPLS TE not initialized
Router#
Router#
```

Figure 4. 26 Information OSPF MPLS traffic-eng link on R1

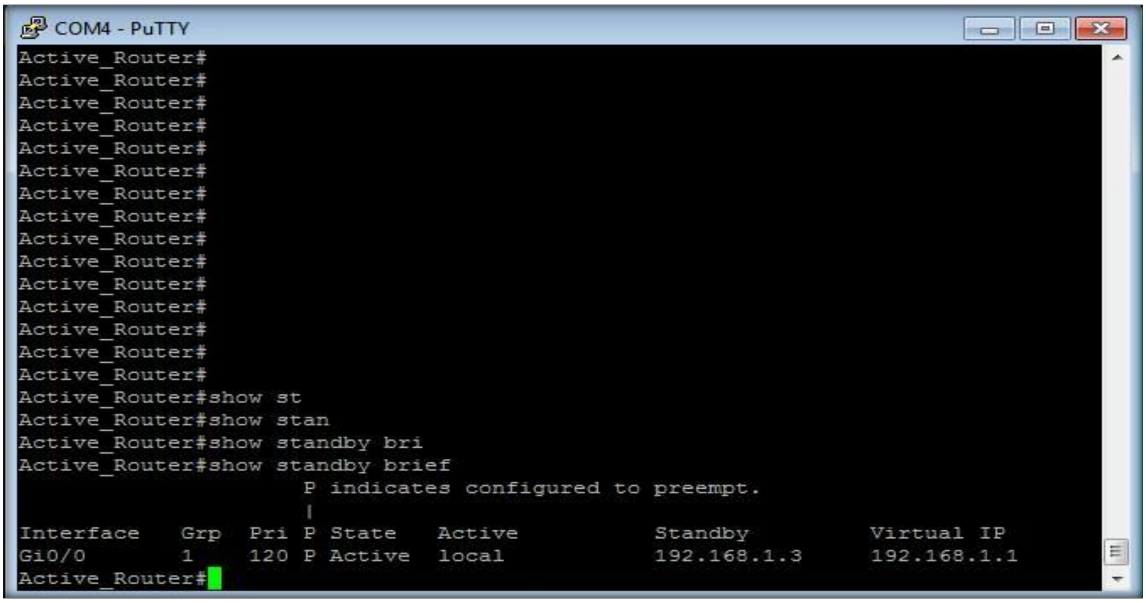
Showing information about routing traffic on R1. It shows the path to the neighboring router and adjust the bandwidth manually, for instance, the bandwidth here is 25mb/s, similar to figure 4.27.



```
Router#show ip ospf mpl
Router#show ip ospf mpls tra
Router#show ip ospf mpls traffic-eng lin
Router#show ip ospf mpls traffic-eng link

            OSPF Router with ID (2.2.2.2) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 3.

  Links in hash bucket 16.
    Link is associated with fragment 0. Link instance is 3
      Link connected to Point-to-Point network
      Link ID : 3.3.3.3
      Interface Address : 192.168.23.2
      Neighbor Address : 192.168.23.3
      Admin Metric te: 64 igp: 64
      Maximum bandwidth : 193000
      Maximum reservable bandwidth : 250000
      Number of Priority : 8
      Priority 0 : 250000       Priority 1 : 250000
      Priority 2 : 250000       Priority 3 : 250000
      Priority 4 : 250000       Priority 5 : 250000
      Priority 6 : 250000       Priority 7 : 250000
      Affinity Bit : 0x0

  Links in hash bucket 17.
    Link is associated with fragment 1. Link instance is 3
      Link connected to Point-to-Point network
      Link ID : 4.4.4.4
      Interface Address : 192.168.24.2
      Neighbor Address : 192.168.24.4
      Admin Metric te: 64 igp: 64
      Maximum bandwidth : 193000
      Maximum reservable bandwidth : 250000
      Number of Priority : 8
      Priority 0 : 250000       Priority 1 : 250000
      Priority 2 : 250000       Priority 3 : 250000
      Priority 4 : 250000       Priority 5 : 250000
      Priority 6 : 250000       Priority 7 : 250000
      Affinity Bit : 0x0

            OSPF Router with ID (2.2.2.200) (Process ID 200)

  Area 0 MPLS TE not initialized

            OSPF Router with ID (2.2.2.100) (Process ID 100)

  Area 0 MPLS TE not initialized
Router#
```

Figure 4. 27 Information OSPF MPLS traffic-eng link on R2

HSRP and DHCP in Enterprise

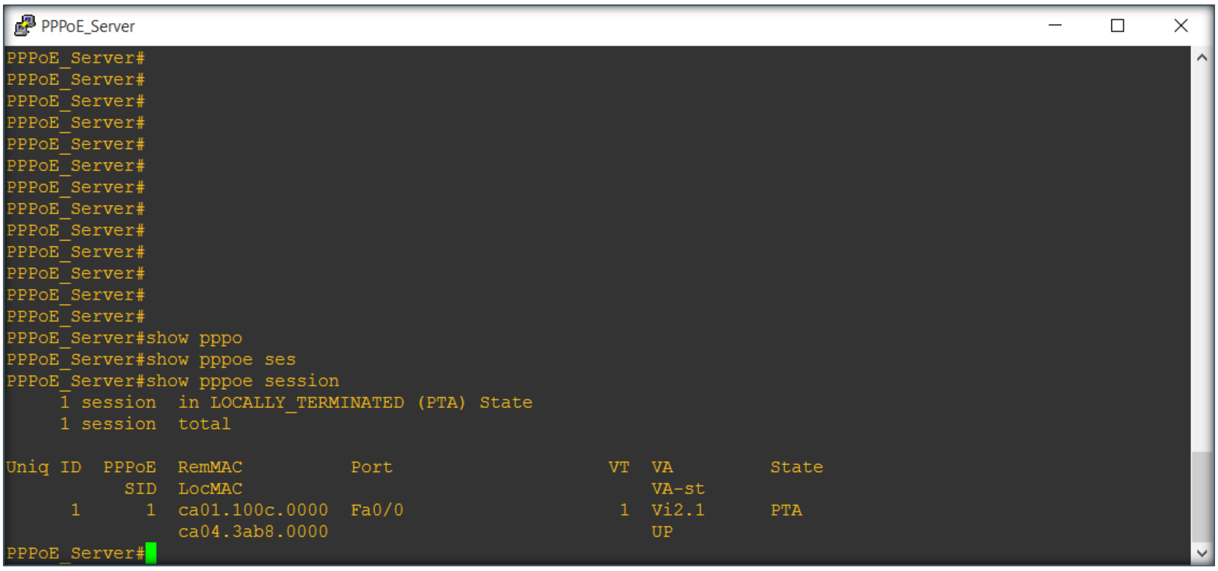


```
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#
Active_Router#show st
Active_Router#show stan
Active_Router#show standby bri
Active_Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0       1    120 P Active  local           192.168.1.3     192.168.1.1
Active_Router#
```

Figure 4. 28 Show standby brief

The role of G0/0 is an active router which is enable and has an address 192.168.1.3 when the active router got failure at standby for example active router dead, it will automatic turn on a preventive router.

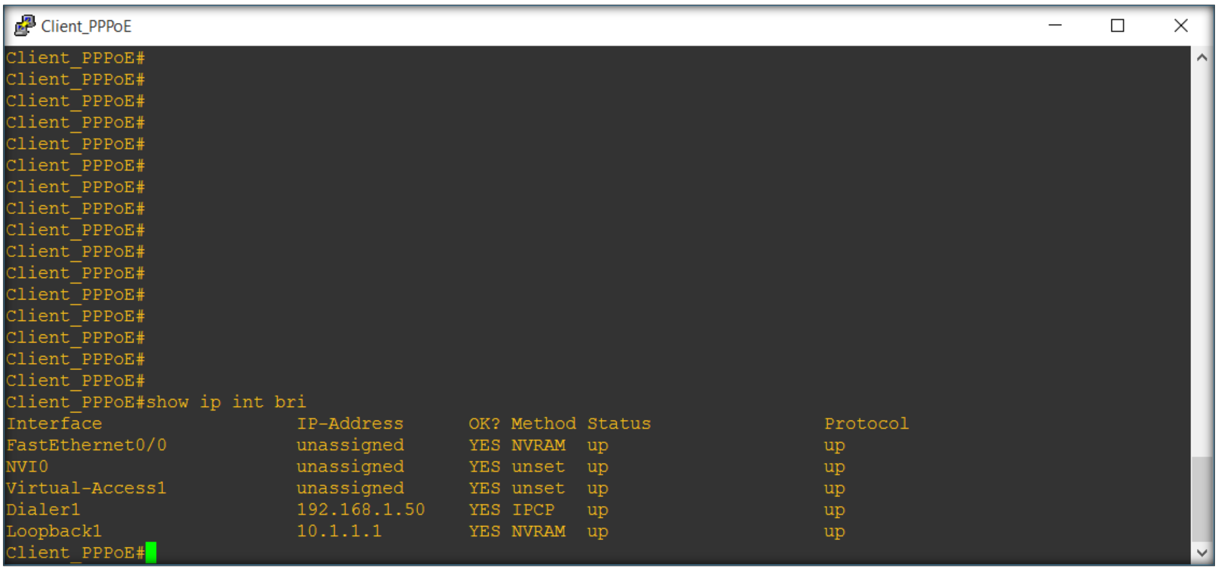
PPPoE ADSL



```
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#show pppo
PPPoE_Server#show pppoe ses
PPPoE_Server#show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
      1      1  ca01.100c.0000  Fa0/0                    1  Vi2.1      PTA
                ca04.3ab8.0000                              UP
PPPoE_Server#
```

Figure 4. 29 show pppoe session on PPPoE_Server

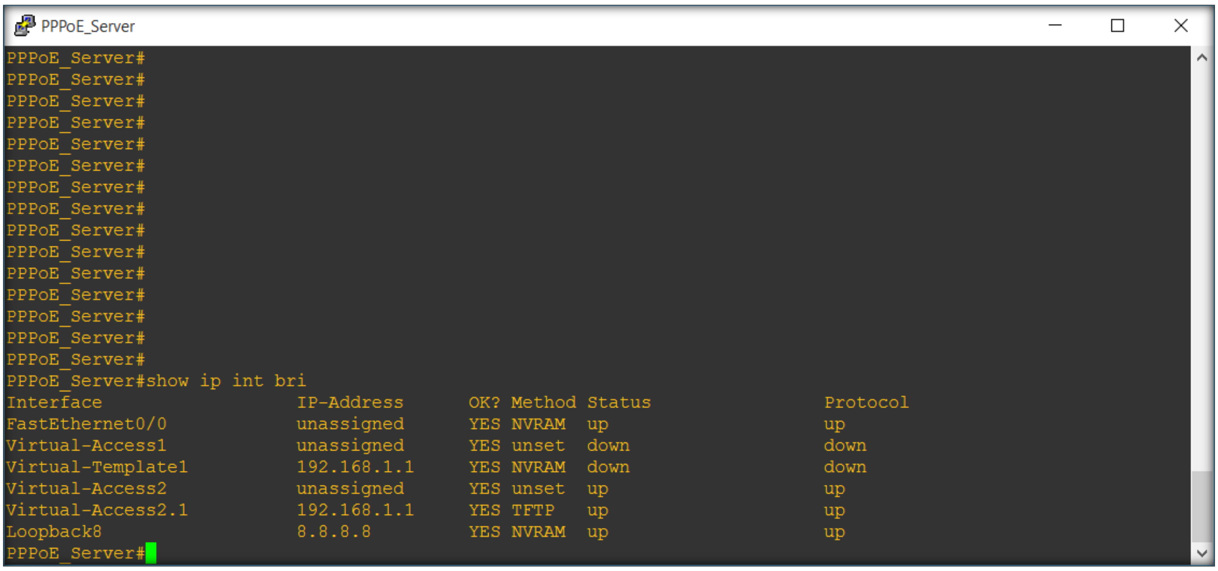
Checking pppoe session up or down.



```
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#show ip int bri
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
NVI0                       unassigned      YES unset  up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Dialer1                    192.168.1.50    YES IPCP   up                    up
Loopback1                  10.1.1.1        YES NVRAM  up                    up
Client_PPPoE#
```

Figure 4. 30 Show ip interface brief on Client_PPPoE

Checking Client_PPPoE is received IP Address from Server.

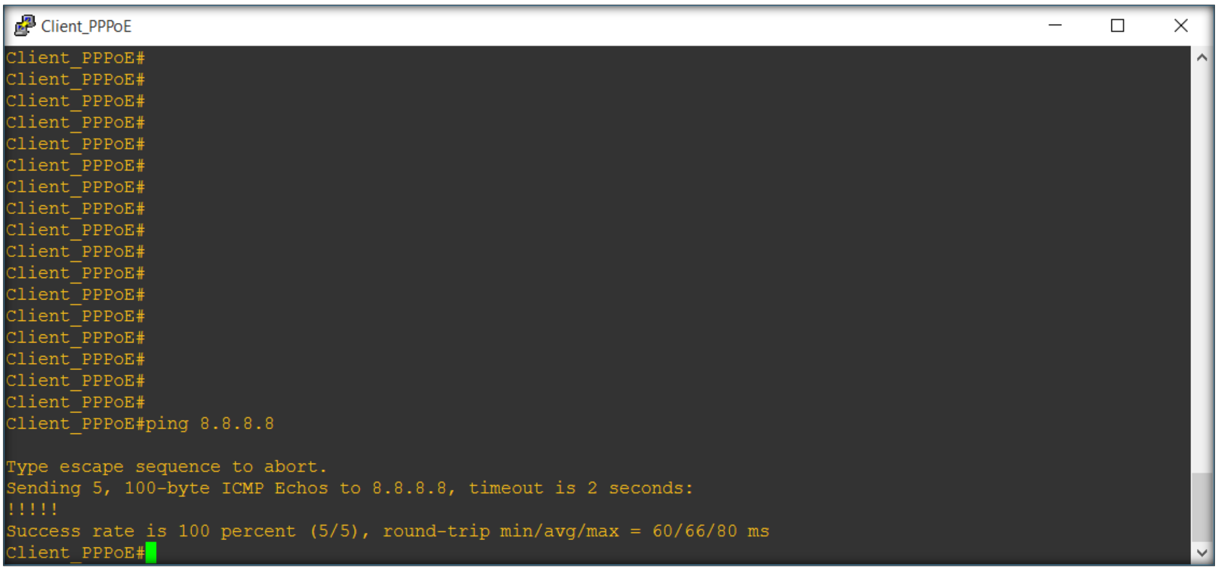


```
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#
PPPoE_Server#show ip int bri
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
Virtual-Access1            unassigned      YES unset  down                  down
Virtual-Template1          192.168.1.1     YES NVRAM  down                  down
Virtual-Access2            unassigned      YES unset  up                    up
Virtual-Access2.1          192.168.1.1     YES TFTP   up                    up
Loopback8                  8.8.8.8         YES NVRAM  up                    up
PPPoE_Server#
```

Figure 4. 31 Show ip interface brief

Checking status information of PPPoE_Server after having configured it.

Check from the client pinged host



```
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#
Client_PPPoE#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/80 ms
Client_PPPoE#
```

Figure 4. 32 Ping PPPoE_Server from Client_PPPoE

Checking Client_PPPoE can ping to Internet.

Chapter 5: Conclusion

5.1 Summary and conclusion

The project helps us get an overview about VPN, while introducing new technologies which is being favored at present is MPLS, a technology that combines edge routing network and fast packet switching core network. One of the important applications of the MPLS VPN MPLS. Topic researches in detail MPLS VPN, enables secure communication between the client sites when transmitted over the network and also ensures the path of the packets are safer transmissions.

Thanks to the advantages of service quality over IP networks and the new VPN deployments have overcome many technological problems that are unresolved before. MPLS is an effective option in deployment of enterprise information infrastructure.

However, virtual private networks based on MPLS still have difficulty to be overcome, such as:

- Simultaneous supporting multiple protocols will face complex issues in the pot.

- Difficult to support QoS continuously.

- Unifying VC needs to be research much more detail to solve problems inserting packets when identical labels.

5.2 Future work

In future if service vendors use QoS they can supply a variety of services with guaranteed quality for a maximum number of clients.

Current development trend of MPLS is ATOM (Any traffic Over MPLS) that is capable to meet any kind of services such as: voice, video, fax, data, etc.

Solving the problem of bandwidth and installation costs.

BIBLIOGRAPHY

[1] "Cisco," [Online]. Available: www.cisco.com.

[2] B. Morgan and N. Lovering, CCNP ISCW Official Exam Certification Guide, Indianapolis: Cisco Press, 2008.

[3] J. Guichard and I. Pepelnjak, MPLS and VPN Architectures, Cisco Press, 2002.

[4] D. Hucaby, S. McQuerry and A. Whitaker, Cisco Router Configurationg Handbook, Second Edition, 2010.

[5] Trung Tâm Tin Học VNPRO, CCNA Routing & Switching LabPro, TP. Hồ Chí Minh: Nhà Xuất Bản Thông Tin và Truyền Thông, 2011.

Appendix

Step 1: In the model for the router R1, R2, R3, R4 join routing protocol MPLS / VPN network core of the service provider, for example on the R1:

```
R1(config)#router ospf 1
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# network 192.168.13.0 0.0.0.255 area 0
R1(config-router)# network 192.168.14.0 0.0.0.255 area 0
R1(config-router)# network 100.100.100.100 0.0.0.0 area 0
R1(config-router)# network 200.200.200.200 0.0.0.0 area 0
```

Step 2: Next, we create a routing table to connect customers with service provider through edge router. We will configure more than 2 edge routers R1 and R2, specifically router R1 is similar to R2

```
R1(config)#ip vrf CUS_A
R1(config-vrf)#rd 1:1
R1(config-vrf)# route-target export 1:1
R1(config-vrf)# route-target import 1:1
R1(config-vrf)#bgp next-hop Loopback1

R1(config)#ip vrf CUS_B
R1(config-vrf)#rd 1:2
R1(config-vrf)# route-target export 1:2
R1(config-vrf)# route-target import 1:2
R1(config-vrf)#bgp next-hop Loopback2
```

Step 3: Assign ports correspondingly with the routing table VRF and then set up IP again since when they are in the routing table, all of the data of the old IP will be erased

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding CUS_A
R1(config-if)#ip address 172.16.1.1 255.255.255.0
```

```
R1(config)#interface FastEthernet3/0
R1(config-if)#ip vrf forwarding CUS_B
R1(config-if)#ip address 172.16.3.1 255.255.255.0
```

Step 4: Run the protocol ospf for customers' routing table to join in routing table VRF

```
R1(config)#router ospf 100 vrf CUS_A
R1(config-router)#router-id 1.1.1.100
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config)#router ospf 200 vrf CUS_B
R1(config-router)#router-id 1.1.1.200
R1(config-router)#network 172.16.3.0 0.0.0.255 area 0
```

Traffic Engineering

Step 1: Create tunnel traffic engineering beside using command IP unnumbered to allow processing operations IP in interface serial without assigning IP. It can borrow another interface's IP that was configured. This method is used to save address space.

```
R1(config)#interface Tunnel1
R1(config-if)#ip unnumbered Loopback0
R1(config-if)#mpls ip
R1(config-if)#tunnel destination 2.2.2.2
R1(config-if)#tunnel mode mpls traffic-eng
R1(config-if)#tunnel mpls traffic-eng autoroute announce
R1(config-if)# tunnel mpls traffic-eng path-option 8 explicit name TUNNEL1
R1(config-if)# tunnel mpls traffic-eng path-option 9 explicit name TUNNEL2

R1(config)#interface Tunnel2
R1(config-if)#ip unnumbered Loopback0
R1(config-if)#mpls ip
R1(config-if)#tunnel destination 2.2.2.2
R1(config-if)#tunnel mode mpls traffic-eng
```

```
R1(config-if)#tunnel mpls traffic-eng autoroute announce
R1(config-if)# tunnel mpls traffic-eng path-option 8 explicit name TUNNEL2
R1(config-if)# tunnel mpls traffic-eng path-option 9 explicit name TUNNEL1
```

Step 2: Enable Traffic-eng of the routing area so that they could see each other through traffic-eng tunnel

```
R1(config)#router ospf 1
R1(config-router)#mpls traffic-eng router-id Loopback0
R1(config-router)#mpls traffic-eng area 0
```

Step 3: Show router the ways through created tunnel and assign value of the packet transferring speed (mb/s), the example here is 2mb/s which are similar to the other router in ISP network.

```
R1(config)#interface serial1/0
R1(config-if)#mpls ip
R1(config)#mpls traffic-eng tunnels
R1(config)#ip rsvp bandwidth 2000 2000

R1(config)#interface serial1/1
R1(config-if)#mpls ip
R1(config)#mpls traffic-eng tunnels
R1(config)#ip rsvp bandwidth 2000 2000
```

Step 4: Show the packet the way in tunnel 1 and 2 and show what tunnels to go through and enable tunnel function

```
R1(config)#ip route 100.100.100.101 255.255.255.255 Tunnel1
R1(config)#ip route 200.200.200.201 255.255.255.255 Tunnel2

R1(config)#ip explicit-path name TUNNEL1 enable
R1(cfg-ip-expl-path)#next-address 192.168.13.3
R1(cfg-ip-expl-path)#next-address 192.168.23.2
R1(cfg-ip-expl-path)#next-address 2.2.2.2
```

```
R1(config)#ip explicit-path name TUNNEL2 enable
R1(cfg-ip-expl-path)#next-address 192.168.14.4
R1(cfg-ip-expl-path)#next-address 192.168.24.2
R1(cfg-ip-expl-path)#next-address 2.2.2.2
```

IPsec VPN

Step 1: Configure IKE policy

```
R1(config)#crypto isakmp policy 1
R1(config- isakmp)#encryption 3des
R1(config- isakmp)#hash md5
R1(config- isakmp)#group 2
R1(config- isakmp)#authentication pre-share
```

Step 2: Determine key information and the path of the packet

```
R1(config)#crypto isakmp key 123456 address 0.0.0.0 0.0.0.0
```

Step 3: Configure IPSEC policy

```
R1(config)#crypto ipsec transform-set LuanVan_TS esp-3des esp-md5-hmac
```

Step 4: Create a profile for ipsec

```
R1(config)#crypto ipsec profile LuanVan_PF
R1(config-profile)#set transform-set LuanVan_TS
```

Step 5: Create tunnel 3, show the address from the start and finish line and enable IPsec ipv4 then enable created profile protection mode then rout the packet destination

```
R1(config)#interface Tunnel3
R1(config-if)#ip unnumbered Loopback0
R1(config-if)#tunnel source 172.16.1.2
R1(config-if)#tunnel destination 172.16.2.2
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile LuanVan_PF
R1(config)#ip route 6.6.6.6 255.255.255.0 Tunnel3
```

Model of installing a company network and provide redundant IP via DHCP Server for LAN

Step 1: The first thing to do is to connect the devices together and planning of IP as shown

Step 2: Ensure that all addresses on the LAN can see each other, we use OSPF routing protocol

```
DHCP_Server(config)#router ospf 1
DHCP_Server(config-if)#network 192.168.2.0 0.0.0.255 area 0
DHCP_Server(config-if)#network 192.168.3.0 0.0.0.255 area 0
Active_Router(config)#router ospf 1
Active_Router (config-if)#network 192.168.2.0 0.0.0.255 area 0
Active_Router (config-if)#network 192.168.1.0 0.0.0.255 area 0
Standby_Router(config)#router ospf 1
Standby_Router (config-if)# network 192.168.3.0 0.0.0.255 area 0
Standby_Router (config-if)# network 192.168.1.0 0.0.0.255 area 0
```

Step 3: Active router and Standby Router likely become the Active router if it has higher priority (configured preempt)

- If you do not configure the "preempt" for the Routers when Active_Router dead, Standby_Router become Active then Active_Router resurrection cannot be Active again despite Active_Router has the higher priority than Standby_Router.

- By default, HSRP router is running on the "non-preempt" means not to seize

- Therefore we need to configure "preempt" if the road network and internet needs is the highest priority

- Standby Router is the default standby router priority = 100 < Active Router therefore it is okay not to be fixed.

```
Active_Router(config)#interface g0/0
Active_Router(config-if)#standby 1 ip 192.168.1.1
Active_Router(config-if)#standby 1 priority 120
Active_Router(config-if)#standby 1 preemt
Active_Router(config-if)#standby 1 track g0/1
Standby_Router(config)#interface g0/0
Standby_Router(config-if)#standby 1 ip 192.168.1.1
```

Step 4: Configuring DHCP Server and Relay Agent to issue dynamic IP for LAN

```
DHCP_Server(config)#ip dhcp excluded_address 192.168.1.1 192.168.1.10
DHCP_Server(dhcp-config)#network 192.168.1.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.1.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8
Active_Router(config)#service dhcp
Active_Router(config)#interface g0/0
Active_Router(config-if)#ip helper_address 192.168.1.2
Standby_Router(config)#service dhcp
Standby _Router(config)#interface g0/0
Standby _Router(config-if)#ip helper_address 192.168.1.3
```

Network model of a service provider offers user ADSL to rent through DSLAM

Configuring router Client_PPPoE

Step 1: Build interface dialer 1 used to create configuration templates

```
Client_PPPoE(config)#int dialer 1
Client_PPPoE(config-if)#encapsulation ppp
Client_PPPoE(config-if)#ip address negotiated
```

Step 2: Create a dialer pool 1 for authentication chap and enter Username and Password information from service providers

```
Client_PPPoE(config-if)#dialer pool 1
Client_PPPoE(config-if)#ppp authentication chap callin
Client_PPPoE(config-if)#ppp chap hostname PPPoE
Client_PPPoE(config-if)#ppp chap password cisco
Client_PPPoE(config-if)#int f0/0
Client_PPPoE(config-if)#no ip add
Client_PPPoE(config-if)#pppoe-client dial-pool-number 1
Client_PPPoE(config-if)#no shut
```

Step 3: perform NAT Overload mechanism so that users can access the Internet

```
Client_PPPoE(config)#int lo1
Client_PPPoE(config-if)#ip add 10.1.1.1 255.255.255.0
Client_PPPoE(config)#int dialer 1
Client_PPPoE(config-if)#ip nat outside
Client_PPPoE(config)#int lo1
Client_PPPoE(config-if)#ip nat inside
Client_PPPoE(config)# ip nat inside source list 1  int dialer 1 overload
Client_PPPoE(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Configure two Bridge routers of the customers and service provider

Configuring the VPI / VCI with value 0/35 on router Brigde_Customer and the same value for VPI / VCI 0/38 on Brigde_Provider to mapped to the uplink port on the DSLAM

```
Brigde_Customer(config)#bridge 1 protocol ieee
Brigde_Customer(config)#int atm1/0.35 point-to-point
Brigde_Customer(config-subif)#pvc 0/35
Brigde_Customer(config-subif)#exit
Brigde_Customer(config)#int atm1/0
Brigde_Customer(config-if)#no shut
Brigde_Customer(config)#int atm1/0.35 point-to-point
Brigde_Customer(config-subif)#bridge-group 1
Brigde_Customer(config)#int f0/0
Brigde_Customer(config-if)#bridge-group 1
Brigde_Customer(config-if)#no shut
```

```
Brigde_Provider(config)#bridge 1 protocol ieee
Brigde_Provider(config)#int atm1/0.38 point-to-point
Brigde_ Provider (config-subif)pvc 0/38
Brigde_ Provider (config-if)#exit
Brigde_ Provider (config)#int atm1/0
Brigde_ Provider (config-if)#no shut
Brigde_ Provider (config)#int atm1/0.38 point-to-point
Brigde_ Provider (config-subif)#bridge-group 1
Brigde_ Provider (config)#int f0/0
Brigde_ Provider (config-if)#bridge-group 1
Brigde_ Provider (config-if)#no shut
```

Configure router PPPoE_Server of ISP service provider

Step 1: Assign IP address for virtual-template then configure username, password and protocol for user authentication from the service provider

```
PPPoE_Server(config)#int virtual-template 1
PPPoE_Server(config-if)#ip add 192.168.1.1 255.255.255.0
PPPoE_Server(config-if)#exit
PPPoE_Server(config)#username PPPoE password cisco
PPPoE_Server(config)#aaa new-model
PPPoE_Server(config)#aaa authentication ppp default local
PPPoE_Server(config)#int virtual-template 1
PPPoE_Server(config-if)#aaa authentication chap default
PPPoE_Server(config-if)#exit
```

Step 2: create bba-group pppoe then let it connect to router Brigde_Provider to enable them and join in pppoe

```
PPPoE_Server(config)#bba-group pppoe CLIENT_ADSL
PPPoE_Server(config-bba-group)#virtual-template 1
PPPoE_Server(config-bba-group)#exit
PPPoE_Server(config)#int f0/0
PPPoE_Server(config-if)#no shut
PPPoE_Server(config-if)#pppoe enable group CLIENT_ADSL
PPPoE_Server(config-if)#exit
```

Step 3: Create a pool to provide IP for customer when they require to hire ADSL Internet connection

```
PPPoE_Server(config)#ip local pool POOL_ADSL 192.168.1.10 192.168.1.254
PPPoE_Server(config)#int virtual-template 1
PPPoE_Server(config-if)#peer default ip address pool POOL_ADSL
```