A

Project Report

On

MPLS Cloud using multi-protocol routing and VRF packet Switching for Banking Network.

Submitted by:

Dhairya N. Bhatt

Prof. Abhinav Dave

Faculty Guide

Academic Year

2020-2021

Table of Contents: Page No.

List of Figures:

INTRODUCTION:

1.1 Problem summary:

In the generation of High-speed internet and telecom networks everyone wants zero lag network connectivity service which provide them data and security all over the range. As the demand increases day by day it is difficult to store the information of routing data of network around the and this could also be a reason for depletion in the speed of data flowing around the network. Many Organization wants their data to be travel safely over the encrypted tunnels due to which they didn’t got capture by hackers and other illegal firms. Also, the Devices which are in the network infrastructure get destructed because of the high amount of load balancing and information tables in the network.

1.2 Project summary:

Our project is based on Multiprotocol Label Switching which provides high-performance data flows within the internet. It is a Major type of platform which is used for data-carrying technique for high-performance telecommunications networks. MPLS concept combines and well execute two major aspects of the Asynchronous Transfer Mode (ATM) technology. MPLS Protocol initially generate an IP address for every packet present in the network. There are four types of router consisted by MPLS which are provider edge router, customer edge router, provider core router, autonomous system boundary router. The core router or we can it as a master router is the head of MPLS network because all process which combined and redistribute all the routing protocol are configured on this router. The Routing Protocols managed by Cisco such as EIGRP, RIP, OSPF, MBGP, here the MBGP plays the most important role to deal with the entire scenario of network. When the IP’s are allotted, they were carry forward to the Label distribution Protocol this LDP service is running in the provider edge router (PER) which is present outside the core which label the packet with LDP instead of assigning IP. The MPLS service consist of 3 main operations which are carried out for the network are push, swap, pop. We can say that at PER the

IP have been swap by Label and when they reach to the CER the label had to be pop and IP are applied back.

The MPLS traffic has been carried over the MPLS VPN. There are so many configuration that had to be done to store the routing table of all the customer in the service, for which VRF is configured. The main work of Virtual Routing forwarding (VRF) is to separate the routing tables of the customer if they are in same network or in the different network. The main Advantage of using MPLS that it forwards unicast routing if there packet of RIP then it will be forwarded to the network which is running on RIP protocol. The MPLS doesn't store the routing table of the router instead of these it will forward it to another. There are so many other protocols which are working in the MPLS to provide fast and secure data flow over the network.

1.3 Purpose:

The main Aim of developing such a routing technique that directs data transfer from one node to another via the shortest path present in the network without overhead of carrying long IP addresses, And thus also avoiding complex lookups in the routing tables and speeding traffic of the network.

1.4 Objective:

The main object is to create a secure network for the Banks which helps to securely travel their whole data over the encrypted tunnel using MPLS VPN and also the devices which are also present in the network does not get affected by the overhead storing of routing tables in the memory which enhance there speed traffic control for the network and also provide with a redundancy path at the failure.

1.5 Literature Review:

Sr No.	Paper title	Conclusion
1	***Review on Mobile MPLS Techniques***	Mobile MPLS (Multi-Protocol Label Switching) is a new technique which integrates the Mobile IP (MIP) and MPLS and thus inherits the advantages of both. MIP supports the mobility whereas MPLS provides faster streaming throughout the network, hence providing requisite QoS to the application. The objective of this paper is to survey the efforts that have been done to enhance the MIP functionality by integrating with MPLS and also to guarantee QoS provided to the users by the network. It first briefs the MIP and MPLS, along with their shortcomings. From there it examines the different initiatives to improve the performance of network in terms of hand-off, delay, QoS, Optimal path selection and lots more.
2	***Systems and Methods for policy-enabled communication networks***	Embodiments of the present invention relate to systems and methods for policy-based management of a multiprotocol label switching (“MPLS”) network. In an embodiment, a system includes a policy-based network administration system, and the policy-based network administration system includes a plurality of policies. The system also includes an MPLS network, which is coupled to the policy-based network administration system.

1.6 Materials/Tools Required:

1. Hardware:

Routers (7200)

Layer 2 Switches (2960)

Layer 3 Switches (3560)

Ethernet Cables (cross cables, straight cables)

2. Software:

Cisco Packet Tracer

GNS 3 (Graphical Network Simulator)

Wireshark (Network protocol Analyzer)

1.6.1 Router:

(Figure-1 Router)

A router is a physical or virtual appliance that passes information between two or more packet-switched computer networks. A router inspects a given data packet’s destination Internet-protocol address (IP address). Calculate the best way for it reach its destination and then forwards it accordingly.

A router is a common type of Gateway. It is positioned where two or more networks meet at each point of presence on the internet. Hundreds of routers might forward a single packet as it moves from one network to the next on the way to its destination. In the Open System Interconnection (OSI) model, routers are associated with the network layer (Layer 3).

Traditional routers are stand-alone devices that use proprietary software. In contrast, a virtual router is a software instance that performs the same functions as physical router. Virtual router typically run on commodity servers, either alone or packaged with other virtual network functions, like firewall packet filter, load balancing and wide area network (WAN) optimization capabilities.

How a router works:

A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address.

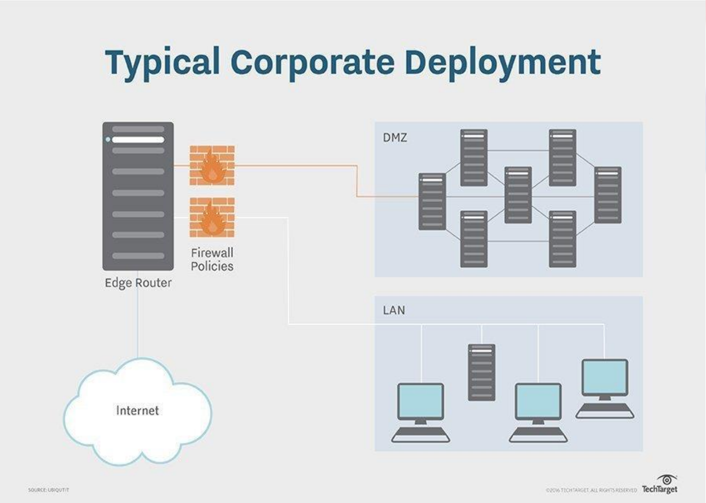
A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP).

Routing tables can be static- i.e., manually configured or dynamic. Dynamic router automatically updates their routing tables based on the network activity, exchanging information with other devices via routing protocol.

Many routers also perform network address translation (NAT), shielding the private IP addresses of a local area network (LAN) by readdressing all outgoing traffic with a single shared public IP address. NAT helps both conserves globally valid IP addresses and improve network security.

Types of Router:

1) Core Router used by Internet Service Providers (ISP's) are the fastest and most powerful, sitting at the center of the internet and forwarding information along the main fiber optic backbone. Enterprise routers connect large organizations networks to these core routers.
2) An edge router, also known as an ***access router***, is a lower-capacity device that resides at the boundary of a LAN and connects it to a the public internet or a private wide area network (WAN) and/or external local area network (LAN). Home and small office routers are considered subscriber edge routers.
3) Branch routers link an organization's remote office locations to its WAN, connecting to the primary campus network's edge routers. Branch routers often provide additional features, like time-division multiplexing, wireless LAN management capabilities and WAN application acceleration.
4) A logical router is a configured partition of a traditional network hardware, or physical, router. It replicates the hardware's functionality, creating multiple routing domains within a single router. Logical routers perform a subset of the tasks that can be handled by the physical router, and each can contain multiple routing instances and routing tables.



5) A wireless router works in the same way as the router in a hard-wired home or business local area network (LAN), but allows greater mobility for notebook or portable computers. Wireless routers use the 802.11g specification, a standard that offers transmission over short distances.

Routing Protocols:

Routing protocols determine how a router identifies other routers on the network, keeps track of all possible destinations and makes dynamic decisions for where to send each network message.

1) **Open Shortest Path First** (OSPF) - used to find the best path for packets as they pass through a set of connected networks. OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs).
2) **Interior Gateway Routing Protocol** (IGRP)- determines how routing information between gateways will be exchanged within an autonomous network. The routing information can then be used by other network protocols to specify how transmissions should be routed.
3) **Enhanced Interior Gateway Routing Protocol** (EIGRP) - evolved from IGRP. If a router can't find a route to a destination in one of these tables, it queries its neighbors for a route and they in turn query their neighbors until a route is found. When a routing table entry changes in one of the routers, it notifies its neighbors of the change instead of sending the entire table.
4) **Exterior Gateway Protocol** (EGP) - determines how routing information between two neighbor gateway hosts, each with its own router, is exchanged. EGP is commonly used between hosts on the Internet to exchange routing table information.
5) **Routing Information Protocol** (RIP) - the original protocol for defining how routers should share information when moving traffic among an interconnected group of local area networks. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

1.6.2 Layer 2 Switch:

(Figure-2 Switch)

Layer 2 Switch is responsible for a lot of operations at the data link layer of the OSI model. Some of their works involve MAC Address Forwarding, Ingress Queue, Access Control List (ACL), MAC Table, CAM Table etc. Let's take a deeper look into these functionalities.

Layer 2 Switch, also called as Ethernet switch, operates at the Data Link Layer of the OSI model. One of the most important functions of these switches is that they make decisions about forwarding frames based on the destination MAC addresses found within the frame.

1) Store-and-Forward mode:

In a network, when a switch receives a frame, the frame is first checked for the errors using cyclic redundancy check (CRC) and forwarded. This type of operation by a Layer 2 Switch is called store-n-forward mode. The store-n-forward mode results in latency in frame transmission because an entire frame has to be stored before being transmitted to the another port.

2) Cut-through-Switching:

In the case of cut-through switching, some models of a switch bypass the CRC check which results in lowering the latency of the frame transmission because the entire frame is not stored before transmission to another port.

3) MAC-Address-Forwarding:

The switch has to be intelligent enough to figure out where a frame must be sent. For that purpose, a switch maintains the MAC address table. Well, the MAC address table is either learnt by the switch over a period of time or the network admin just punches in the address table information in the switch memory.

So, when a frame arrives at one of the ports of the switch, the switch checks the source MAC addresses of the frame. If the MAC address is already not there in the table, the MAC address, switch port, and VLAN (Virtual Lan) will then get recorded in the forwarding table. The forwarding table is also called the ***CAM (Content Addressable Memory) table.***

4) Unicast-Flooding:

But have you ever wondered what happens to a frame if the destination MAC address of that frame is not known to the switch? In that case, a switch decided to go for unicast flooding. Unicast flooding is a method to forward the frame through all ports within a VLAN except the port the frame was received on.

5) MAC-Table:

MAC and CAM table are almost the same tables. The term CAM simply refers to the way the switch uses memory (in a content-addressable) manner to look up the MAC address to the port association.

The Layer 2 forwarding table is also called the MAC table. The MAC table typically contains information about MAC addresses and destination ports. So, when a packet is received, a switch takes a reference for the destination MAC address of the incoming frame in the MAC table and forward the frames to the destination ports specified in the table.

6) Access Control List (ACL):

If you think ACL only applies to routers, then that is not the case. Switches can also have ACLs based on MAC and IP addresses. The difference between layer 2 and layer 3 switches is that layer 3 switch can support ACLs based on both MAC and IP addresses whereas Layer 2 switches support ACLs based only on MAC addresses.

Layer 2 Switching:

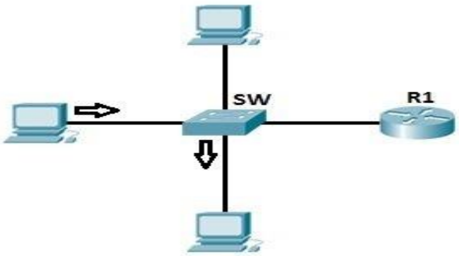
Layer 2 switching *(or* ***Data Link layer switching****)* is the process of using devices' MAC addresses to decide where to forward frames. Switches and bridges are used for Layer 2 switching. They break up one large collision domain into multiple smaller ones.

In a typical LAN, all hosts are connected to one central device. In the past, the device was usually a hub. But hubs had many disadvantages, such as not being aware of traffic that passes through them, creating one large collision domain, etc. To overcome some of the problems with hubs, bridges were created. They were better than hubs because they created multiple collision domains, but they had limited number of ports. Finally, switches were created and are still widely used today. Switches have more ports than bridges, can inspect incoming traffic and make forwarding decisions accordingly. Also. each port on a switch is a separate collision domain, so no packet collisions should occur.

Layer 2 switches are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses to decide what to do with the frame – to forward, flood, or drop it. Here are other major advantages of Layer 2 switching:

- fast hardware-based bridging
- wire speed
- low latency
- low cost

Here is an example of the typical LAN network – the switch serves as a central device that connects all devices together:



Switches increase the number of collision domains. Each port is one collision domain, which means that the chances for collisions to occur are minimal. A switch learns which device is connected to which port and forwards a frame based on the destination MAC address included in the frame. This reduces traffic on the LAN and enhances security.

Features of L2 Switch:

- Layer-2 Switch act as a network bridge that links up various end devices of a computer networking system on one single platform. They are able to transport data very rapidly and competently from the source to the destination end in LAN networks.
- Layer-2 switches perform the switching function to re-arrange the data frames from the source to a destination end by learning the MAC address of the destination node from the address table of the Switch.
- The MAC address table provisions the unique address of each device of layer-2, on the basis of which it can identify the end devices and the node on which the data is to be delivered.
- Layer-2 Switch splits a bulky complicated LAN network into small VLAN networks.
- By configuring multiple VLAN's within a vast LAN network, the switching becomes faster as it is not being physically connected.

Application of L2 Switch:

- Through Layer-2 switches, we can send data frame from the source to the destination that is situated in the same VLAN easily without being physically connected or being at the same location.
- Thus, the servers of a software company can be put centrally at one location and the clients dispersed at the other locations can access the data easily without latency and thereby save the server cost and time.
- Organizations can make internal communications by configuring the hosts on the same VLAN by using these types of switches without the need of any internet connection.
- Software testers also use these switches for sharing their tool by keeping it centrally at one server location and the other server can access them by being far apart and not physically connected by configuring all on the same VLAN of the networking system.

1.6.3 Layer 3 Switch:

(Figure-3 L3 Switch)

- The layer-2 switch fails when we need to transfer the data between different LAN or VLAN’s.

- This is where the Layer-3 switches come in the picture as the technique they use for routing the data packets to the destination is using IP addresses and subnetting.

- The layer-3 switches work at the 3rd Layer of the OSI reference model and perform the routing of data packets using IP addresses. They have faster-switching speed than the layer-2 switches.

- They are even faster than the conventional routers as they perform the routing of data packets without using additional hops, thereby leading to better performance. Due to the functionality of this routing technique in the Layer-3 switches, they are implemented for network building of inter and intra networks.

- In order to understand the functions of Layer-3 switches, we need to understand the concept of routing first.

- The layer-3 device at the source end firstly looks at its routing table which has all the information regarding the source and destination IP addresses and subnet mask.

- Later, based on the information that it gathers from the routing table it delivers the data packet to the destination and can pass along the data further between different LAN, MAN, and WAN networks. It follows the shortest and secure path to deliver data between the end devices. This is the overall concept of routing.

- Various networks can be linked together by STM links which have very high bandwidths and DS3 links as well. The type of connectivity depends upon the various parameters of the network.

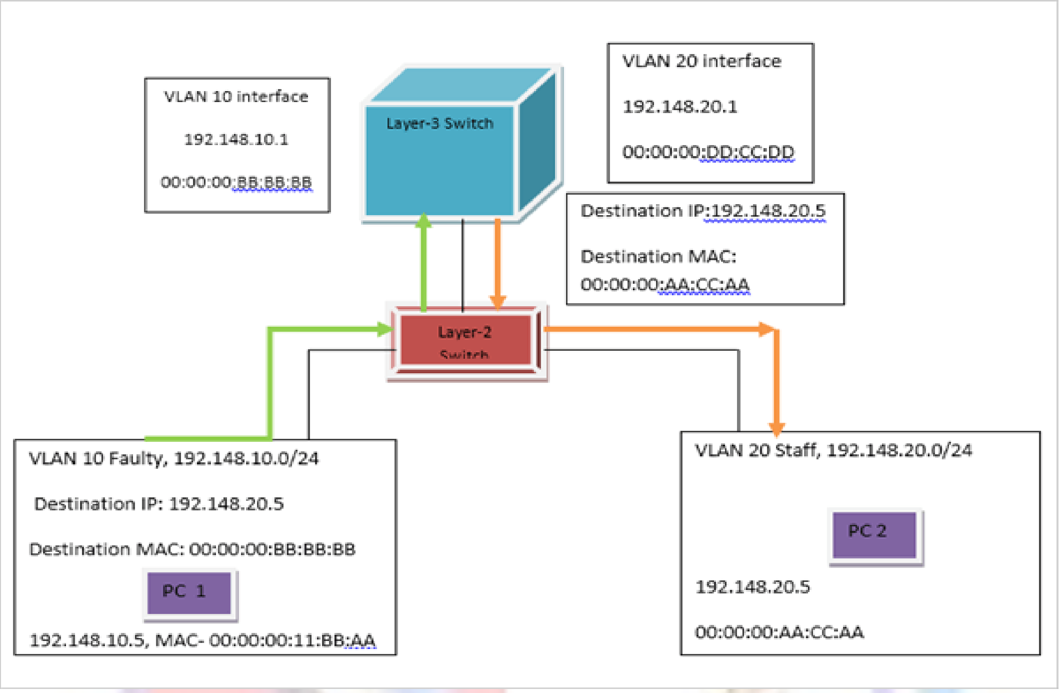
Features of L3 Switch:

- It performs the static routing to transfer data between different VLAN's. Whereas the layer-2 device can transfer data between the networks of the same VLAN only.
- It also performs dynamic routing in the same way in which a router performs. This dynamic routing technique allows the switch to execute optimal packet routing.
- It provides a set of multiple paths according to the real-time scenario of the network to deliver the data packets. Here, the switch can select the most feasible path for routing the data packet. The most popular routing techniques include RIP and OSPF.
- The switches have the capability to recognize the IP address related information that is heading towards the switch about the traffic.
- Switches have the capability to deploy QoS classifications depending upon subnetting or VLAN traffic tagging instead of configuring the switch port manually as in the case of layer-2 switches.
- They require more power to operate and tender higher bandwidths links between the switches which are almost more than 10Gbits.
- They provide highly secure paths for data exchange. Thereby, they are implemented in such instances where data security is a prime concern.
- The features associated with switches like 802.1x authentication, loopback detection, and ARP inspection make it efficient to use at instances where secure data transmission is essential.

Application of L3 Switch:

- It is widely used in data centers and vast campus like universities where there is a very big setup of computer networking. Owing to its features like static and dynamic routing and its fast switching speed than a router, it is used in LAN connectivity for interconnection of several VLAN and LAN networks.
- The layer-3 switch in combination with a number of layer-2 switches supports more users to connect on the network without the need for implementation of an extra layer-3 switch and more bandwidth. Thus, it is widely implemented in universities and small-scale industries. In case if the number of end users on a network platform increases, then without any enhancement of the network, it can be accommodated in the same running scenario easily.
- Thus, the layer-3 switch can easily deal with high bandwidth resources and end-user application as it is offering 10Gbits bandwidth.
- They have the skills to unburden the overloaded routers. This can be done by configuring a layer-3 switch, each with a main router in a wide area networking scenario so that the switch can manage all the local level VLAN routing.
- By following the above type of scenario, the router working efficiency will improve and it can be used dedicatedly for long distance (WAN) connectivity and data transmission.
- A layer-3 switch is smart enough to handle and manage the routing and traffic controlling of locally connected servers and end devices utilizing its high bandwidth. Thus the firms generally use a L-3 switch to connect their monitoring servers and host nodes in any NOC centers of a sub-system which are part of a big computer networking system.

Inter-vlan Routing at L3 Switch:

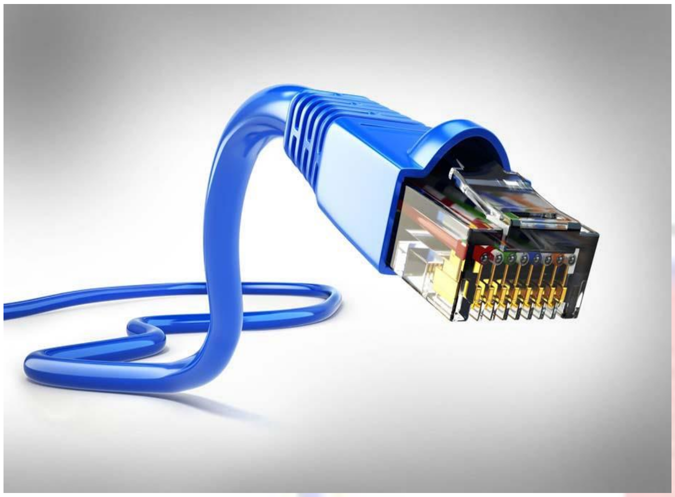


PC 1 of a faculty VLAN in a university wants to communicate with the PC 2 of some other VLAN of a staff member. As both end devices are of different VLAN, we need L-3 switch for routing the data from host 1 to host 2.

Firstly, with the help of the hardware part of the MAC address table, the L-2 switch will locate the destination host. Then, it will learn the destination address of the receipt host from the MAC table. After that, the layer-3 switch will perform the switching and routing part on the basis of IP address and subnet mask.

It will find out that PC1 wants to communicate with the destination PC of which of the VLAN networks present there. Once it gathers all the necessary information, it will establish the link between them and route the data to the receiver from the sender's end.

1.6.4 Ethernet Cables:



(Figure-4 Ethernet Cables)

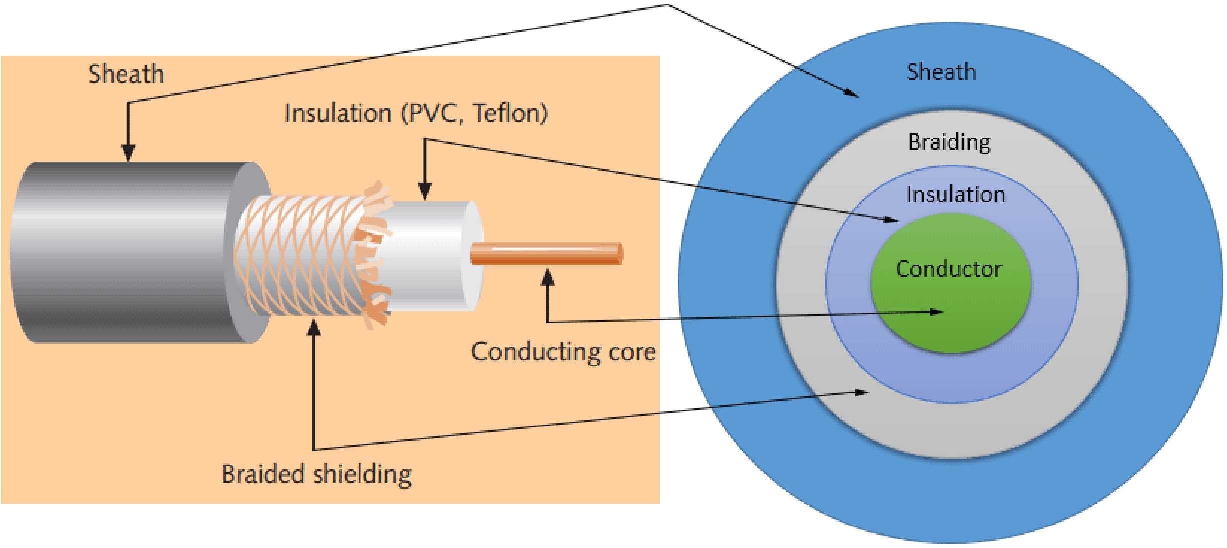
An Ethernet cable resembles a phone cable, but is larger and has more wires. Both cables share a similar shape and plug, but an Ethernet cable has eight wires, while phone cables have four. Ethernet cable connectors are also larger. Ethernet cables come in different colors, but phone cables are usually grey.

Ethernet cables plug into Ethernet ports, which are larger than phone cable ports. An Ethernet port on a computer is accessible through the Ethernet card on the motherboard. This port is usually on the back of a desktop computer, or on the side of a laptop.

Ethernet cables are manufactured in two basic forms:

- Solid Ethernet cables offer slightly better performance and improved protection against electrical interference. They're also commonly used on business networks, wiring inside office walls, or under lab floors to fixed locations.
- Stranded Ethernet cables are less prone to physical cracks and breaks, making them more suitable for travelers or in-home network setups.

Coaxial Cable:



Invented in the 1880s, coaxial cable (also called coax) was best known as the kind of cable that connected television sets to home antennas. Coaxial cable is also a standard for 10 Mbps Ethernet cables.

When 10 Mbps Ethernet was most popular, during the 1980s and early 1990s, networks typically used one of two kinds of coax cable — thinnest (10BASE2 standard) or thick net (10BASE5). These cables consist of an inner copper wire of varying thickness surrounded by insulation and another shielding. Their stiffness caused network administrators difficulty when installing and maintaining thinnest and thick net.

Sheath

This is the outer layer of the coaxial cable. It protects the cable from physical damage.

Braided shield

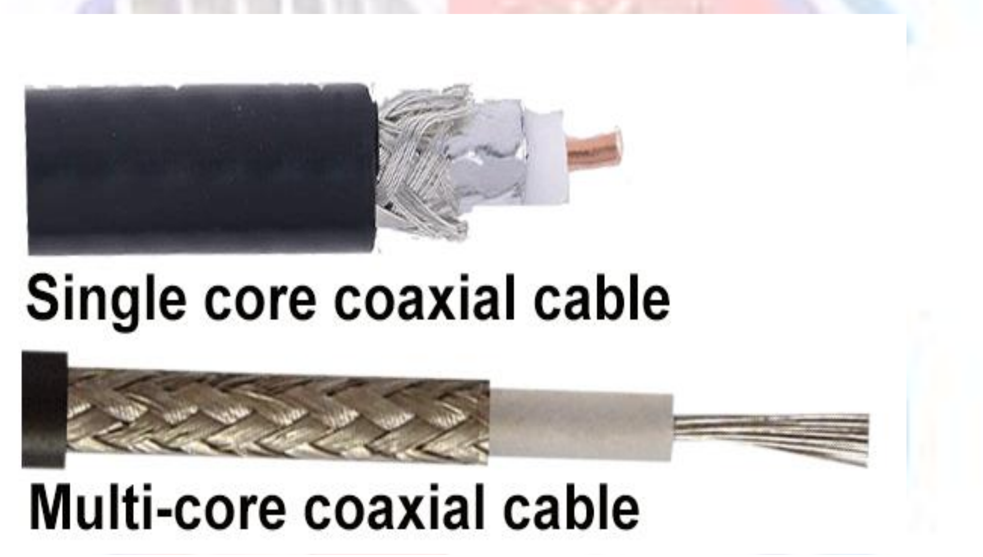
This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

Insulation

Insulation protects the core. It also keeps the core separate from the braided-shield. Since both the core and the braided-shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.

Conductor

The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.

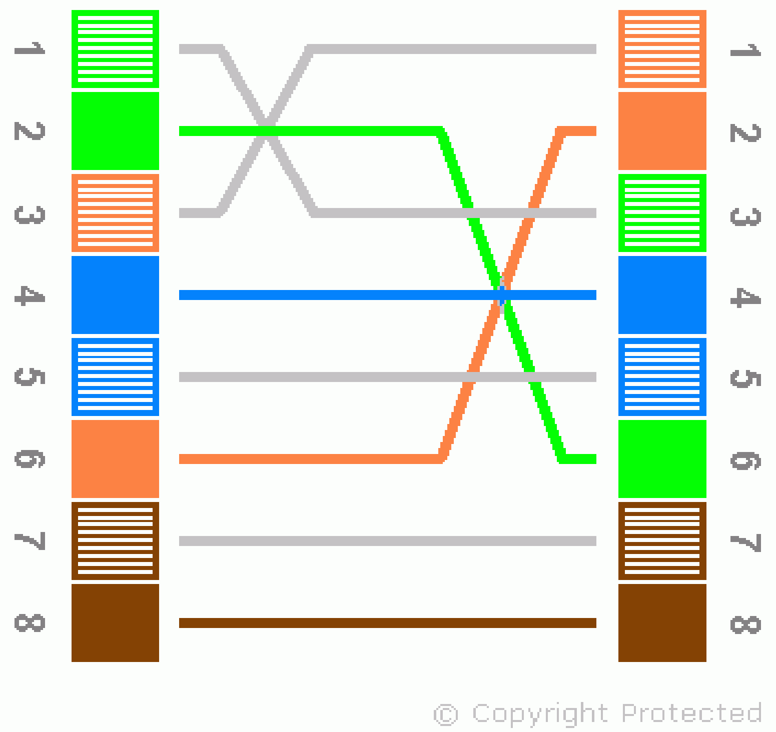


The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.

At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.

Because of low-cost and long durability, coaxial cables were used in computer networking for nearly two decades (80s and 90s). Coaxial cables are no longer used to build any type of computer network.

Configuration:

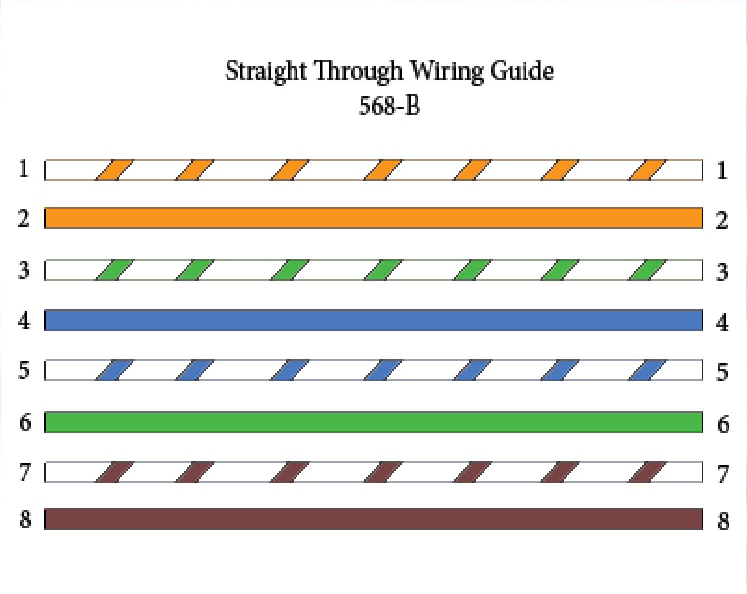


Uses:

- Hub to hub
- Router to router / between two routers
- Switch to switch / between switches
- For computer to computer
- PC to PC

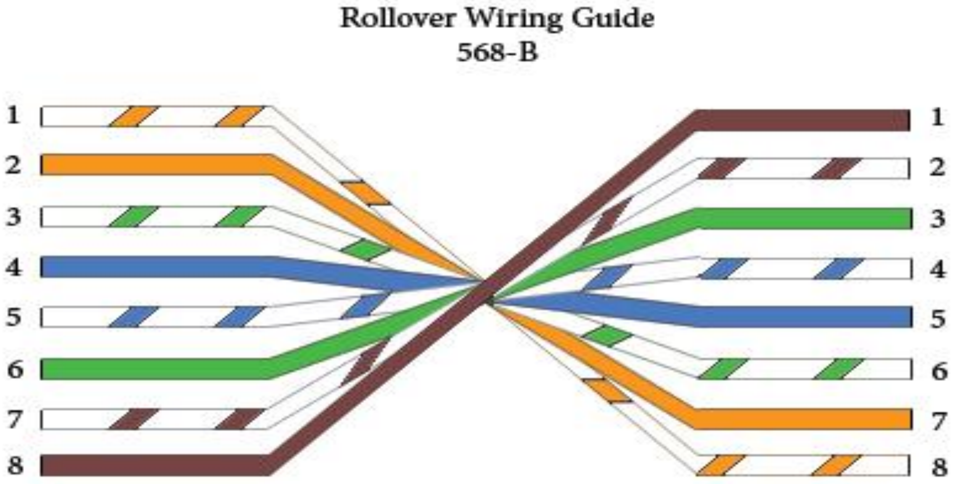
Straight Through Cables:

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words, Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2, etc. Straight-Through wired cables are most commonly used to connect a host to a client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers, and other network client devices to the router switch or hub (the host device in this instance)



Roll Over Cable:

Rollover wired cables, most commonly called rollover cables, have opposite Pin assignments on each end of the cable or, in other words, it is "rolled over." Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Yost cables are most commonly used to connect to a device's console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.



1.6.5 Cisco Packet Tracer and GNS3

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

GNS3 is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. Dynagen runs on top of Dynamips to create a more user friendly, text-based environment. A user may create network topologies using simple Windows ini-type files with Dynagen running on top of Dynamips.

1.6.6 Wireshark:

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

- Wireshark is very similar to tcp dump, but has a graphical front-end, plus some integrated sorting and filtering options.
- Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering[*citation needed*].
- On GNU/Linux, BSD, and macOS, with libpcap 1.0.0 or later, Wireshark 1.4 and later can also put wireless network interface controllers into monitor mode.
- If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the TZSP protocol or the protocol used by OmniPeek, Wireshark dissects those packets, so it can analyze packets captured on a remote machine at the time that they are captured.

Features:

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

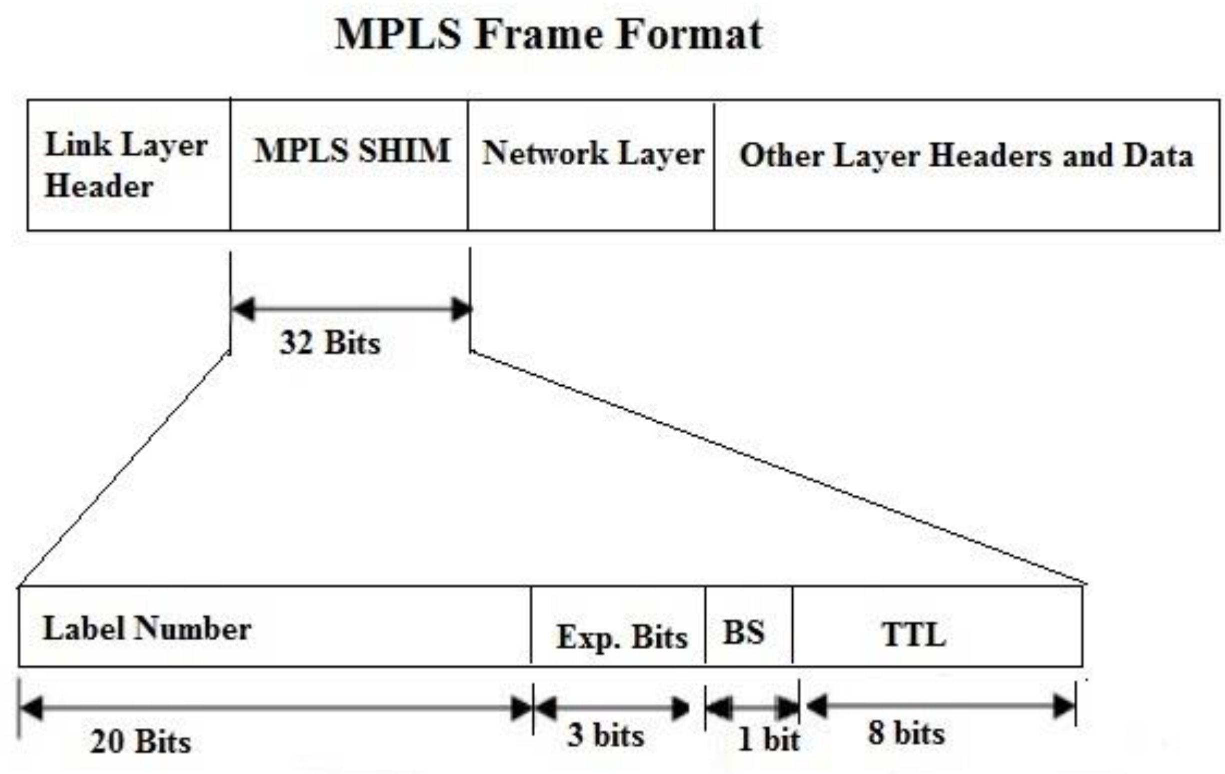
- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

Wireshark's native network trace file format is the libpcap format supported by libpcap and Win cap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

Project Description

3.1 Description

The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching.

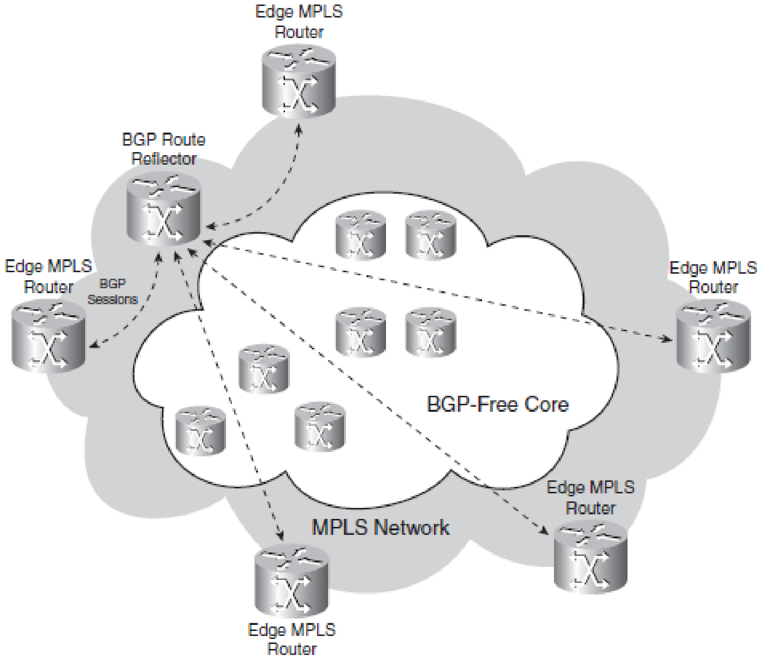


Benefits of MPLS

This section explains briefly the benefits of running MPLS in your network. These benefits include the following:

- The use of one unified network infrastructure
- Better IP over ATM integration
- Border Gateway Protocol (BGP)-free core
- The peer-to-peer model for MPLS VPN
- Optimal traffic flow
- Traffic engineering

Consider first a bogus reason to run MPLS. This is a reason that might look reasonable initially, but it is not a good reason to deploy MPLS.

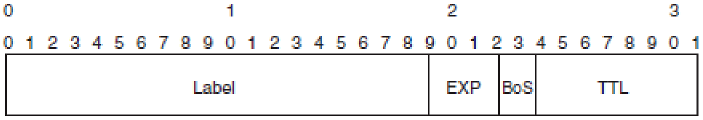


Traffic Engineering

The basic idea behind traffic engineering is to optimally use the network infrastructure, including links that are underutilized, because they do not lie on the preferred path. This means that traffic engineering must provide the possibility to steer traffic through the network on paths different from the preferred path, which the least-cost path is provided by IP routing. The least-cost path is the shortest path as computed by the dynamic routing protocol. With traffic engineering implemented in the MPLS network, you could have the traffic that is destined for a particular prefix or with a particular quality of service flow from point A to point B along a path that is different from the least-cost path. The result is that the traffic can be spread more evenly over the available links in the network and make more use of underutilized links in the network. Figure 1-9 shows an example of this.

Labels

One MPLS label is a field of 32 bits with a certain structure. Figure 2-1 shows the syntax of one MPLS label.



The first 20 bits are the label value. This value can be between 0 and 2^{20}–1, or 1,048,575. However, the first 16 values are exempted from normal use; that is, they have a special meaning. The bits 20 to 22 are the three experimental (EXP) bits. These bits are used solely for quality of service (QoS).

Abstract

Today hundreds of millions of users are interconnected by communication channels allowing them to communicate and to share information Now with the ever-increasing expansion of companies and industries, every company has its branches and sites spread all over the globe.

The company needs to have connectivity between its various sites along with features like privacy and security. The use of MPLS VPN network and Multi-VRF enables the service provider to handle multiple sites on one CE router itself.

The Internet is a network of networks with a myriad of computer devices, including smartphones, game consoles (handheld/stationary), IP televisions, tablet computers, laptop computers, desktop computers, palmtop computers, etc. With ever increasing number of network devices, the exhaustion of IPv4 address space has become inevitable.

Thus, migration from IPv4 to IPv6 (which offers a much larger address space) is necessary. Migration technique to IPv6 network is proposed in this project that overcomes all the limitations available in existing IPv4 network.

FEATURES:

- **Faster Speed:** Due to the labelling technology, the speed of performing lookups for destinations and routing is much faster than the standard IP table lookups non-MPLS routers have to perform.
- **QoS:** This is a big one. MPLS networks achieve greater Quality of Service for their customers. Quality of Service (QoS) means exactly that –you can expect a higher standard of service such as reliability, speed, and voice quality. This is for a few reasons, one already mentioned above.
- **Faster Restoration:** MPLS networks are also able to restore interrupted connections at a faster speed than typical networks. Obviously, this is a benefit.
- **Security:** MPLS offers greater security and are often required for companies which need enhanced privacy and security for their network needs. Some industries like the Health Care and Financial
- industries are examples of industries mandated by Federal law to comply to specific requirements for network security

IPsec Tunnel:

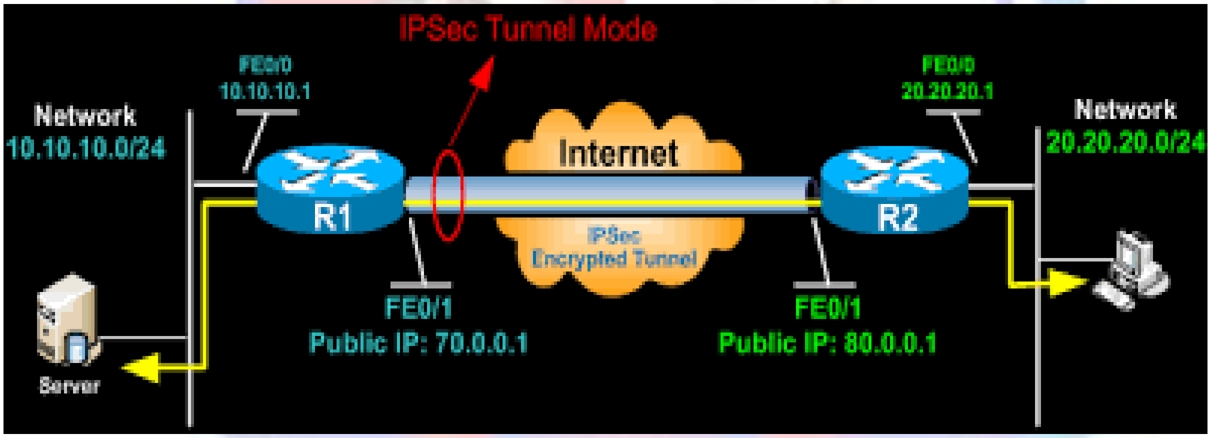
An Internet Protocol Security (IPsec) tunnel is a set of standards and protocols originally developed by the Internet Engineering Task Force (IETF) to support secure communication as packets of information are transported from an IP address across network boundaries and vice versa.
An IPSec tunnel allows for the implementation of a virtual private network (VPN) which an enterprise may use to securely extend its reach beyond its own network to customers, partners and suppliers.

IPSec VPNs may be classified as:

Intranet VPNs: Connect company headquarters with offices in different locations.

Extranet VPNs: Connect enterprises with business partners or suppliers.

Remote-Access VPNs: Connect individual, remote users such as traveling executives or telecommuters with their company network.



Protocol:

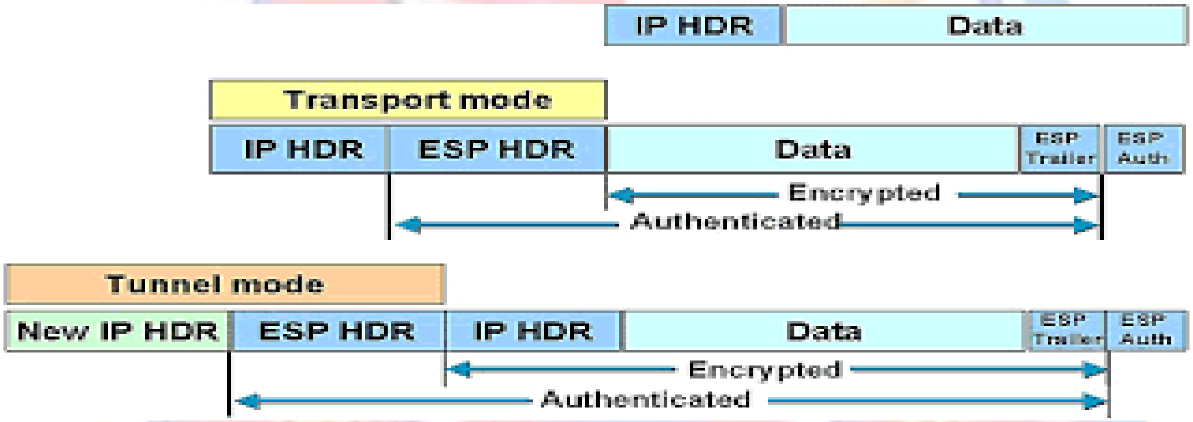
(1) Internet Security Association and Key Management Protocol (ISAKMP)
A framework for the negotiation and management of security associations between peers (traverses UDP/500)

(2) Internet Key Exchange (IKE)
Responsible for key agreement using asymmetric cryptography

(3) Encapsulating Security Payload (ESP)
Provides data encryption, data integrity, and peer authentication; IP protocol 50

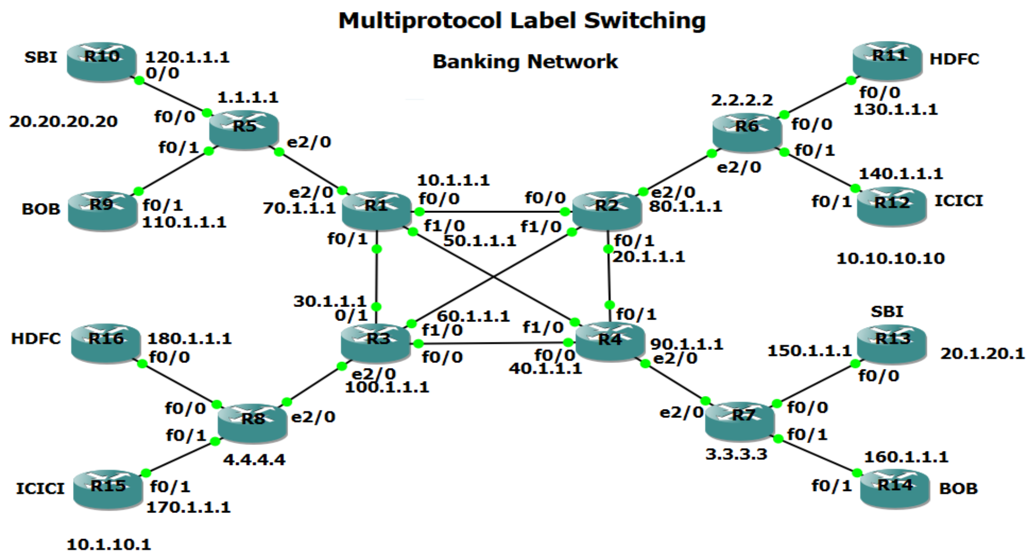
(4) Authentication Header (AH)
Provides data integrity and peer authentication, but not data encryption; IP protocol 51

IPsec Modes:

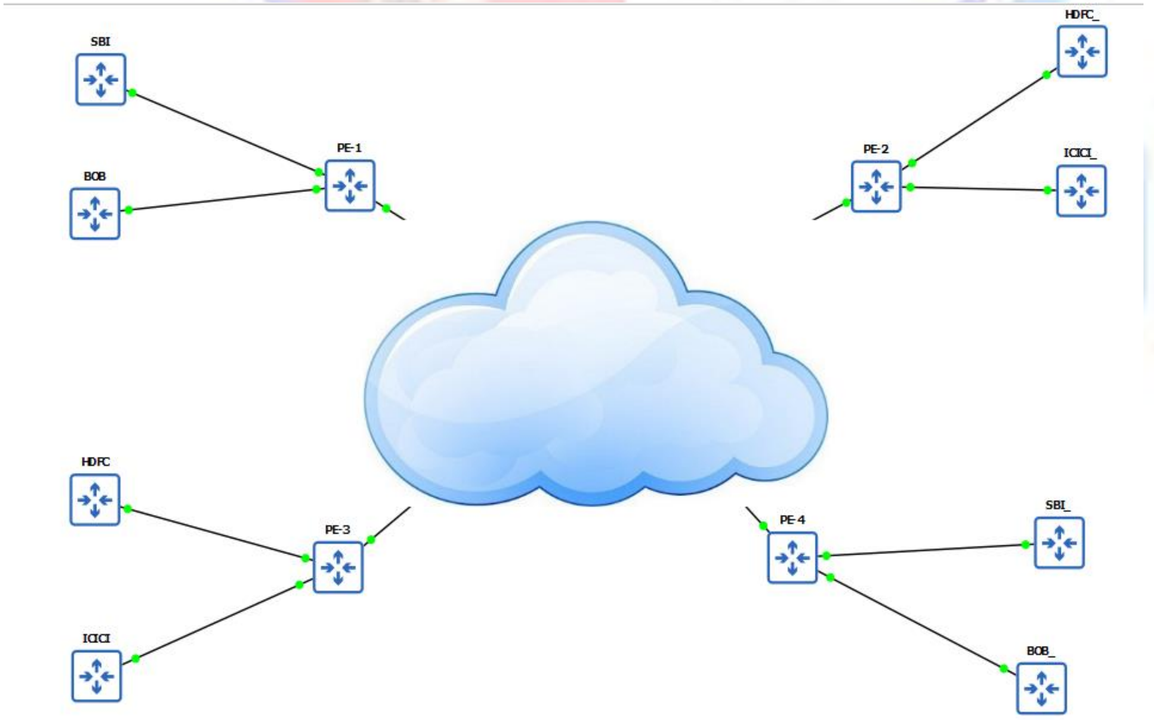


3.1.1 Topology

1. **Actual Topology:**



2. **Representation Topology:** Router 1 to 4 can be represented as cloud which means core routers for storage purpose. Router 5 to 8 are provider edge routers and routers 9 to 16 are customer edge routers with name of bank written on them.



3.1.2 Configurations

1. Core Routers (1 to 4)

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
 ip address 30.1.1.2 255.255.255.0
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet1/0
 ip address 50.1.1.1 255.255.255.0
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface Ethernet2/0
 ip address 70.1.1.1 255.255.255.0
 half-duplex
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 30.1.1.0 0.0.0.255 area 0
 network 50.1.1.0 0.0.0.255 area 0
 network 70.1.1.0 0.0.0.255 area 0
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
End
```

Note: IP address, VRFs and IPSEC-VPN will vary according to routers.

2. PE (provider edge) Routers (5 to 8)

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
ip vrf BOB
 rd 100:2
 route-target export 100:2
 route-target import 100:2
!
ip vrf HDFC
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
ip vrf ICICI
 rd 100:4
 route-target export 100:4
 route-target import 100:4
!
ip vrf SBI
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
```

```
mpls label protocol ldp
!
ip tcp synwait-time 5
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key BANK address 90.1.1.2
!
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
!
crypto map ipsec-map 10 ipsec-isakmp
 set peer 90.1.1.2
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group5
 match address 100
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding SBI
 ip address 120.1.1.2 255.255.255.0
 ip ospf 2 area 0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip vrf forwarding BOB
 ip address 110.1.1.2 255.255.255.0
 ip ospf 3 area 0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 70.1.1.2 255.255.255.0
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
 crypto map ipsec-map
!
interface Vlan1
 no ip address
!
router ospf 2 vrf SBI
 router-id 1.1.1.2
 log-adjacency-changes
 redistribute bgp 100 subnets
!
router ospf 3 vrf BOB
 router-id 1.1.1.3
 log-adjacency-changes
 redistribute bgp 100 subnets
!
router ospf 1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 70.1.1.0 0.0.0.255 area 0
 network 110.1.1.0 0.0.0.255 area 0
 network 120.1.1.0 0.0.0.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf SBI
  redistribute ospf 2 vrf SBI match internal external 1 external 2
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf ICICI
  redistribute ospf 5 vrf ICICI match internal external 1 external 2
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf HDFC
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf BOB
  redistribute ospf 3 vrf BOB match internal external 1 external 2
  no synchronization
 exit-address-family
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 100 permit ip 70.1.1.0 0.0.0.255 90.1.1.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Note: IP address, VRFs and IPSEC-VPN will vary according to routers.

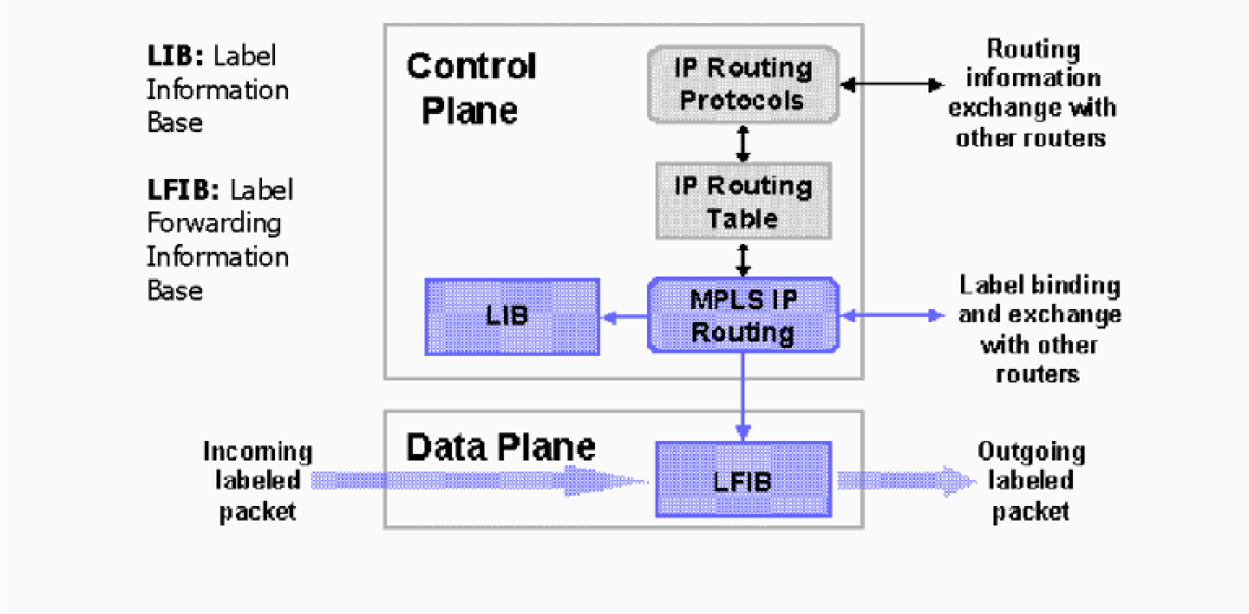
3. CE (Customer Edge) Routers (9 to 16)

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R10
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key bank address 150.1.1.1
!
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
!
crypto map ipsec-map 10 ipsec-isakmp
 set peer 150.1.1.1
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group5
 match address 100
!
interface FastEthernet0/0
 ip address 120.1.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map ipsec-map
!
```

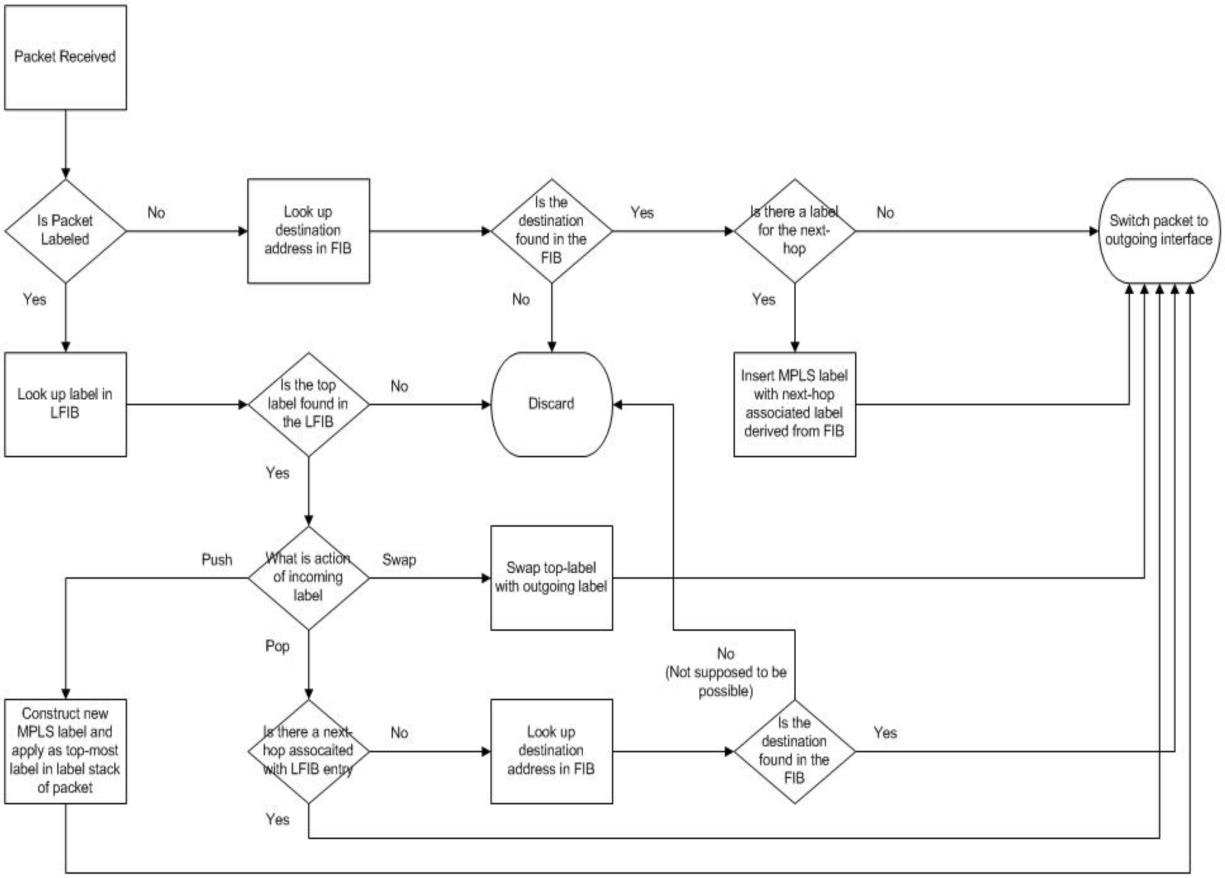
```
interface FastEthernet0/1
 ip address 20.20.20.20 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 network 20.20.20.0 0.0.0.255 area 0
 network 120.1.1.0 0.0.0.255 area 0
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 100 permit ip 120.1.1.0 0.0.0.255 150.1.1.0 0.0.0.255
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Note: IP address, VRFs and IPSEC-VPN will vary according to routers

3.2 Block Diagram


LIB: Label Information Base
LFIB: Label Forwarding Information Base
Control Plane
IP Routing Protocols
Routing information exchange with other routers
IP Routing Table
LIB
MPLS IP Routing
Label binding and exchange with other routers
Data Plane
Incoming labeled packet
LFIB
Outgoing labeled packet

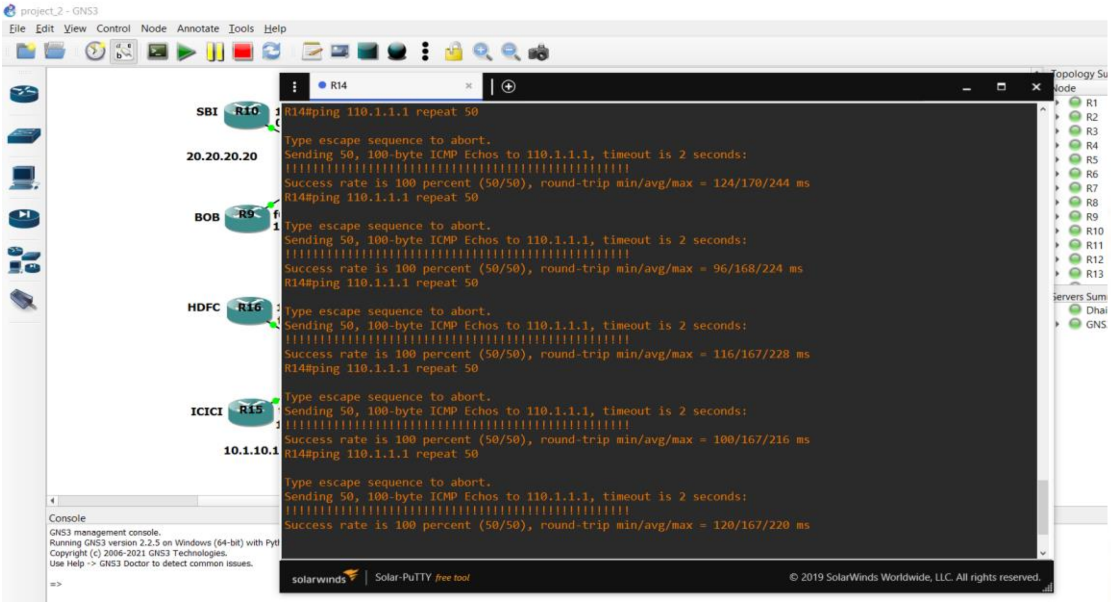
3.3 Flow Chart


Packet Received
Is Packet Labeled
No
Yes
Look up destination address in FIB
Is the destination found in the FIB
Yes
No
Is there a label for the next-hop
No
Yes
Switch packet to outgoing interface
Look up label in LFIB
Is the top label found in the LFIB
No
Yes
Discard
Insert MPLS label with next-hop associated label derived from FIB
What is action of incoming label
Push
Swap
Pop
Swap top-label with outgoing label
Construct new MPLS label and apply as top-most label in label stack of packet
Is there a next-hop associcated with LFIB entry
No
Yes
Look up destination address in FIB
No
(Not supposed to be possible)
Is the destination found in the FIB
Yes

3.4 Expected Output

1. Fast Speed: MPLS network is fast as compared to IP routing.

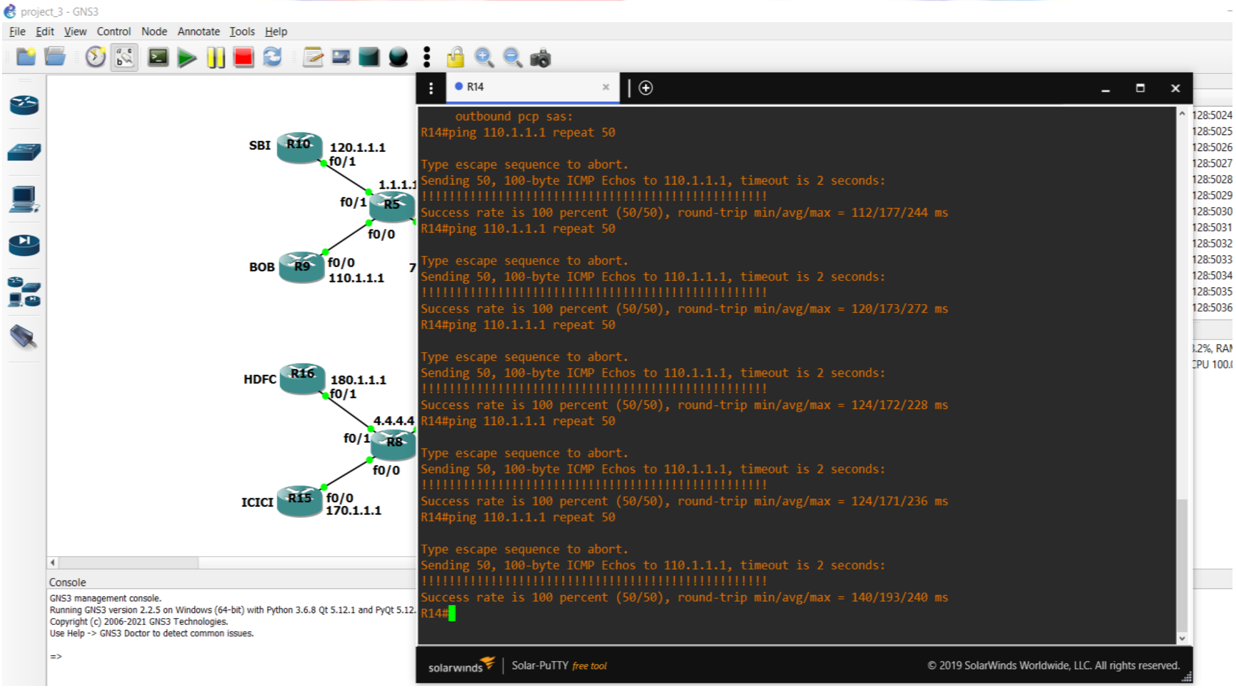
- MPLS: min/avg/max – 111.2/167.8/226.4 ms



```
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 124/170/244 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 96/168/224 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 116/167/228 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 100/167/216 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 120/167/220 ms
```

```
Console
GNS3 management console.
Running GNS3 version 2.2.5 on Windows (64-bit) with Pyt
Copyright (c) 2006-2021 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

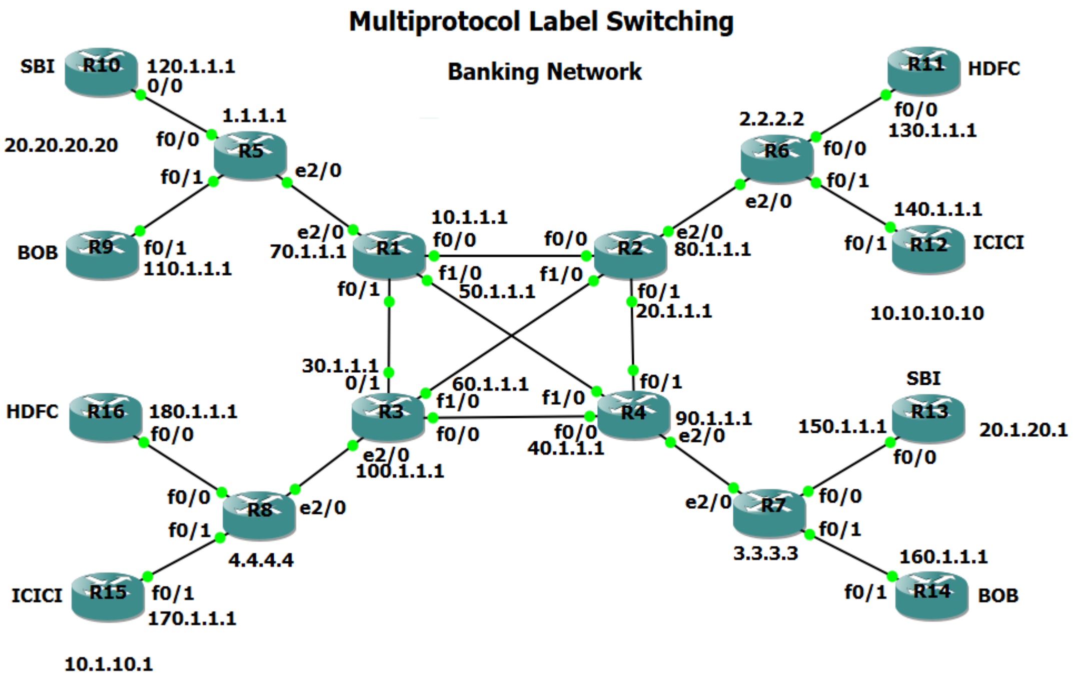
- OSPF: min/avg/max – 124/177.2/244 ms



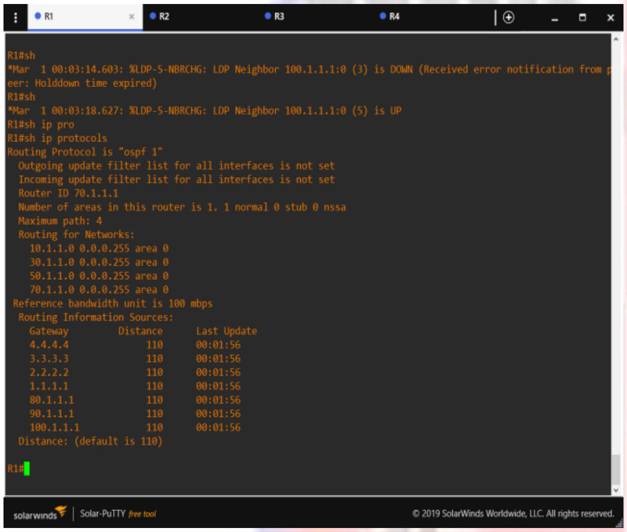
```
     outbound pcp sas:
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 112/177/244 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 120/173/272 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 124/172/228 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 124/171/236 ms
R14#ping 110.1.1.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 140/193/240 ms
R14#
```

```
Console
GNS3 management console.
Running GNS3 version 2.2.5 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2021 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

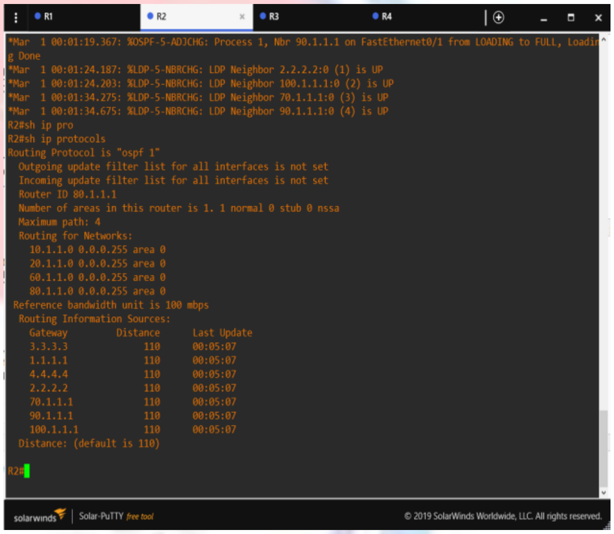
2. The use of one unified network infrastructure: There are some non-IP technologies which cannot be transmitted simply in IP infrastructure. For these technologies we have to use frame relay or ATM layer 2 switch along with IP routing protocol. But with use of MPLS-enabled Layer 3 IP backbone, we can carry non-IP traffic also in one infrastructure.



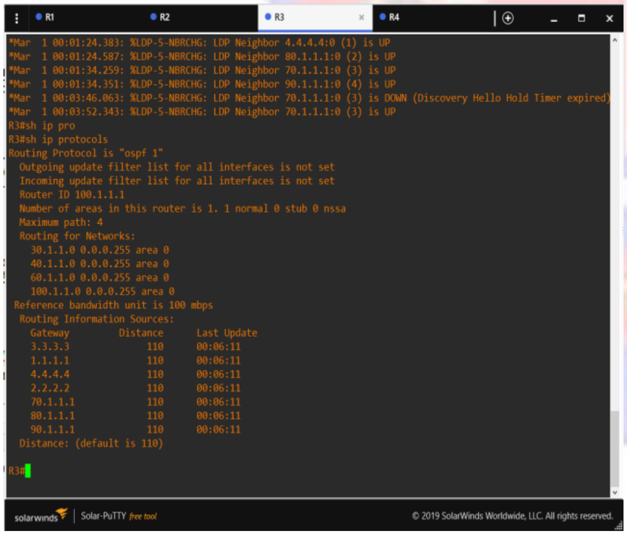
3. Border Gateway Protocol (BGP)-free core: If packet is to be send to different autonomous system, an Exterior Border Gateway Protocol (EBGP) is to be used and BGP is best EBGP protocol. This means that all routers in the service provider network must run BGP. MPLS, however, enables the forwarding of packets based on a label lookup rather than a lookup of the IP addresses. MPLS enables a label to be associated with an egress router rather than with the destination IP address of the packet. In our topology R1, R2, R3, R4 are core routers which are BGP free.



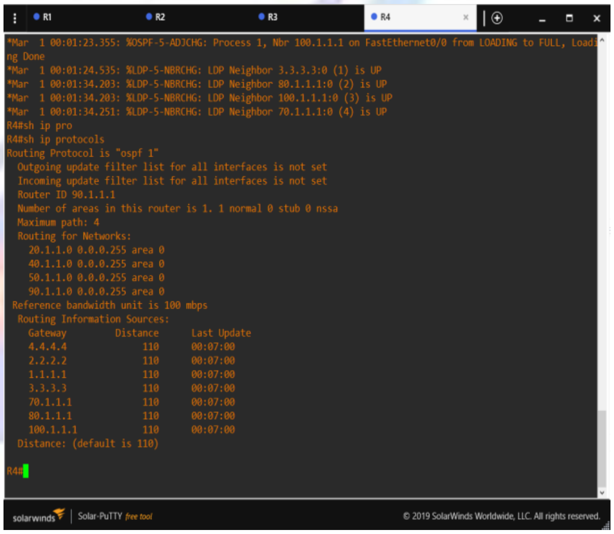
```
R1#sh
*Mar  1 00:03:14.603: %LDP-5-NBRCHG: LDP Neighbor 100.1.1.1:0 (3) is DOWN (Received error notification from p
eer: Holddown time expired)
R1#sh
*Mar  1 00:03:18.627: %LDP-5-NBRCHG: LDP Neighbor 100.1.1.1:0 (5) is UP
R1#sh ip pro
R1#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 70.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.0 0.0.0.255 area 0
    30.1.1.0 0.0.0.255 area 0
    50.1.1.0 0.0.0.255 area 0
    70.1.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    4.4.4.4              110      00:01:56
    3.3.3.3              110      00:01:56
    2.2.2.2              110      00:01:56
    1.1.1.1              110      00:01:56
    80.1.1.1             110      00:01:56
    90.1.1.1             110      00:01:56
    100.1.1.1            110      00:01:56
  Distance: (default is 110)

R1#
```



```
*Mar  1 00:01:19.367: %OSPF-5-ADJCHG: Process 1, Nbr 90.1.1.1 on FastEthernet0/1 from LOADING to FULL, Loadin
g Done
*Mar  1 00:01:24.187: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (1) is UP
*Mar  1 00:01:24.203: %LDP-5-NBRCHG: LDP Neighbor 100.1.1.1:0 (2) is UP
*Mar  1 00:01:34.275: %LDP-5-NBRCHG: LDP Neighbor 70.1.1.1:0 (3) is UP
*Mar  1 00:01:34.675: %LDP-5-NBRCHG: LDP Neighbor 90.1.1.1:0 (4) is UP
R2#sh ip pro
R2#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 80.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.0 0.0.0.255 area 0
    20.1.1.0 0.0.0.255 area 0
    60.1.1.0 0.0.0.255 area 0
    80.1.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:05:07
    1.1.1.1              110      00:05:07
    4.4.4.4              110      00:05:07
    2.2.2.2              110      00:05:07
    70.1.1.1             110      00:05:07
    90.1.1.1             110      00:05:07
    100.1.1.1            110      00:05:07
  Distance: (default is 110)

R2#
```

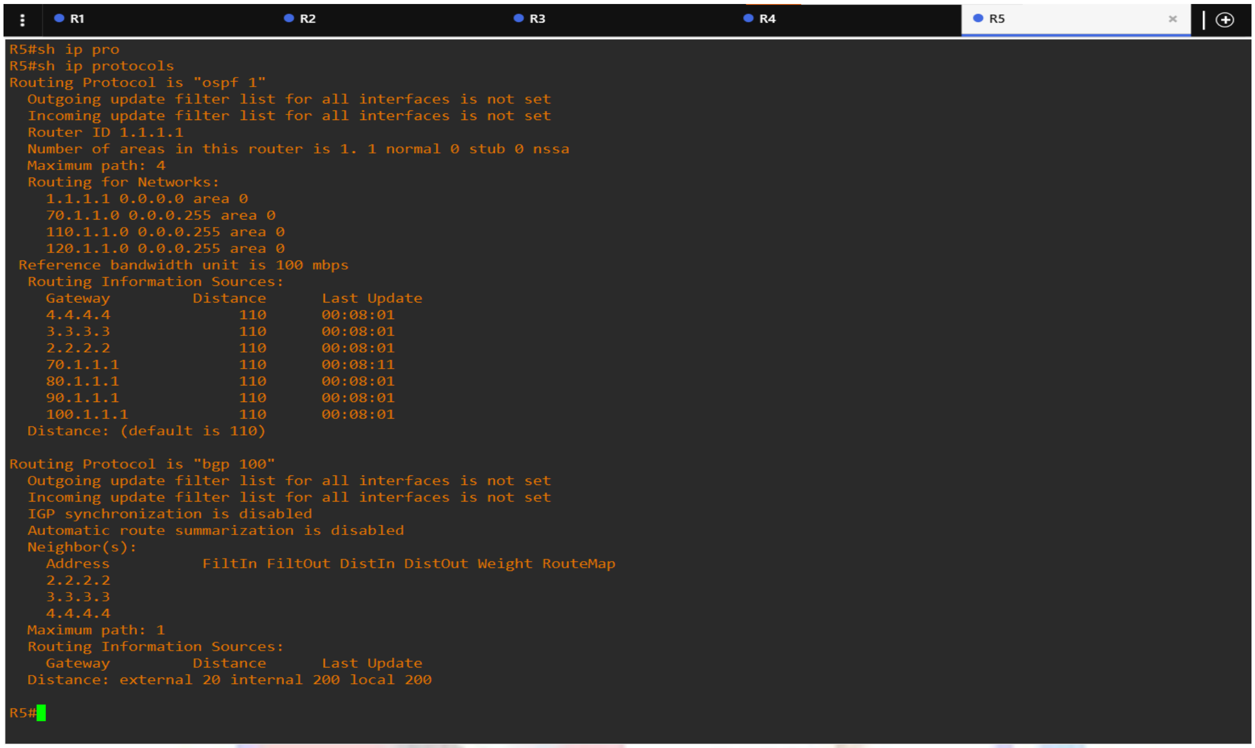


```
*Mar  1 00:01:24.383: %LDP-5-NBRCHG: LDP Neighbor 4.4.4.4:0 (1) is UP
*Mar  1 00:01:24.587: %LDP-5-NBRCHG: LDP Neighbor 80.1.1.1:0 (2) is UP
*Mar  1 00:01:34.259: %LDP-5-NBRCHG: LDP Neighbor 70.1.1.1:0 (3) is UP
*Mar  1 00:01:34.351: %LDP-5-NBRCHG: LDP Neighbor 90.1.1.1:0 (4) is UP
*Mar  1 00:03:46.063: %LDP-5-NBRCHG: LDP Neighbor 70.1.1.1:0 (3) is DOWN (Discovery Hello Hold Timer expired)
*Mar  1 00:03:52.343: %LDP-5-NBRCHG: LDP Neighbor 70.1.1.1:0 (3) is UP
R3#sh ip pro
R3#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 100.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    30.1.1.0 0.0.0.255 area 0
    40.1.1.0 0.0.0.255 area 0
    60.1.1.0 0.0.0.255 area 0
    100.1.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:06:11
    1.1.1.1              110      00:06:11
    4.4.4.4              110      00:06:11
    2.2.2.2              110      00:06:11
    70.1.1.1             110      00:06:11
    80.1.1.1             110      00:06:11
    90.1.1.1             110      00:06:11
  Distance: (default is 110)

R3#
```



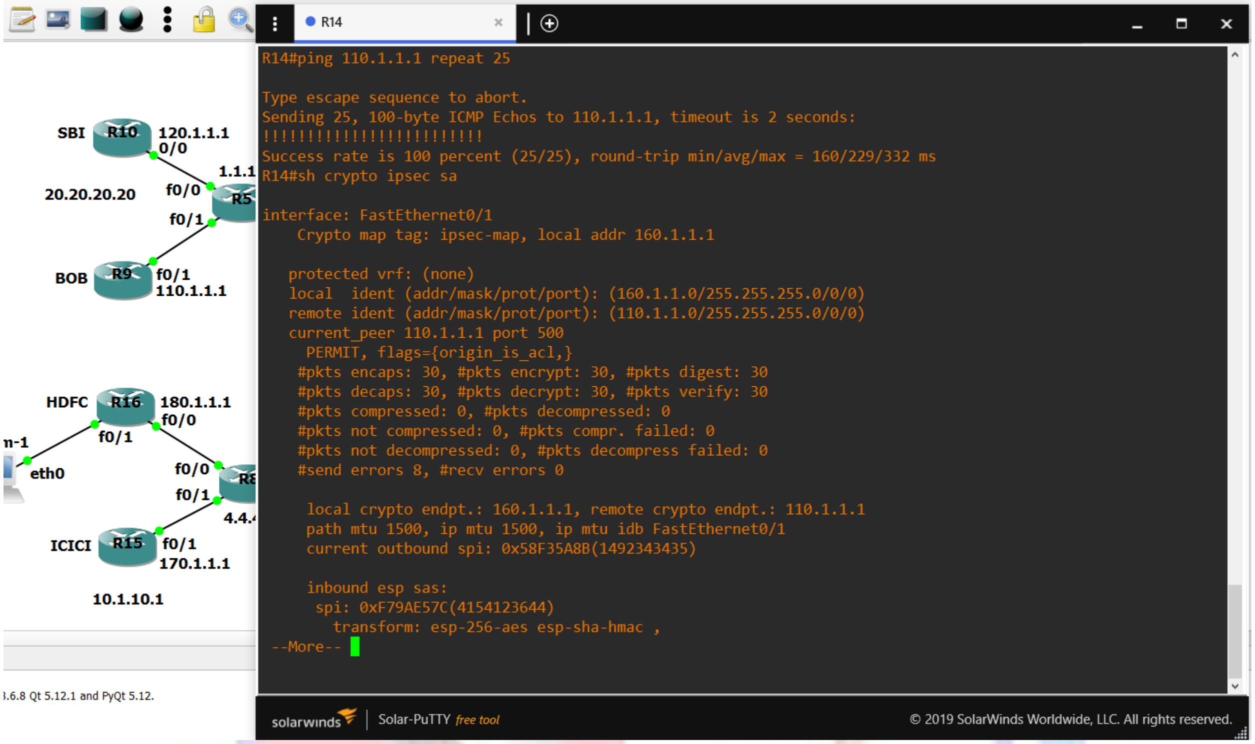
```
*Mar  1 00:01:23.355: %OSPF-5-ADJCHG: Process 1, Nbr 100.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loadi
ng Done
*Mar  1 00:01:24.535: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (1) is UP
*Mar  1 00:01:34.203: %LDP-5-NBRCHG: LDP Neighbor 80.1.1.1:0 (2) is UP
*Mar  1 00:01:34.203: %LDP-5-NBRCHG: LDP Neighbor 100.1.1.1:0 (3) is UP
*Mar  1 00:01:34.251: %LDP-5-NBRCHG: LDP Neighbor 70.1.1.1:0 (4) is UP
R4#sh ip pro
R4#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 90.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    20.1.1.0 0.0.0.255 area 0
    40.1.1.0 0.0.0.255 area 0
    50.1.1.0 0.0.0.255 area 0
    90.1.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    4.4.4.4              110      00:07:00
    2.2.2.2              110      00:07:00
    1.1.1.1              110      00:07:00
    3.3.3.3              110      00:07:00
    70.1.1.1             110      00:07:00
    80.1.1.1             110      00:07:00
    100.1.1.1            110      00:07:00
  Distance: (default is 110)

R4#
```

But Routers R5, R6, R7 and R8 are not core routers, hence there is BGP protocols running in them.



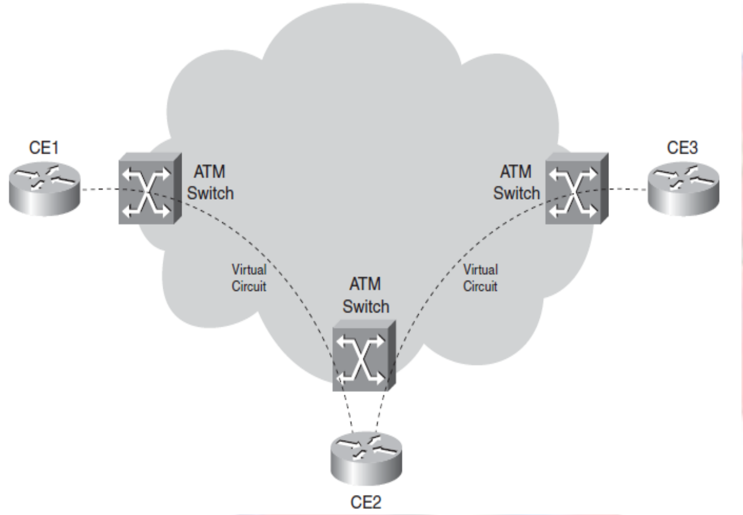
```
R5#sh ip pro
R5#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    1.1.1.1 0.0.0.0 area 0
    70.1.1.0 0.0.0.255 area 0
    110.1.1.0 0.0.0.255 area 0
    120.1.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    4.4.4.4              110      00:08:01
    3.3.3.3              110      00:08:01
    2.2.2.2              110      00:08:01
    70.1.1.1             110      00:08:11
    80.1.1.1             110      00:08:01
    90.1.1.1             110      00:08:01
    100.1.1.1            110      00:08:01
  Distance: (default is 110)

Routing Protocol is "bgp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    2.2.2.2
    3.3.3.3
    4.4.4.4
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: external 20 internal 200 local 200

R5#
```

4. The peer-to-peer model for MPLS VPN: IPSEC-VPN is configured to provide end-to-end encryption

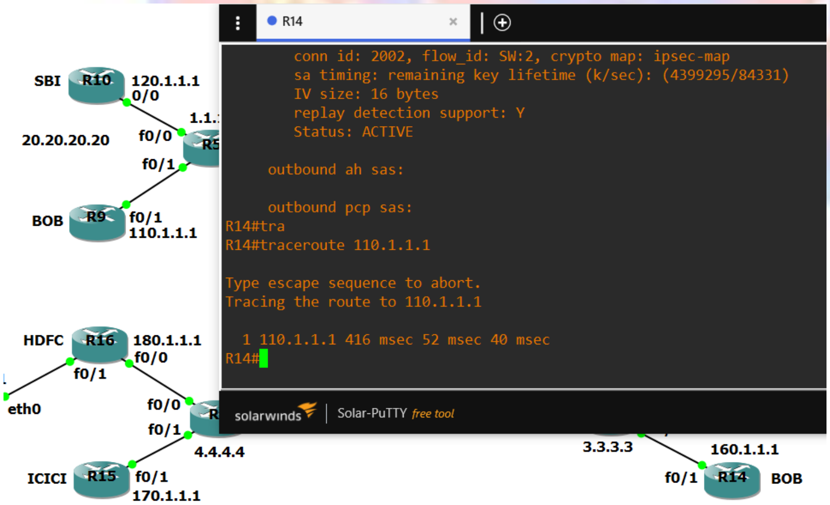


```
R14#ping 110.1.1.1 repeat 25

Type escape sequence to abort.
Sending 25, 100-byte ICMP Echos to 110.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (25/25), round-trip min/avg/max = 160/229/332 ms
R14#sh crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: ipsec-map, local addr 160.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (160.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (110.1.1.0/255.255.255.0/0/0)
   current_peer 110.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 8, #recv errors 0

     local crypto endpt.: 160.1.1.1, remote crypto endpt.: 110.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x58F35A8B(1492343435)

     inbound esp sas:
      spi: 0xF79AE57C(4154123644)
        transform: esp-256-aes esp-sha-hmac ,
 --More--
```

5. Optimal Traffic flow: For any router to send traffic directly to any other router at the edge, a virtual circuit must be created between them directly. Creating the virtual circuits manually is tedious. In any case, if the requirement is the any-to-any connection between sites, it is necessary to have a full mesh of virtual circuits between the sites, which is cumbersome and costly.



If the sites are only interconnected, the traffic from CE1 to CE3 must first go through CE2. The result is that the traffic crosses the ATM backbone twice and takes a detour through the router CE2. When using MPLS VPN, the traffic flows directly between all customer sites. If I want to connect two customers, say CE1 and CE2, I will be able to connect them directly without configuring full mesh connectivity.



```
        conn id: 2002, flow_id: SW:2, crypto map: ipsec-map
        sa timing: remaining key lifetime (k/sec): (4399295/84331)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
R14#tra
R14#traceroute 110.1.1.1

Type escape sequence to abort.
Tracing the route to 110.1.1.1

  1 110.1.1.1 416 msec 52 msec 40 msec
R14#
```

References

https://www.networkworld.com/article/2297171/network-security-mpls-explained.html

https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

https://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

https://searchnetworking.techtarget.com/definition/Multiprotocol-Label-Switching-MPLS

https://www.rcrwireless.com/20140513/fundamentals/mpls-routing

https://www.forcepoint.com/cyber-edu/mpls-multiprotocol-label-switching

https://searchnetworking.techtarget.com/tip/Configuring-MPLS-and-VRF-Cisco-CCIP-MPLS-certification-Lesson-6#:~:text=Virtual%20Routing%20and%20Forwarding%20(VRF,customer%20edge%20(CE)%20routers.&text=This%20unique%20separation%20of%20routing,customers%20are%20using%20identical%20addressing.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/12_2sba/feature/guide/vrflite.html

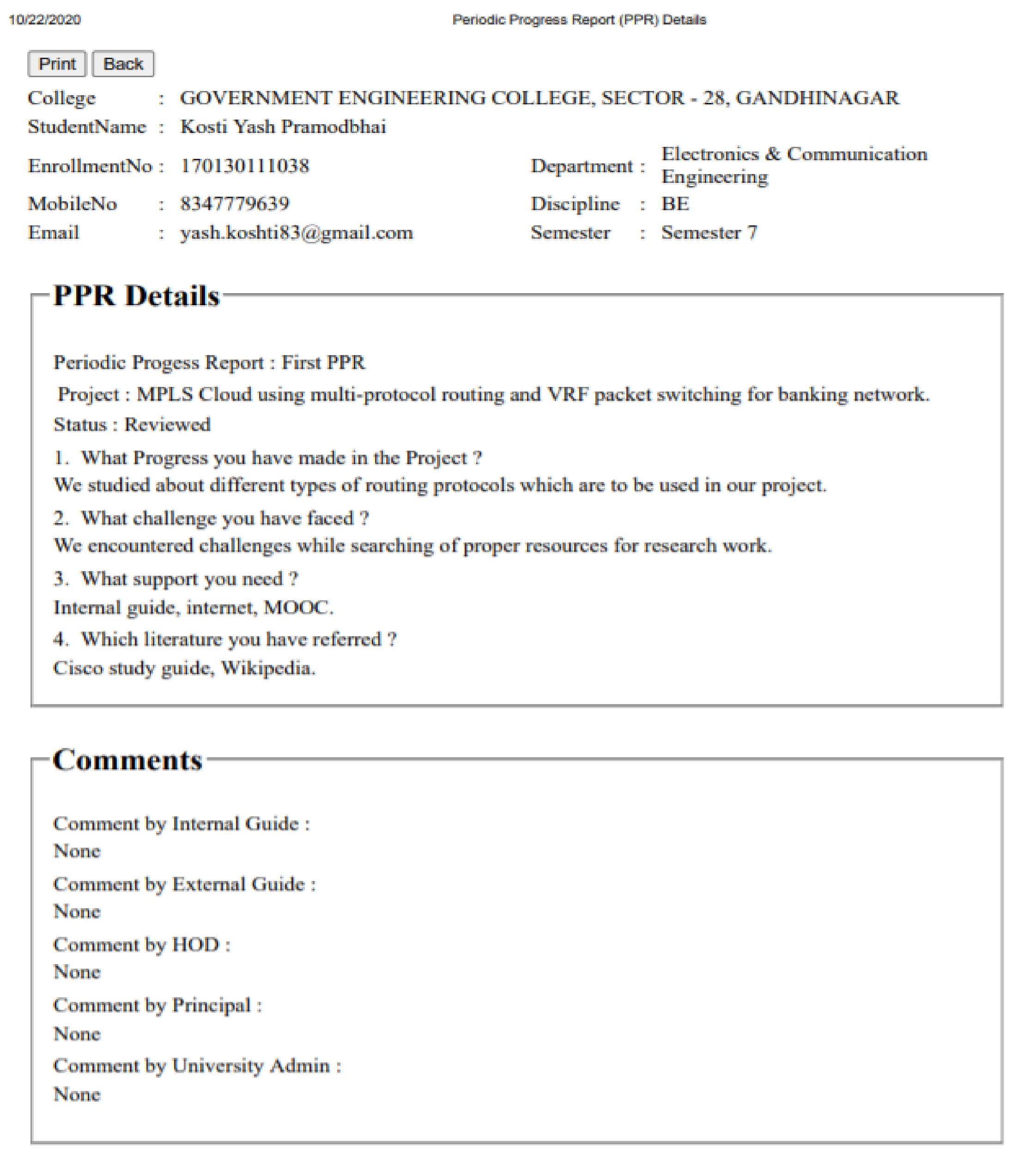
https://www.cisco.com/c/en/us/td/docs/ios xml/ios/mp_l3_vpns/configuration/xe-16/mp-l3-vpns-xe-16-book/mpls-vpn-vrf-selection-using-policy-based-routing.html

https://networklessons.com/tag/vrf

https://www.plixer.com/blog/what-is-vrf-virtual-routing-and-forwarding/

Appendix:

1) PPR
2) PSAR



10/22/2020 Periodic Progress Report (PPR) Details

College :	GOVERNMENT ENGINEERING COLLEGE, SECTOR - 28, GANDHINAGAR		
StudentName :	Kosti Yash Pramodbhai		
EnrollmentNo :	170130111038	Department :	Electronics & Communication Engineering
MobileNo :	8347779639	Discipline :	BE
Email :	yash.koshti83@gmail.com	Semester :	Semester 7

PPR Details

Periodic Progess Report : First PPR

Project : MPLS Cloud using multi-protocol routing and VRF packet switching for banking network.

Status : Reviewed

1. What Progress you have made in the Project ?

We studied about different types of routing protocols which are to be used in our project.

2. What challenge you have faced ?

We encountered challenges while searching of proper resources for research work.

3. What support you need ?

Internal guide, internet, MOOC.

4. Which literature you have referred ?

Cisco study guide, Wikipedia.

Comments

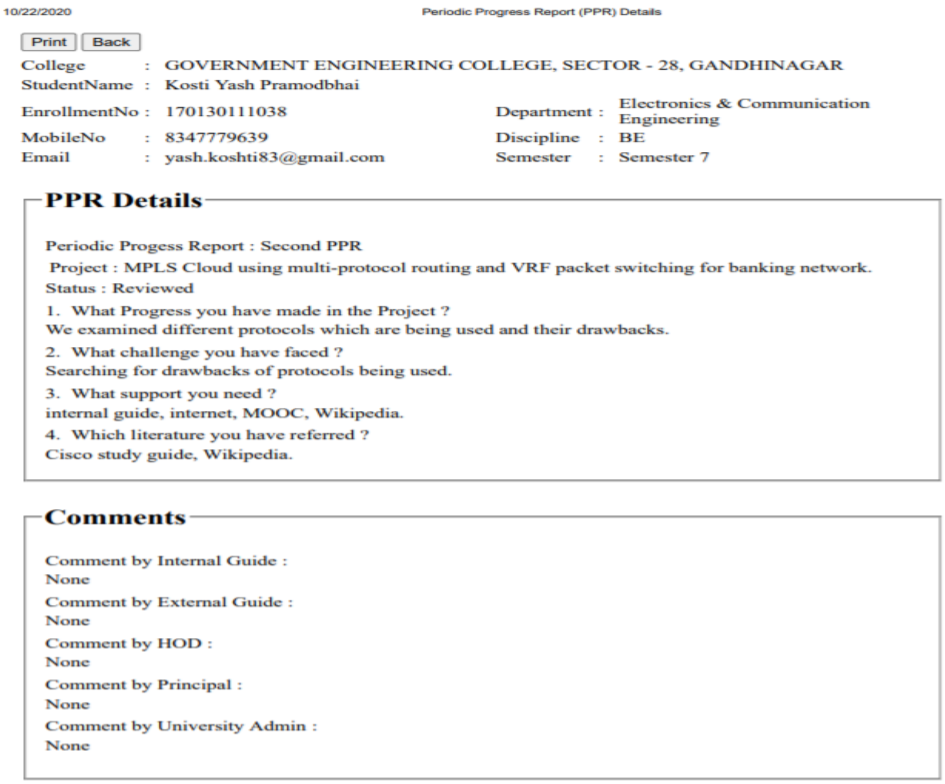
Comment by Internal Guide :
None

Comment by External Guide :
None

Comment by HOD :
None

Comment by Principal :
None

Comment by University Admin :
None



10/22/2020 Periodic Progress Report (PPR) Details

College : GOVERNMENT ENGINEERING COLLEGE, SECTOR - 28, GANDHINAGAR
StudentName : Kosti Yash Pramodbhai
EnrollmentNo : 170130111038 Department : Electronics & Communication Engineering
MobileNo : 8347779639 Discipline : BE
Email : yash.koshti83@gmail.com Semester : Semester 7

PPR Details

Periodic Progess Report : Second PPR
Project : MPLS Cloud using multi-protocol routing and VRF packet switching for banking network.
Status : Reviewed

1. What Progress you have made in the Project ?
We examined different protocols which are being used and their drawbacks.

2. What challenge you have faced ?
Searching for drawbacks of protocols being used.

3. What support you need ?
internal guide, internet, MOOC, Wikipedia.

4. Which literature you have referred ?
Cisco study guide, Wikipedia.

Comments

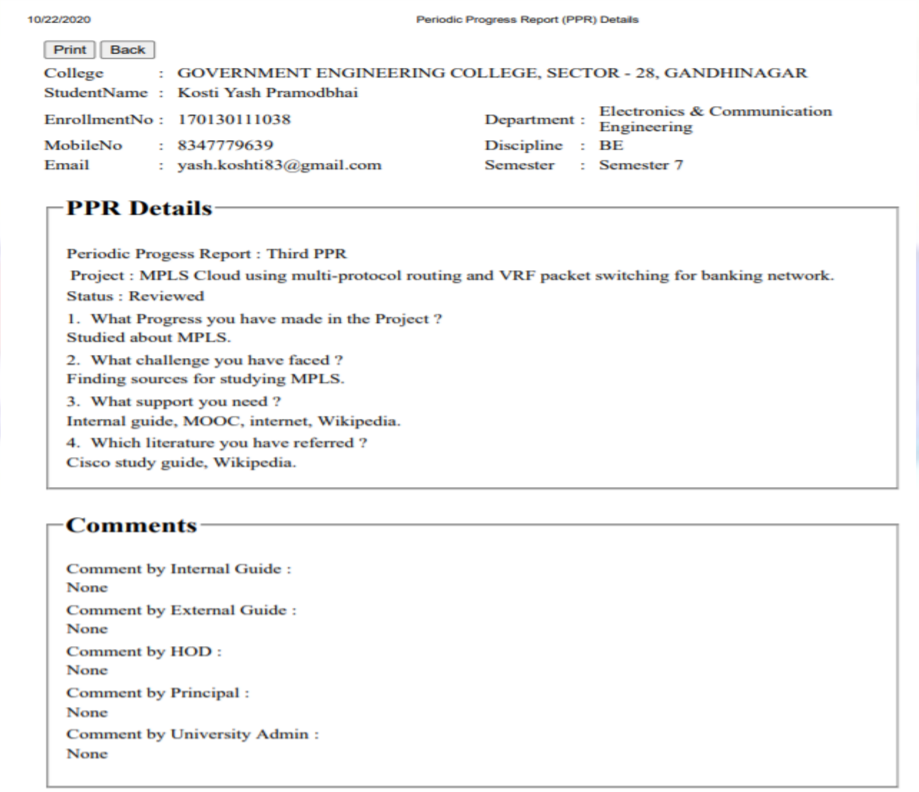
Comment by Internal Guide :
None

Comment by External Guide :
None

Comment by HOD :
None

Comment by Principal :
None

Comment by University Admin :
None



10/22/2020 Periodic Progress Report (PPR) Details

College : GOVERNMENT ENGINEERING COLLEGE, SECTOR - 28, GANDHINAGAR
StudentName : Kosti Yash Pramodbhai
EnrollmentNo : 170130111038 Department : Electronics & Communication Engineering
MobileNo : 8347779639 Discipline : BE
Email : yash.koshti83@gmail.com Semester : Semester 7

PPR Details

Periodic Progess Report : Third PPR
Project : MPLS Cloud using multi-protocol routing and VRF packet switching for banking network.
Status : Reviewed

1. What Progress you have made in the Project ?
Studied about MPLS.

2. What challenge you have faced ?
Finding sources for studying MPLS.

3. What support you need ?
Internal guide, MOOC, internet, Wikipedia.

4. Which literature you have referred ?
Cisco study guide, Wikipedia.

Comments

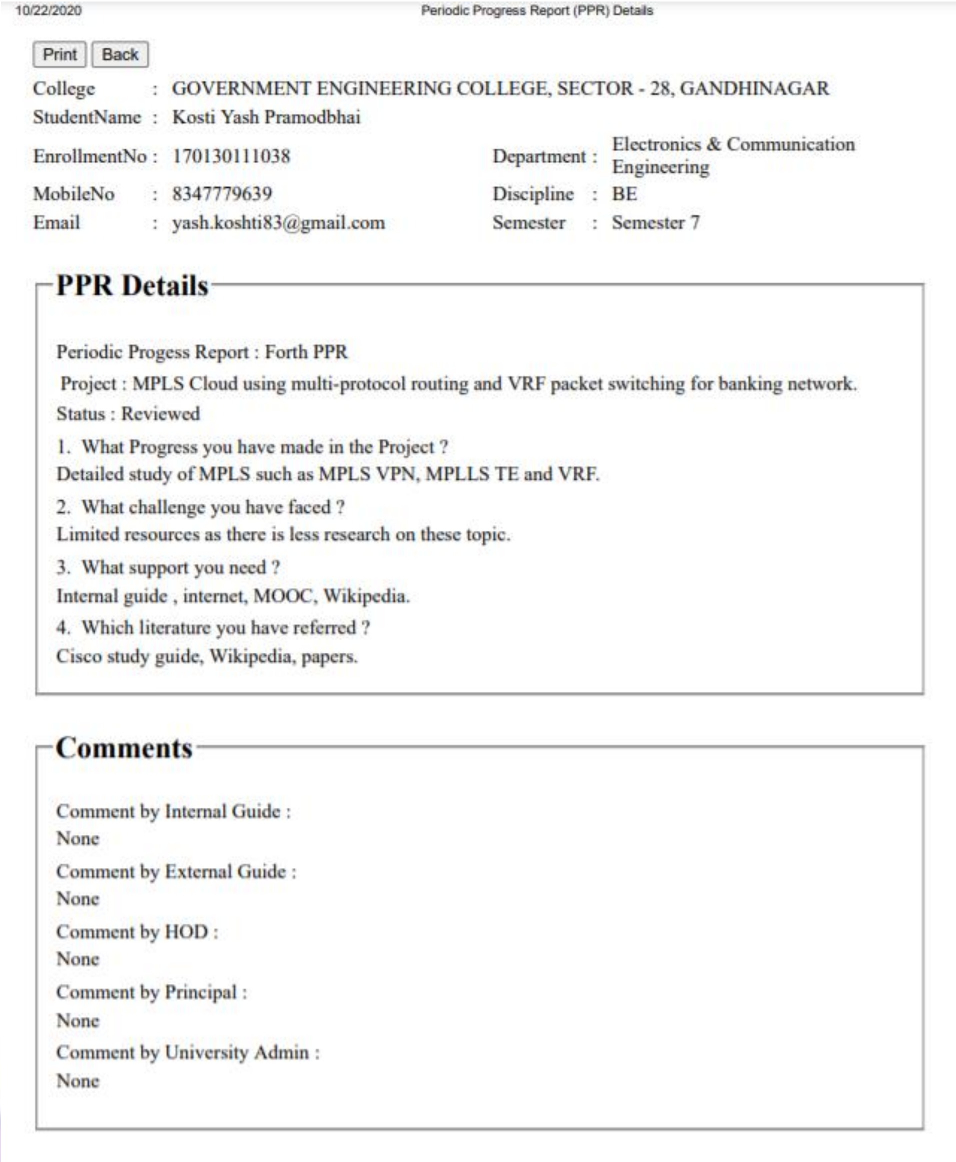
Comment by Internal Guide :
None

Comment by External Guide :
None

Comment by HOD :
None

Comment by Principal :
None

Comment by University Admin :
None



10/22/2020 Periodic Progress Report (PPR) Details

College	: GOVERNMENT ENGINEERING COLLEGE, SECTOR - 28, GANDHINAGAR		
StudentName	: Kosti Yash Pramodbhai		
EnrollmentNo	: 170130111038	Department :	Electronics & Communication Engineering
MobileNo	: 8347779639	Discipline	: BE
Email	: yash.koshti83@gmail.com	Semester	: Semester 7

PPR Details

Periodic Progess Report : Forth PPR

Project : MPLS Cloud using multi-protocol routing and VRF packet switching for banking network.

Status : Reviewed

1. What Progress you have made in the Project ?

Detailed study of MPLS such as MPLS VPN, MPLLS TE and VRF.

2. What challenge you have faced ?

Limited resources as there is less research on these topic.

3. What support you need ?

Internal guide , internet, MOOC, Wikipedia.

4. Which literature you have referred ?

Cisco study guide, Wikipedia, papers.

Comments

Comment by Internal Guide :

None

Comment by External Guide :

None

Comment by HOD :

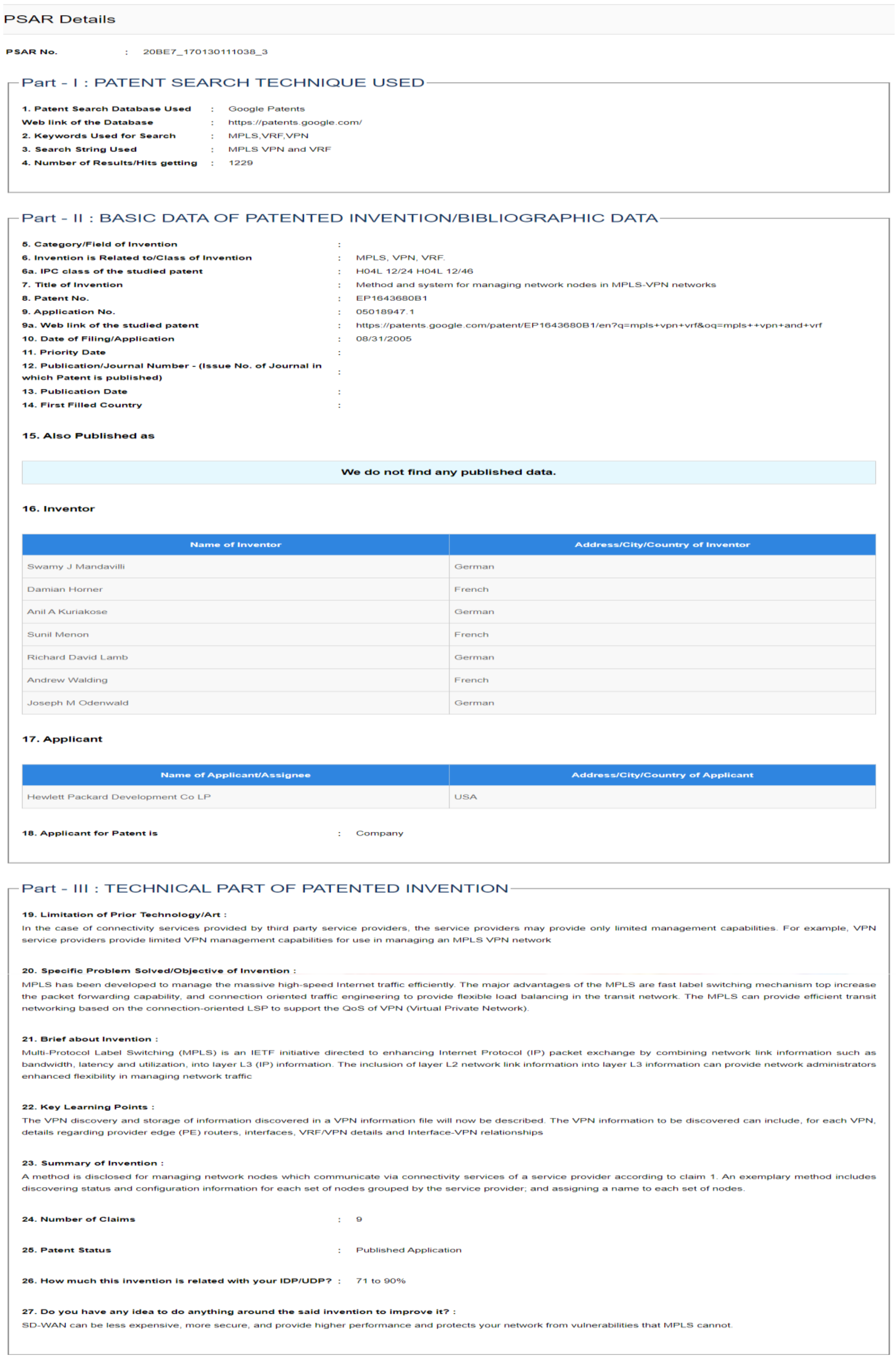
None

Comment by Principal :

None

Comment by University Admin :

None



PSAR Details

PSAR No. : 20BE7_170130111038_3

Part - I : PATENT SEARCH TECHNIQUE USED

1. Patent Search Database Used : Google Patents
Web link of the Database : https://patents.google.com/
2. Keywords Used for Search : MPLS,VRF,VPN
3. Search String Used : MPLS VPN and VRF
4. Number of Results/Hits getting : 1229

Part - II : BASIC DATA OF PATENTED INVENTION/BIBLIOGRAPHIC DATA

5. Category/Field of Invention :
6. Invention is Related to/Class of Invention : MPLS, VPN, VRF.
6a. IPC class of the studied patent : H04L 12/24 H04L 12/46
7. Title of Invention : Method and system for managing network nodes in MPLS-VPN networks
8. Patent No. : EP1643680B1
9. Application No. : 05018947.1
9a. Web link of the studied patent : https://patents.google.com/patent/EP1643680B1/en?q=mpls+vpn+vrf&oq=mpls++vpn+and+vrf
10. Date of Filing/Application : 08/31/2005
11. Priority Date :
12. Publication/Journal Number - (Issue No. of Journal in which Patent is published) :
13. Publication Date :
14. First Filled Country :

15. Also Published as

We do not find any published data.

16. Inventor

Name of Inventor	Address/City/Country of Inventor
Swamy J Mandavilli	German
Damian Horner	French
Anil A Kuriakose	German
Sunil Menon	French
Richard David Lamb	German
Andrew Walding	French
Joseph M Odenwald	German

17. Applicant

Name of Applicant/Assignee	Address/City/Country of Applicant
Hewlett Packard Development Co LP	USA

18. Applicant for Patent is : Company

Part - III : TECHNICAL PART OF PATENTED INVENTION

19. Limitation of Prior Technology/Art :
In the case of connectivity services provided by third party service providers, the service providers may provide only limited management capabilities. For example, VPN service providers provide limited VPN management capabilities for use in managing an MPLS VPN network

20. Specific Problem Solved/Objective of Invention :
MPLS has been developed to manage the massive high-speed Internet traffic efficiently. The major advantages of the MPLS are fast label switching mechanism top increase the packet forwarding capability, and connection oriented traffic engineering to provide flexible load balancing in the transit network. The MPLS can provide efficient transit networking based on the connection-oriented LSP to support the QoS of VPN (Virtual Private Network).

21. Brief about Invention :
Multi-Protocol Label Switching (MPLS) is an IETF initiative directed to enhancing Internet Protocol (IP) packet exchange by combining network link information such as bandwidth, latency and utilization, into layer L3 (IP) information. The inclusion of layer L2 network link information into layer L3 information can provide network administrators enhanced flexibility in managing network traffic

22. Key Learning Points :
The VPN discovery and storage of information discovered in a VPN information file will now be described. The VPN information to be discovered can include, for each VPN, details regarding provider edge (PE) routers, interfaces, VRF/VPN details and Interface-VPN relationships

23. Summary of Invention :
A method is disclosed for managing network nodes which communicate via connectivity services of a service provider according to claim 1. An exemplary method includes discovering status and configuration information for each set of nodes grouped by the service provider; and assigning a name to each set of nodes.

24. Number of Claims : 9

25. Patent Status : Published Application

26. How much this invention is related with your IDP/UDP? : 71 to 90%

27. Do you have any idea to do anything around the said invention to improve it? :
SD-WAN can be less expensive, more secure, and provide higher performance and protects your network from vulnerabilities that MPLS cannot.