
2018

# Implementing MPLS VPN on an existing Large OSPF Network

# Table of Contents

Table of Figures ..... 2
1. Executive Summary ..... 3
2. Acronyms ..... 5
3. Overview ..... 6
3.1. Current Network Depolyment ..... 6
4. Project Objectives ..... 7
4.1. Project Business and Technical Goals ..... 7
4.2. Capital and Operating Requirement ..... 8
5. Requirements ..... 9
6. Network Diagram ..... 10
7. Configuration ..... 12
7.1. Routing table of PE-1 ..... 17
7.2. Create VRFs on PE1 end PE2. ..... 18
7.3. Assign Interfaces to a specific VRF. ..... 20
7.4. No connectivity of customer network with ISP network ..... 20
7.5. Connectivity of regional site-3 ..... 20
8. Gantt chart ..... 21
9. System Development Plan ..... 21
10. Conclusion ..... 23
11. References ..... 23

# Table of Figures

Figure 1 VPN Site to Site Network ..... 3
Figure 2 Price of equipment used in network ..... 8
Figure 3 Network Diagram for MPLS VPN ..... 10
Figure 4 Routing table of PE-1 ..... 18
Figure 5 Create VRFs on PE1 ..... 19
Figure 6 Create VRFs PE2. ..... 19
Figure 7 Assign Interface to VRF ..... 20
Figure 8 No connectivity of customer network with ISP network ..... 20
Figure 9 Connectivity of regional site-3 ..... 21
Figure 10 Gantt Chart ..... 21

# 1. Executive Summary

MPLS technology for the next generation networks that is attracting networking experts around the globe. MPLS is essentially a hybrid forwarding/routing strategy which streamlines the backbone switching of IP packets between layer 2 and layer 3. Instead of IP address or MAC address, MPLS works on small labels. These lables are inserted between layer 2 and layer 3 of OSI. Forwarding decisions are based on these labels instead of having to look at complex IP tables. Thus, it reduces the overhead and makes forwarding decisions more efficient.

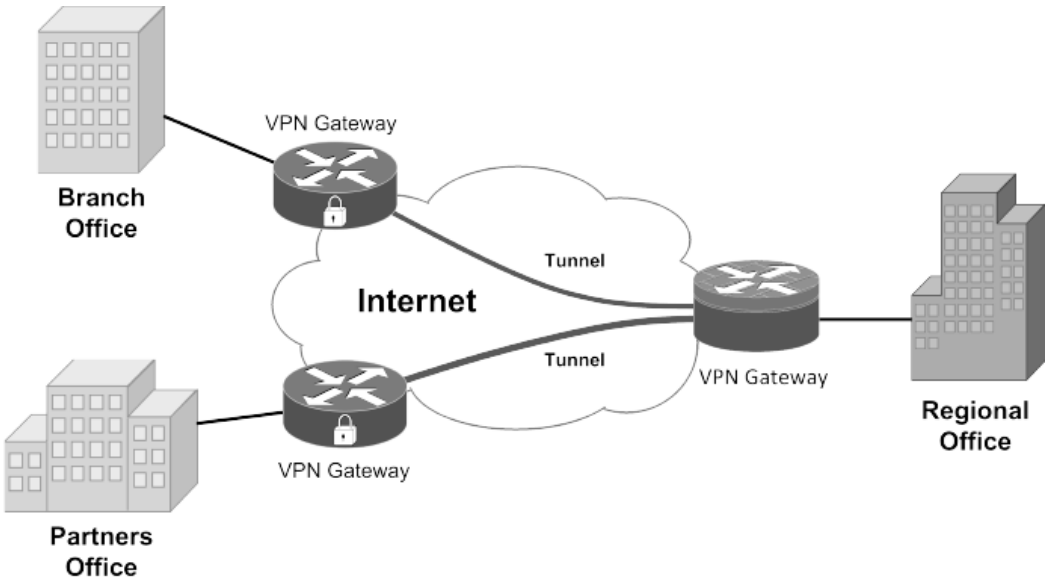



**Figure 1 VPN Site to Site Network**

The question arises about MPLS based VPN in a real network scenario. A MPLS based VPN is the implementation of VPN using the MPLS cloud. All the customer sites communicate with each other using the MPLS enabled provider network. MPLS labels make a tunnel in this scenario.

This report presents what makes today's communication fast by designing and deploying a communication network MPLS VPN for an office with an existing OSPF network. The network connectivity among the offices at different geographic locations has become a challenge for network professionals. VPN is used to counter this narrative. It has become a popular industry solution in recent years. MPLS is a relatively newer WAN technology providing advantages over other technologies. At the same time, it is compatible with existing technologies like ATM, FR, Ethernet and SONET.

In addition to updating the hardware, the proposed solution outlines some changes in the network configuration. These changes, if implemented, will provide greater reliability and security for all users of the MPLS-VPN network. Along with the new hardware, the new network configuration explore new possibilities in using the network to increase overall productivity and, in the end, better serve the needs of their customers.

The solution outlined below will provide the greatest benefit possible for implementation of new technology meeting all of the current needs and providing for future expansion--at the lowest cost possible. The total estimated cost for the project is just under $900,000; this takes into account not only resolving current network problems, but also the overall cost of network ownership in the future.

## 2. Acronyms

- VPN: Virtual Private Network
- MPLS: Multiprotocol Label Switching
- ATM: Asynchronous Transfer Mode
- FR: Frame Relay
- IPsec: Internet Protocol Security Protocol
- WAN: Wide Area Network
- LAN: Local Area Network
- ISP: Internet Service Provider
- FEC: Forward Equivalency Class
- LIB: Label Information Base
- P-Network Provider Network
- C-Network: Customer Network
- CE: Customer Edge
- PE: Provider Edge
- BGP: Border Gateway Protocol
- MP-BGP: Multi-protocol Border Gateway Protocol
- OSPF: Open Shortest Path First
- PPTP: Point-To-Point Tunneling Protocol
- L2TP: Layer 2 Tunneling Protocol
- SSL: Secure Socket Layer
- VRF: Virtual Routing and Forwarding

# 3. Overview

Technology has transformed the way we communicate. Communications are real-time now which used to take days or even months a couple of centuries back. It has changed everything and everyone from individual to organizations are benefitted from it.

VPN having connectivity via MPLS infrastructure is known as MPLS VPN. It offers many advantages over traditional VPN solutions. In this project, MPLS based VPN is implemented in a corporate environment. Three regional offices of an organization are connected with the central site through MPLS based ISP's network. Hub and spoke topology is implemented in this scenario.

The connectivity among the sites is established and forwarding decisions are made on the bases of MPLS labels instead of IP addresses. Furthermore, it is also observable in results that MPLS doesn't need any other tunneling protocol unlike traditional VPNs. It makes tunnels based on labels.

We gathered the requirements from our client and designed & deployed the MPLS over an existing and production network. The network uses Cisco equipment only. We have used MPLS VPN and have made provisions for which can easily accommodate the network load up to 5 years.

## 3.1. Current Network Depolyment

The current network uses inexpensive switches from several vendors, purchased over time. They comply with various standards, depending on when they were purchased. Specifically, the network is configured.

While the clients are connected in a mostly switched, star-wired bus network using Ethernet 100Base-T technology. In the few instances where switches are not used, hubs serve smaller workgroups of administrative and employee staff. And Internet gateway supports e-mail and online searches. The WAN uses 56-kbps links to two of the remote client and dialup connectivity to the other two. The one router uses static routing that was configured by a previous network designer. A firewall is used to prevents unauthorized access from the PSTN connection into the internal network.

The network using OSPF as a Routing Protocol and has no MPLS configured.

# 4. Project Objectives

1. Provide efficient solution for the requirements of the organization and users.
2. Improve the network's fault tolerance, security, and high-speed connection, which will increase the efficiency of day-to-day operations in the hospital by making access time quicker.
3. Identify the critical points of failure in the existing network and propose on how to eliminate them. Recommend which points of failure should be addressed to increase availability and how to increase this goal.
4. It must be secure, fast, reliable, scalable, etc.
5. The network technologies must be usable/compatible for at least 5 years.

## 4.1. Project Business and Technical Goals

1. **Easier Any-To-Any Connectivity.** Many voice and video applications utilize what is referred to as an any-to-any connection. MLPS improves the traffic flow in these connections by allowing for the interconnection of multiple sites.

2. **Outsourcing Routing Needs.** In an MPLS setup, the provider handles the routing of your network. This eliminates the burden of routing control on your company and makes MPLS operationally simpler than more traditionally routed networks. The removal of the routing burden on a company's network often lessens the strains and improves connectivity.

3. **Quality of Support Specification Is Built In.** With MPLS, companies can customize service level agreements to outline the specific supports they need. These include latency and packet loss minimums for each type of data. This allows the MPLS system to predetermine which packets take priority and to deliver those first – thereby improving connectivity.

## 4.2. Capital and Operating Requirement

This section of the report covers the estimated costs for this project.

| Hardware | Per Unit Cost | Quantity | Total Cost |
|---|---|---|---|
| Cisco Catalyst 6509-E Switch | $ 5,354.95 | 6 | $ 32,129.70 |
| Cisco Catalyst 3560-X Series Switches | $ 8,225.47 | 13 | $ 106,931.11 |
| Cisco Nexus 7000 Series Switches | $ 12,739.00 | 2 | $ 25,478.00 |
| Cisco 881 Integrated Services Router | $ 618.99 | 8 | $ 4,951.92 |
| CyberPower CP1500AVRLCD UPS - 900 Watt - 8.5 Ah | $ 149.99 | 20 | $ 2,999.80 |
| Cisco ASA 5510 Security Plus Firewall Edition - Security appliance | $ 2,475.00 | 8 | $ 19,800.00 |
| Cisco Small Business Pro POES5 PoE splitter | $ 24.99 | 6 | $ 149.94 |
| Cisco 10/100 8-Port VPN Router | $ 266.95 | 4 | $ 1,067.80 |
| Cisco Catalyst 3560G-24TS Switch - 24 ports - L3 - managed | $ 2,235.00 | 10 | $ 22,350.00 |
| RJ 45 Plugs *Pack of 50 | $ 49.99 | 12 | $ 599.88 |
| Cisco Small Business VC 220 Dome Network Camera | $ 567.47 | 5 | $ 2,837.35 |
| T1 Access Installation (monthly fee) | $ 350.00 | 4 | $ 1,400.00 |
| T3 Acess Installation (monthly fee) | $ 7,000.00 | 1 | $ 7,000.00 |
| 5-Mbps increments times $75 plus $5 per PVC | $ 5.00 | 4 | $ 20.00 |
| Labor (@ $75 per hr) | $ 75.00 | 900 | $ 67,500.00 |
| Network Analysis and Design | $ 150,000.00 | 1 | $ 150,000.00 |
| Network implementation | $ 150,000.00 | 1 | $ 150,000.00 |
| Training | $ 100,000.00 | 1 | $ 100,000.00 |
| Ongoing Network Supposrt and Maintenance | $ 100,000.00 | 1 | $ 100,000.00 |
| Other neccessay labor | $ 20,000.00 | 1 | $ 20,000.00 |
| | | | |
| **TOTAL COST** | | | **$ 815,215.50** |

Figure 2 Price of equipment used in network

## 5. Requirements

The requirements of the network extracted from the information given by the client are listed below:

1- The users must be able to communicate with users on other site including servers.
2- A secure connection is required between two sites.
3- Installation of routers, switches and firewalls on both sites.
4- Installation and configuration of Access point APs and IP Phones. (IP phones are used for voice over IP, for transmitting the voice calls over IP Network, such as the internet, instead of Traditional PSTN.)
5- This network must be designed to support future expansion.
6- The Documentation of the network must be complete and comprehensive.
7- Network technologies such as: MPLS VPN etc. is required to ensure requirement fulfillment.

## 6. Network Diagram

This network design leverages is based on the earlier deployed network which and is completely based on Cisco devices.

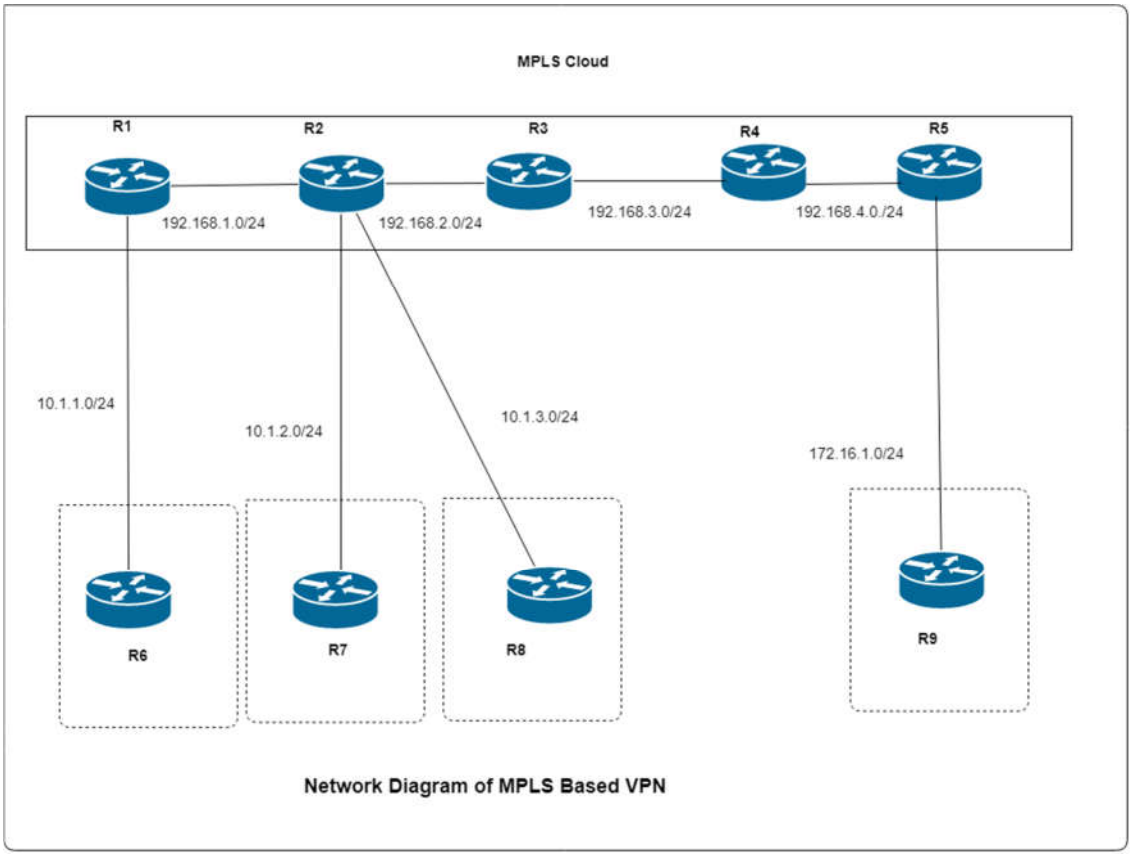



Figure 3 Network Diagram for MPLS VPN

- **Routers R1-R5** constitutes the MPLS network. It is also called the provider's network. MPLS is running on this network. In the context of MPLS VPN, routers R1, R2 and R5 are called Provider Edge (PE) routers. They are the devices that have direct connectivity with a customer's network.

- **Routers R6-R9** are called Customer Edge (CE) routers, they are gateways of a customer's network and the only device having connectivity with an ISP's network. The whole customer's network is called C-network.

- **Configuration at CE devices:** At CE devices, no special configuration is required. The only requirement is to assign IP addresses to interfaces and enable any IGP to carry the customer routes to connected PE devices.

- **Configuration at PE devices:** In the context of MPLS VPN, most important configurations are done in PE devices. All the parameters should be configured carefully to establish the VPN connectivity. One of the most important parameters is the configuration of Virtual Routing and Forwarding (VRF) instances. Inside, VRFs Route Distinguishers (RD) and route targets (export/imports) are defined.

- **PE-CE Routing:** PE-CE is routing that is achieved by using a BGP protocol. Any other Interior Gateway Protocol (IGP) like RIP, EIGRP or static routing can be used instead of BGP. If we use any other IGP, then we have to redistribute the routes from IGP to MP-BGP to share the VPN routes among the PE devices. This increases the complexity in configuration at PE devices. Hence, BGP is used because it shares the routes by default with MP-BGP and no routes re-distribution is required.

- **Provider network:** OSPF is configured as routing protocol in the provider network. Then MPLS is enabled on all provider network routers. MPLS labels are assigned based on routes of OSPF. MPLS doesn't work without a routing protocol in a network. It can work with any IGP running in the network.

- **MP-BGP Session:** It is possible that some VPN sites have exactly the same IP address. To overcome this problem, VPNv4 addresses are used. In VPNv4 RD is added to the IP address to make a unique 96 bit long address. But the issue arising is that it no longer remains an IPV4 or IPV6 address. A normal routing protocol cannot carry this routing information. Hence, MP-BGP is used to carry the VPNv4 addresses to other PE devices. In this scenario, MP-BGP sessions are established from routers R1 and R2 to router R5. As it is hub and spoke topology, we don't need MP-BGP connectivity between R1 and R2. [1]

# 7. Configuration

We configured the routers as mention in the table:

Table 1 Configuration of Routers

| **Router 6** |
| --- |
| R6#sh running-config<br>Building configuration...<br>current configuration : 1902 bytes version 12.4<br>hostname R6<br>interface Loopback0<br>ip address 10.2.1.10 255.255.255.255<br>!<br>interface FastEthernet0/0<br>ip address 10.1.1.1 255.255.255.0 duplex auto<br>speed auto<br>router bgp 65020<br>bgp log-neighbor-changes<br>neighbor 10.1.1.2 remote-as 65000<br>!<br>address-family ipv4<br>redistribute connected<br>neighbor 10.1.1.2 activate<br>neighbor 10.1.1.2 send-community<br>no auto-summary.<br>no synchronization exit-address-family<br>!<br>ip forward-protocol nd<br>!<br>ip bgp-community new-format<br>!<br>line vty 0 4<br>login<br>!<br>End |

**Router 1**

```
R1#sh running-config
Building configuration...
current configuration : 2422 bytes
!
version 12.4
hostname R1
ip vrf site-1
rd 65000:1
route-target export 65000:1 route-target export 65000:10 route-target
import 65000:4 route-target import 65000:40
!
interface Loopback0
ip address 192.168.1.10 255.255.255.255
!
interface fastethernet0/0
ip vrf forwarding site-1
ip address 10.1.1.2 255.255.255.0 duplex auto
speed auto
interface fastethernet1/0
ip address 192.168.1.1 255.255.255.252 duplex auto
speed auto
mpls ip
router ospf 100
log-adjacency-changes
network 192.168.1.0 0.0.0.3 area 1 network 192.168.1.10 0.0.0.0 area 1
!
router bgp 65000
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 192.168.4.10 remote-as 65000
neighbor 192.168.4.10 update-source Loopback0
!
address-family vpnv4
neighbor 192.168.4.10 activate
```

```
neighbor 192.168.4.10 send-community both exit-address-family
!
address-family ipv4 vrf site-1
neighbor 10.1.1.1 remote-as 65020
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 send-community
no synchronization
exit-address-family
end
```

**Router 2**

```
R2#sh running-config
building configuration...
!version 12.4
hostname R 2
ip cef
ip vrfsite - 2
rd 65000:2
route - target export 65000: 20
route - target import 65000:40
!
ip vrf site-3
rd 65000:3
route -target export 65000: 30
route - target import 65000:40
interface Loopback0
ip address 193.168.2.10 255.255.255.255
interface fastethernet0/0
ip vrf forwarding site-2
ip address 10.1.7.2 255.255.255.0
interface fastethernet0/1
ip vrf forwarding site-3
IP address 10.1.8.2 255.255.255.0
interface fastethernet1/0
```

```
ip address 193.168.1.2 255.255.255.252
mpls ip

router ospf 100
log-adjacency-changes
network 193.168.1.0 0.0.0.3 area 1
network 193.168.2.0 0.0.0.3 area 1
network 193.168.2.10 0.0.0.3 area 1
!
nob
no bgp defaultipv4 - unicast
bgp log-neighbor-changes
neighbor 193.168.4.10 remote-as65000
neighbor 193.168.4.10 update-source
Loopback0
!
address-family vpnv4
neighbor 193.168.4.10 activate
neighbor 193.168.4.10 send-community both
exit-address-family
!
address-family vpnv4 vrf site-3
neighbor 10.1.8.1 remote-as65040
neighbor 10.1.8.1 activate
neighbor 10.1.8.1 send-community no synchronization
exit-address-family
!
address-family vpnv4 vrf site-2
neighbor 10.1.7.1 remote-as65030
neighbor 10.1.7.1 activate
neighbor 10.1.7.1 send-community
end
```

**Router-5**

```
R5#sh running -config
Building configuration...
Current configuration : 2671 bytes
version 12.4
hostname R5
ip vrf site-1
route-target import 65000:20
route-target import 65000:30
!
ip vrf site-4
rd 65000:4
route-target export 65000:40
route-target import 65000:10
route-target import 65000:20
route-target import 65000:30
interface Loopback0
ip address 193.168.4.10 255.255.255.255
!
interface FastEthernet0/0
ip vrf forwarding site-4
ip address 172.16.1.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet2/0
ip address 193.168.4.2 255.255.255.252
duplex auto
speed auto
mpls ip
router ospf 100
log-adjacency-changes
network 193.168.4.0 0.0.0.3 area 1
network 193.168.4.10 0.0.0.0 area 1
```

```
!
Router bgp 65000
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 193.168.1.10 remote-as 65000
neighbor 193.168.1.10 update-source Loopback0
neighbor 193.1613.2.10 remote-as 65000
neighbor 193.168.2.10 update-source Loopback0
!
address-family vpnv4
neighbor 193.168.1.10 activate
neighbor 193.168.1.10 send-community both neighbor
193.168.2.10 activate
neighbor 193.168.2.10 send-community both exit-address-family
!
address-family ipv4 vrf site-4
neighbor 172.16.1.1 remote-as 65010 neighbor
172.16.1.1 activate
neighbor 172.16.1.1 send-community
no synchronization
end
```

## 7.1. Routing table of PE-1

In a VPN implementation the customer network is needed to hide from ISP's network. It is shown in Figure 4 that PE-1 has no route information of any customer sites. All it knows is the destination PE node.

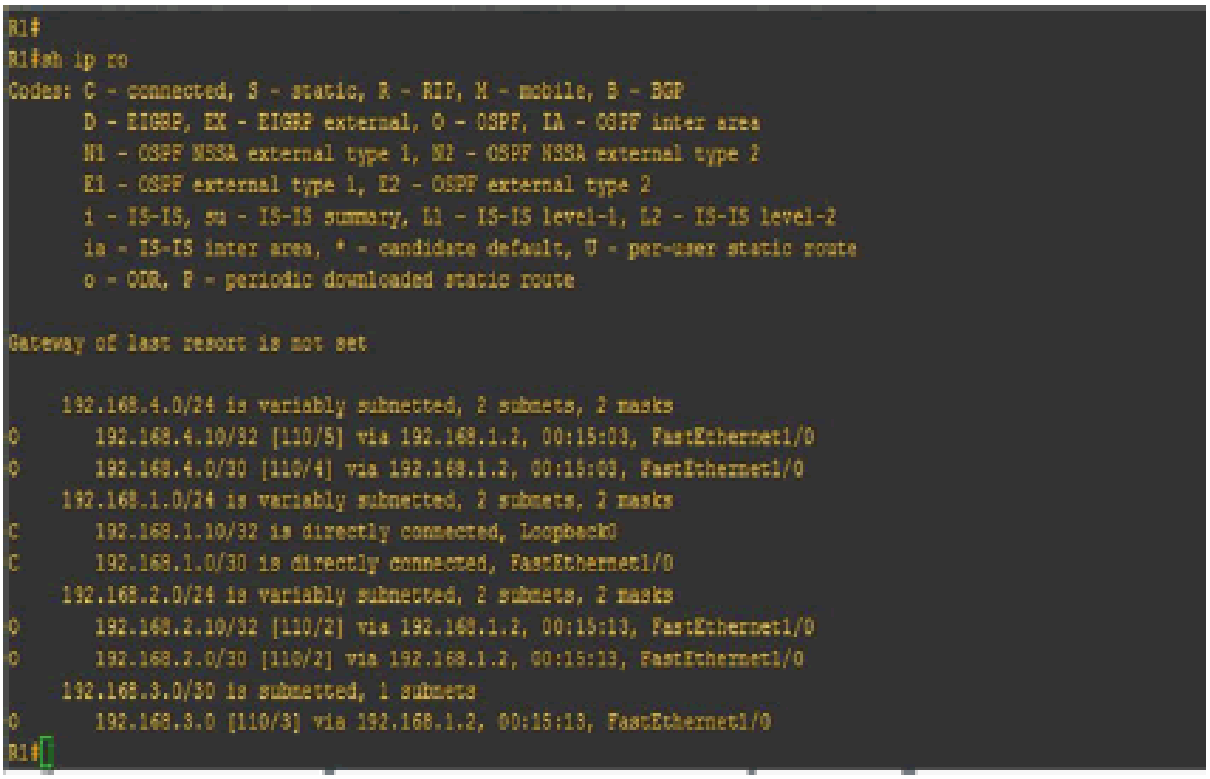



Figure 4 Routing table of PE-1

In a VPN, the customer information is not in the global routing table of the router. In fact, the information is present in VRFs and that is not accessible by the ISP network. That is why customer sites are hidden. Route targets are also defined in VRFs. **Figure 5** shows the VRF information of PE-1. It is important to note that imports the RT which is exported by PE-3. It exports RT 65000:10, which will be imported by PE-3.

## 7.2. Create VRFs on PE1 end PE2.

Same observations can be made in VRFs of PE-2, as shown in **Figure 6**. It has two VRFs and both import the same RT 65000:40, which is the export RF of PE-3. They also export their corresponding RTs, which must be imported at PE-3. At PE-3, all the RTs exported by VRFs in PE-1 and PE-2 must be imported. It should also export its RT of 65000:40. This can be observed in below.

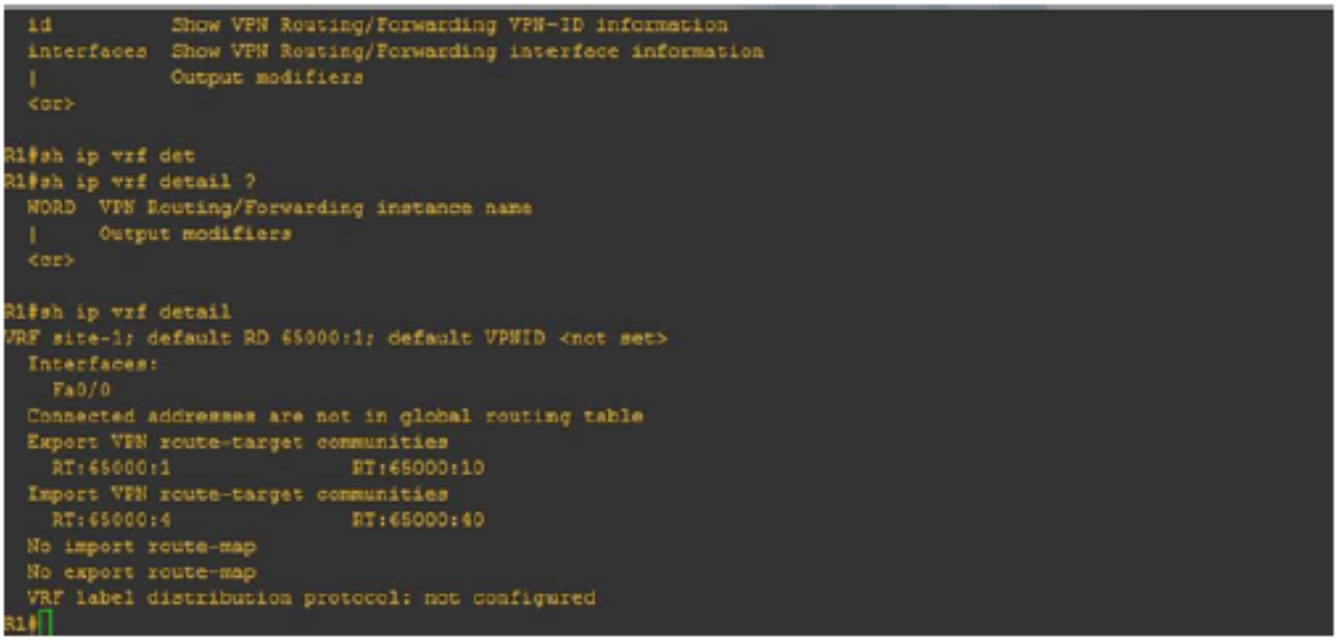



Figure 5 Create VRFs on PE1.

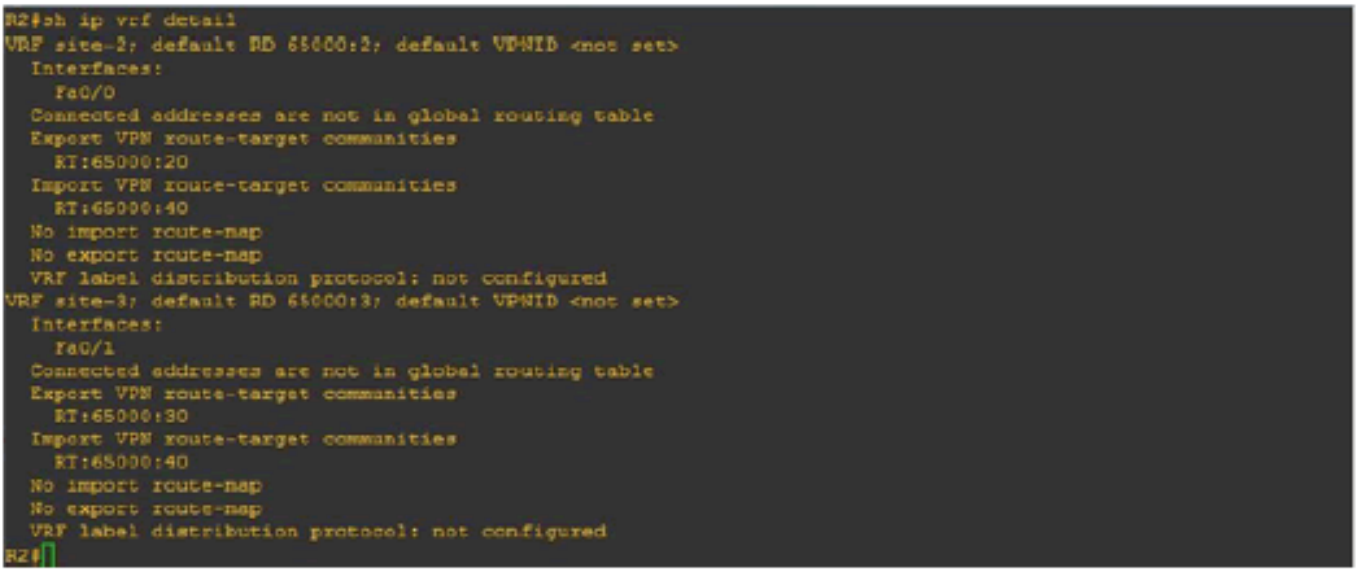



Figure 6 Create VRFs PE2.

## 7.3. Assign Interfaces to a specific VRF.

The IP addresses configured at the customer sites can be found using the command shown in Figure **7**

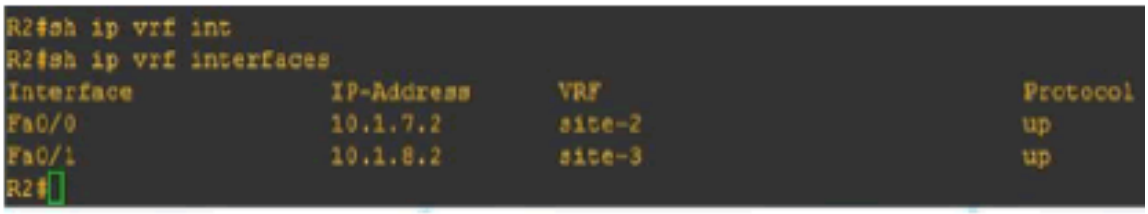



Figure 7 Assign Interface to VRF

## 7.4. No connectivity of customer network with ISP network

If a customer site wants to connect with a node in an ISP's network or vice versa, then this connectivity cannot be established because of the tunneling process. Customer sites are not exposed to public networks. In other words, all customer sites are hidden from an ISP network. This illustration can be seen in Figure 8.


Figure 8 No connectivity of customer network with ISP network

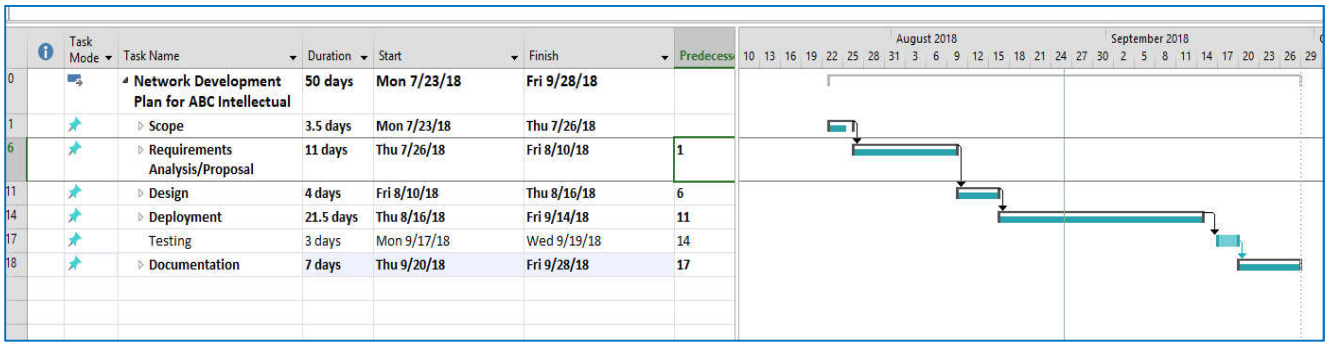
## 7.5. Connectivity of regional site-3

```
R7#
R7#traceroute 172.16.1.1

Type escape sequence to abort.
Tracing the route to 172.16.1.1

  1 10.1.7.2 16 msec 384 msec 172 msec
  2 192.168.3.2 [MPLS: Labels 16/22 Exp 0] 696 msec 456 msec 548 msec
  3 192.168.3.2 [MPLS: Labels 16/22 Exp 0] 524 msec 428 msec 748 msec
  4 172.16.1.2 [AS 65010] [MPLS: Label 22 Exp 0] 652 msec 784 msec 572 msec
  5 172.16.1.1 [AS 65010] 864 msec 1004 msec 900 msec
R7#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 656/785/948 ms
R7#ping 10.1.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.8.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R7#
```

Figure 9 Connectivity of regional site-3

## 8. Gantt chart

The following diagram shows the Gantt chart for the design and deployment of this project:



| | Task Mode | Task Name | Duration | Start | Finish | Predecess |
|---|---|---|---|---|---|---|
| 0 | | Network Development Plan for ABC Intellectual | 50 days | Mon 7/23/18 | Fri 9/28/18 | |
| 1 | | Scope | 3.5 days | Mon 7/23/18 | Thu 7/26/18 | |
| 6 | | Requirements Analysis/Proposal | 11 days | Thu 7/26/18 | Fri 8/10/18 | 1 |
| 11 | | Design | 4 days | Fri 8/10/18 | Thu 8/16/18 | 6 |
| 14 | | Deployment | 21.5 days | Thu 8/16/18 | Fri 9/14/18 | 11 |
| 17 | | Testing | 3 days | Mon 9/17/18 | Wed 9/19/18 | 14 |
| 18 | | Documentation | 7 days | Thu 9/20/18 | Fri 9/28/18 | 17 |



Figure 10 Gantt Chart

## 9. System Development Plan

The following diagram shows the System Development Plan. The bars show the length of each phase:

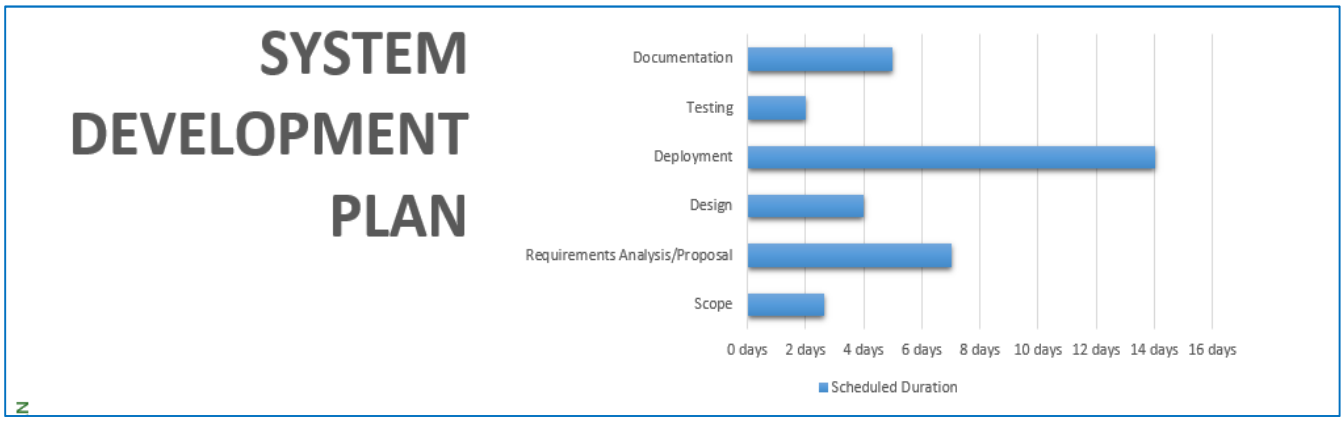



Figure 4 System Development Plan

## 10.Conclusion

In this report, we documented the design and deployment of a secure network for an office with an existing OSPF network. This report also explains the concept of MPLS protocol in depth. MPLS is an emerging technology and is a perfect solution to current IP network problems. It provides much better traffic engineering capability than the other networks. Introduction of labels provide an effective alternative and evades the need of large routing table lookups and results in fast routing. Also by the study of VPN, it can be concluded that MPLS VPN simplifies the network infrastructure by allowing the consolidation of multiple technologies and applications. From the above analysis, it can be seen that MPLS VPN is best among all other VPNs and it works best even in case of overlapping address spaces. The proposed system will provide enhanced security, scalability and high availability and will satisfy customer needs in better way.

In this project we configured many technologies such as VRFs on PE1 end PE2, enable the CEF, configure the label distribution protocol, MPLS etc.

## 11.References

1] Cicso, "MPLS based VPN," [Online]. Available: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13736-mplsospf.html. [Accessed 29 April 2019].

2] Amazon, "Amazon," Amazon.com: Cisco 2951 Integrated Services Router - CA4407 ..., N.D N.D N.D. [Online]. Available: https://www.amazon.com/Cisco-2951-Integrated-Services-Router/dp/B004S10D4K. [Accessed 28 April 2019].

3] Cisco, "Cisco 2951 Integrated Services Router," Cisco, N.D N.D N.D. [Online]. Available: http://www.cisco.com/c/en/us/products/routers/2951-integrated-services-router-isr/index.html. [Accessed 28 April 2019].