International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Implementation of MPLS L3VPN using GNS3

Akshay[1], Pooja Ahlawat[2]

[1]M.Tech. Student, Department of Computer Science & Engineering, R.N. College of Engineering & Management, Maharshi Dayanand University, Rohtak, Haryana, India

[2]Assistant Professor, Department of Computer Science & Engineering, R.N. College of Engineering & Management, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract: ***This paper gives the insight to implement MPLS L3VPN using GNS3. GNS3 is an alternative or complementary software tool to using real computer labs for computer network engineers, administrators. It can also be used to experiment features or to check configurations that need to be deployed later on real devices. GNS3 provides a graphical user interface to design and configure virtual networks, it runs on traditional PC hardware and may be used on multiple operating systems, including Windows, Linux, and Mac OS X.***

Keywords: MPLS, GNS3, L3VPN, Mac OS X.

1. Introduction to MPLS L3VPN

A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.

MPLS L3VPNs are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without customer involvement.

MPLS VPNs (L3VPNs) are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS L3VPN, only the edge router of the service provider that provides services to the customer site needs to be updated.

2. Types of MPLS L3VPN devices VPN Devices

There are two types of VPN devices: customer and provider network devices.

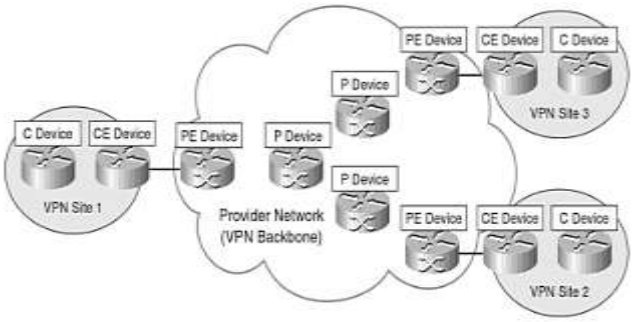


Figure 22: Customer and Provider Network Devices constituting VPN network

Devices in the customer network fall into one of the two categories:

(a) Customer (C) devices:
C devices are simply devices such as routers and switches located within the customer network. These devices do not have direct connectivity to the service provider network. C devices are not aware of the VPN.

(b) Customer Edge (CE) devices:
CE devices are located at the edge of the customer network and connect to the provider network (via Provider Edge [PE] devices).

Devices in the service provider network fall into one of the two categories:

(a) Service Provider (P) devices:
P devices are devices such as routers and switches within the provider network that do not directly connect to customer networks. P devices are unaware of customer VPNs.

(b) Service Provider Edge (PE) devices:
PE devices connect directly to customer networks via CE devices. PE devices are aware of VPN in PE-based VPNs, but are unaware of the VPN in CE-based VPNs.

The current layer 3 and layer 2 technologies makes it hard to fit MPLS within one layer of the OSI model. MPLS alone cannot be considered a layer in the OSI sense, since it does not have a unified format for the transport of data from the layer above: It uses a shim header over SONET or Ethernet; it uses the existing VPI/VCI of ATM. And so on. However, an individual MPLS function could be categorized as either an OSI layer 3 or layer 2 functions [2].

3. Advantages of MPLS L3VPNs

MPLS Layer 3 VPNs (L3VPNs) have a number of significant advantages for service providers (SP) and enterprises alike. These advantages include the following [1]:

(a) MPLS L3VPNs offers an extremely scalable VPN architecture that can scale to thousands of customer sites and VPNs.

(b) MPLS L3VPN s can be offered as a managed service by a service provider to enterprise customers, or

implemented by enterprises themselves to provide clear partition between units or services.

(c) MPLS L3VPNs allow an enterprise to simplify their WAN routing. Customer Edge (CE) routers need only peer with one or more Provider Edge (PE) routers rather than with all the other CE routers in the VPN.

(d) MPLS L3VPNs allow any-to-any connectivity for enterprise customer sites, and can be configured to support quality-of-service (QoS) for real-time and business applications.

(e) MPLS traffic engineering (associated technology) allows service providers to optimally utilize network bandwidth, and support tight service-level agreements (SLA) with fast failover (fast reroute) and guaranteed bandwidth.

4. Disadvantages of MPLS L3VPNs

Disadvantages of MPLS L3VPNs include the following [1]:

(a) MPLS L3VPNs natively support IP traffic transport only. If customers want to support other protocols such as IPX, Generic Routing Encapsulation (GRE) tunnels must be configured between CE routers.

(b) Some service providers do not support native IP multicast traffic transport between sites in MPLS L3VPNs. If a service provider does not offer native IP multicast transport, multicast traffic must be tunneled between customer sites by configuring GRE tunnels between CE routers.

(c) In MPLS L3VPN, the customer does not have complete control of their WAN IP routing. CE routers at the customer VPN sites do not establish direct routing adjacencies, but must instead peer with PE routers.

(d) MPLS L3VPNs are trusted VPNs, and although they offer similar traffic segregation and security to that offered by Frame Relay and ATM, they do not natively (by default) offer the strong authentication and encryption of secure VPNs such as IPsec. If authentication and encryption are required, however, it is possible to protect VPN traffic in transit between PE routers using either IPsec or end-to-end between CE devices.

5. Implementation of MPLS L3VPN using GNS3

The configuration of MPLS Layer 3 VPNs (L3VPNs) consists of three elements:

(a) The configuration of CE Routers
(b) The configuration of PE Routers
(c) The configuration of P Routers

The configuration of PE Routers:

A number of steps are associated with the configuration of PE routers:

(a) Configure a loopback interface for use as the PE Router's BGP router ID/LDP router ID.
(b) Configure the LDP.
(c) Enable MPLS on interfaces connected to other PE or P routers.
(d) Configure the backbone network IGP.
(e) Configure MP-BGP for VPN-IPv4 route exchange wih other PE routers or route reflectors.
(f) Configure the customer VRFs.
(g) Configure the customer VRF interfaces.
(h) Configure the customer VRF routing protocols or static routes.
(i) Redistribute the CE-PR routing protocol or static VRF roués into MPLS-BGP.

The Configuration of P Routers:

The configuration of P routers consists of a subset of the configuration of PE routers:

(a) Configure a loopback interface for use as the P Router's LDP router ID.
(b) Configure the LDP.
(c) Enable MPLS on interfaces connected to PE or other P routers.
(d) Configure the backbone network IGP.

Implementation of MPLS L3VPN Using GNS3

Requirements

Before starting the implementation of MPLS L3VPN using, the routers must achieve the minimum hardware and software requirement to support MPLS L3VPN.

(a) GNS3 Simulator to run and implement MPLS L3 VPN
(b) 4GB RAM, in minimum, installed in the PC/laptop running GNS3
(c) Cisco IOS Image to support MPLS features

Topology and Address Scheme

Using GNS3, a testbed consisting of 7200 and 3600 Series Cisco Routers was built to test the MPLS L3VPN.

I used "c7200-adventerprisek9-mz.152-4.S2.bin" IOS image which is compatible with Cisco 7200 Series Cisco Routers. In other words, the IOS for 7200 Series routers is c7200-adventerprisek9-mz.152-4.S2.bin.

I used "c3660-jsx-mz.123-4.T.bin" IOS image for 3600 Series CISCO Routers.

The MPLS L3VPN network to be implemented is designed and simulated by GNS3 is given as:

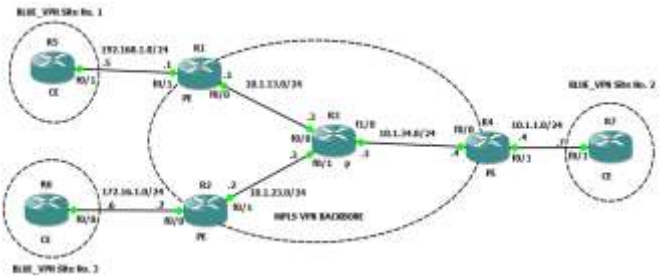


Figure 1: MPLS L3VPN Topology (Full-Mesh Topology) implemented using GNS3

There are four 7200 series Cisco Routers used, three act as PE routers which perform the MPLS L3VPN service, one P router.

There are three 3600 series acting as a CE routers connected directly with PE routers via Fast Ethernet ports. These CE routers are the part of same VPN (L3VPN) named

BLUE_VPN. All devices interfaces are Fast Ethernet set to "auto" duplex and "auto" speed.

The Open Shortest Path First (OSPF) routing protocol was used as the Interior Gateway Protocol (IGP). MP-BGP was used to carry VPNv4 routes as well as exchange VPNv4 labels. The static routing is used in between PE-CE connectivity.

Table 1: Address table

PE/P/CE	ROUTER	INTERFACE	IP ADDRESS	SUBNET
PE	R1	F0/0	10.1.13.1	255.255.255.0
		F0/1	192.168.1.1	255.255.255.0
	R2	F0/0	172.16.1.2	255.255.255.0
		F0/1	10.1.23.2	255.255.255.0
	R4	F0/0	10.1.34.4	255.255.255.0
		F0/1	10.1.1.4	255.255.255.0
P	R3	F0/0	10.1.13.3	255.255.255.0
		F0/1	10.1.23.3	255.255.255.0
		F1/0	10.1.34.3	255.255.255.0
CE	R5	F0/1	192.168.1.5	255.255.255.0
	R6	F0/0	1722.1.1.6	255.255.255.0
	R7	F0/1	10.1.1.7	255.255.255.0

Configuration of MPLS Routers

The configuration of MPLS L3VPN comes under following sections:

Configuration of PE Routers

(a) Configure a loopback interface for use as the PE router's BGP router ID (and update source)/LDP ID.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.255
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.255
R4#config t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#int lo0
R4(config-if)#ip add 4.4.4.4 255.255.255.255
```

(b) Configure LDP.

```
R1(config)#mpls label protocol ldp
R1(config)#mpls ldp router-id loopback 0
R2(config)#mpls label protocol ldp
R2(config)#mpls ldp router-id loopback 0
R4(config)#mpls label protocol ldp
R4(config)#mpls ldp router-id loopback 0
```

(c) Enable MPLS on interfaces connected to other PE or P routers

```
R1(config)#int FastEthernet0/0
R1(config-if)#mpls ip
R2(config)#int FastEthernet0/1
R2(config-if)#mpls ip
R4(config)#int FastEthernet0/0
R4(config-if)#mpls ip
```

(d) Configure the Backbone network IGP

```
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.13.0 0.0.0.255 area 0

 router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.23.0 0.0.0.255 area 0

 router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
 network 10.1.34.0 0.0.0.255 area 0
```

(e) Configure MP-BGP for VPNv4 Route Exchange with other PE Routers or Route Reflectors

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback0
 !
 address-family ipv4
 network 1.1.1.1 mask 255.255.255.255
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community both
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
 exit-address-family
 !
 address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community both
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
 exit-address-family

router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback0
 !
 address-family ipv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community both
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
 exit-address-family
 !
 address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community both
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community both
```

```
 exit-address-family

router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
 network 4.4.4.4 mask 255.255.255.255
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community both
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community both
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community both
 exit-address-family
```

(f) Configure the Customer VRFs and associated routing in BGP

```
ip vrf BLUE_VPN
 rd 100:12
 route-target export 100:12
 route-target import 100:12

address-family ipv4 vrf BLUE_VPN
 redistribute connected
 redistribute static
 exit-address-family
```

(g) Configuring the Customer VRF Interfaces

On R1:

```
interface FastEthernet0/1
 ip vrf forwarding BLUE_VPN
 ip address 192.168.1.1 255.255.255.0
 speed auto
 duplex auto
```

On R2:

```
interface FastEthernet0/0
 ip vrf forwarding BLUE_VPN
 ip address 172.16.1.2 255.255.255.0
 speed auto
 duplex auto
```

On R4:

```
interface FastEthernet0/1
 ip vrf forwarding BLUE_VPN
 ip address 10.1.1.4 255.255.255.0
 speed auto
 duplex auto
```

5.2.3.2 Configuration of P Routers

i. Configure a loopback interface for use as the P router's LDP Router ID

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.255
```

ii. Configure LDP

```
R3(config)#mpls label protocol ldp
R3(config)#mpls ldp router-id loopback 0
```

iii. Enable MPLS on interfaces connected to PE or P Routers

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int fastEthernet 0/0
R3(config-if)#mpls ip
R3(config)#int fastEthernet 0/1
R3(config-if)#mpls ip
R3(config)#int fastEthernet 1/0
R3(config-if)#mpls ip
```

iv. Configure the backbone network IGP

```
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 10.1.13.0 0.0.0.255 area 0
 network 10.1.23.0 0.0.0.255 area 0
 network 10.1.34.0 0.0.0.255 area 0
```

Configuration of CE Routers

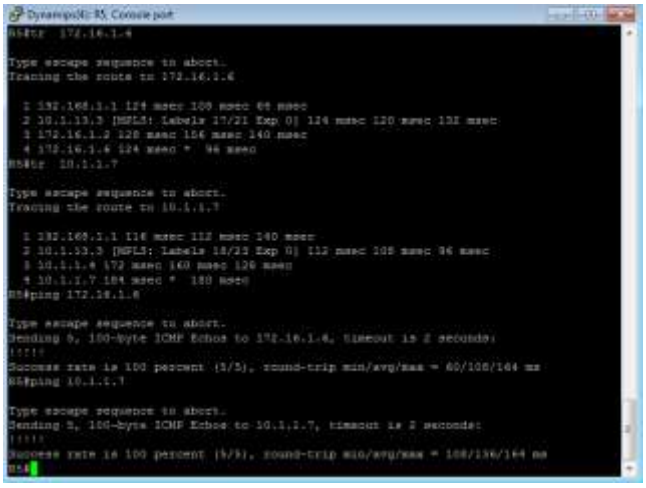
a) Configure the interface connected to PE router

```
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#int f0/1
R5(config-if)#no shut
R5(config-if)#ip add 192.168.1.5 255.255.255.0

R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#int f0/0
R6(config-if)#no shut
R6(config-if)#ip add 172.16.1.6 255.255.255.0

R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#int f0/1
R5(config-if)#no shut
R5(config-if)#ip add 10.1.1.7 255.255.255.0
```

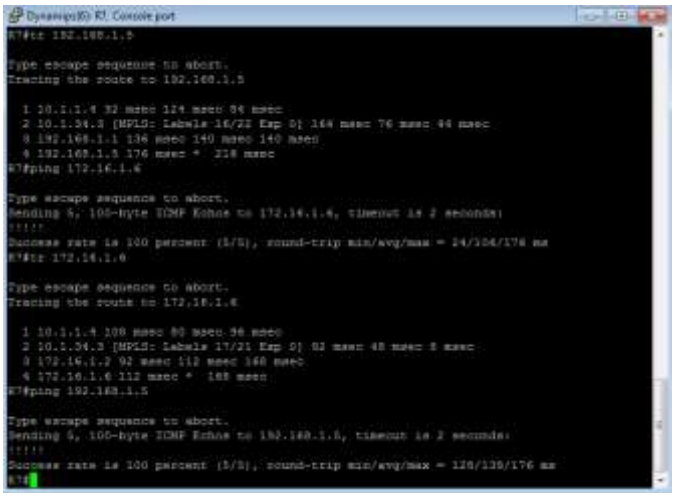
b) Configuring the default routing towards PE router connected to it.

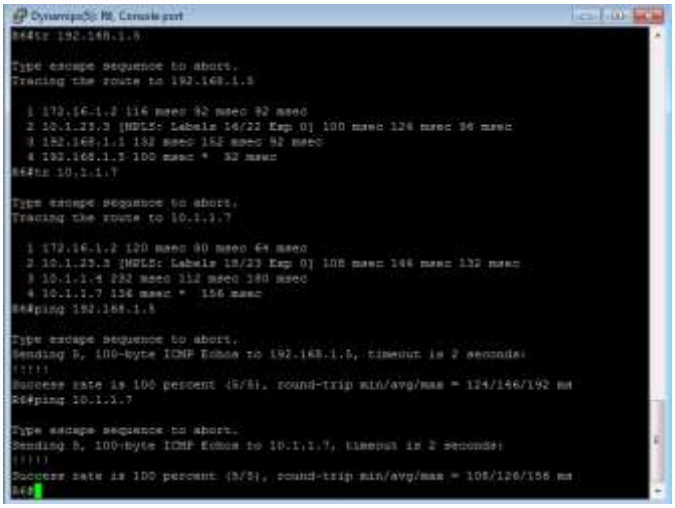
```
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

R6#config t
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2

R7#config t
Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.4
```

The connectivity of CE Router R5 to other CE routers, R6 and R7 is given as:



Alternatively,





6. Conclusion

The main goal of this paper was to implement the MPLS L3VPN using GNS3. I implemented MPLS L3VPN Full-Mesh Topology. In this topology, I had to create all possible MP-BGP to other PE routers. If the number of PE routers increases, the MP-BGP session to all PE routers also increases. Creating/Configuring more MP-BGP proves to be more hectic and time consuming, if PE routers increase in number. To decrease the MP-BGP session between all PE routers, we should implement the RR (Route Reflector) in the MPLS L3VPN network. This reduces the human efforts to create MP-BGP session.

References

[1] Mark Lewis, "Comparing, Designing and Deploying VPNs", Cisco Press.