Journal of Telecommunications System & Management

Ravi Kumar et al., J Telecommun Syst Manage 2017, 6:1
DOI: 10.4172/2167-0919.1000152

Research Article OMICS International

Architecture for MPLS L3 VPN Deployment in Service Provider Network

Ravi Kumar CV*, Dhanumjayulu C, Bagubali A and Bagadi KP

School of Electronics Engineering, VIT University, India

Abstract

Now a days in Service Provider's core network we do not use IP forwarding rather we go for MPLS because it gives more efficient switching of packets. MPLS is the combination of layer-3 routing and layer-2 switching because every network prefix is assigned a particular Label. In this paper I am going to do testing and implement scalability over MPLS L3 VPN. This testing and implementation are to proof the scalability is the one important thing when design MPLS L3 VPN technology.

This Topology of MPLS L3 VPN also provides the secure tunnel between two customer sites. By this implementation we show that there is a transparent tunneling over SP network. We are also avoiding the BGP implementation In SP core. So we call it as BGP free core. This implementation also saves the routing table space on provider routers. We have used the concept of Route Reflector (RR) to avoid more BGP sessions and to make it more scalable.

Keywords: Architecture; Communications; Virtual private networks; Topology

Abbreviations: SP: Service Provider; BGP: Border Gateway Protocol; MPLS: Multi Protocol Label Switching; VPN: Virtual Private Network; OSPF: Open Shortest Path First

Introduction

MPLS

In SP's core network labels are shared between routers using LDP. Label is associated with next-hop IP address. First router will tell the path to follow. All packets that enter the MPLS network get a label depending on is used for incoming unlabeled packets where the router matches the packet's destination IP address to the best prefix in the FIB and forwards the packet base on that entry. The LFIB is used for incoming labeled packets. In this case, the router compares the label in the incoming packet to the list of labels in the LFIB and forwards the packet based on that LFIB entry [1].

VPN

Network connection between devices that do not literally share a physical cable is called VPN. VPN (Virtual Private Network) is simply a way of using a public network for private communications, among a set of users and/or sites [1].

Remote access

Most common form of VPN is dial-up remote access to corporate database-for example, road warriors connecting from laptops.

Site-to-site: Connecting two local networks (may be with authentication and encryption)-for example, a Service Provider connecting two sites of the same company over its shared network.

MPLS VPN uses the power of multiprotocol label switching (MPLS) to create virtual private networks (VPNs). MPLS based Layer 3 virtual private networks (VPNs) allows us to securely connect geographically diverse sites across an MPLS network. MPLS services can be used to connect various sites to a backbone network and to ensure better performance for low-latency applications such as voice over IP (VoIP) and other business-critical functions. Layer 3 VPN utilizes layer 3 VRF (VPN/virtual routing and forwarding) to segment routing tables for each "customer" utilizing the service. The customer router peers with the service provider edge (PE) router and the two exchange routes, which are then placed into a routing table specific to that customer. MP-BGP (Multiprotocol BGP) is required in the cloud to exchange the VPNv4 routes [2].

Topology

This is the topological implementation of MPLS L3 VPN in GNS3. In the Figure 1 topology we have 4 PE's, 2 P's and 7 CE's. We have made one of the PE as Route Reflector to avoid more iBGP sessions. In the topology we have 3 cisco sites, 2 Google sites and 2 VIT sites. Cisco sites are exchanging their routes with other cisco sites but not with any other company sites.

Requisites for Running MPLS L3 VPNs

Basic IP reachability, IGP running, Cisco Express Forwarding (CEF), MPLS, Label Distribution Protocol (LDP), BGP VPNv4 session between the PEs.

VRFs

By creating VRFs we ensure that a virtual router is created inside IOS which has its own routing table. And that routing table is different than global routing table. Whenever we want to differentiate between routes of two companies like in this topology I have 3 Cisco sites 2 Google sites and 2 VIT sites so all can use same Private IP addresses space but they are differentiated by using Route distinguisher which is the characteristics of VRF. While configuring VRF in IOS we have to specify route distinguisher and then Route Targets which are extended communities.

MPLS L3 VPN

It is the best of both worlds from overlay VPNs and peer to peer VPNs. In MPLS L3 VPN no static provisioning is required. Whenever

***Corresponding author:** Ravi Kumar CV, School of Electronics Engineering, VIT University, India, Tel: 9751282729; E-mail: ravikumar.cv@vit.ac.in

Received March 24, 2017; **Accepted** March 31, 2017; **Published** April 11, 2017

Citation: Ravi Kumar CV, Dhanumjayulu C, Bagubali A, Bagadi KP (2017) Architecture for MPLS L3 VPN Deployment in Service Provider Network. J Telecommun Syst Manage 6: 152. doi: 10.4172/2167-0919.1000152

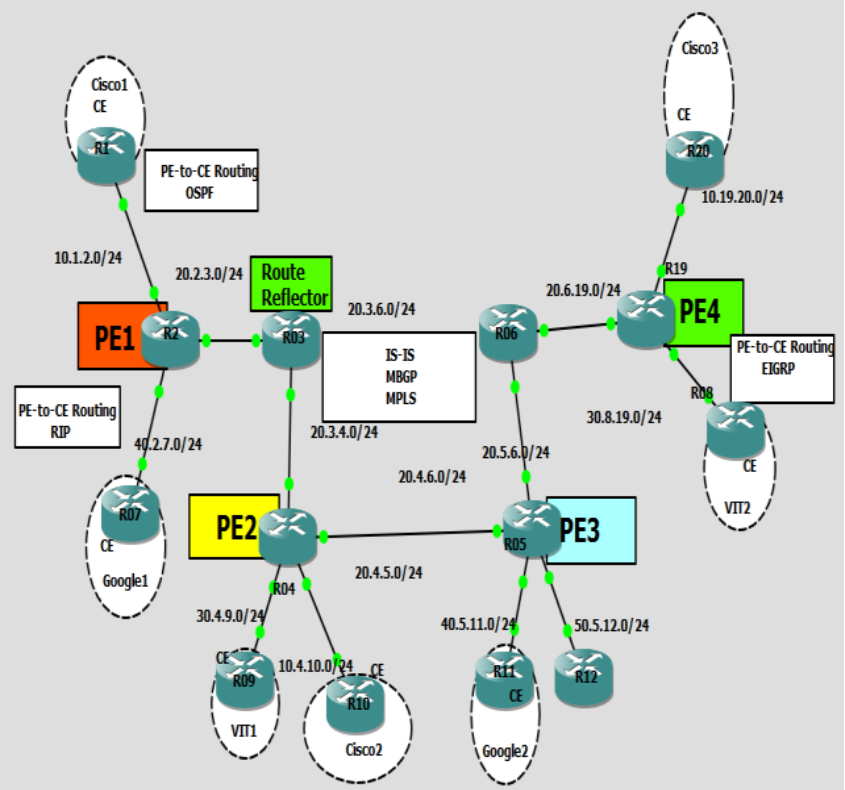

Figure 1: MPLS L3 VPN GNS3 topology.

we want to add new sites we can add very easily without reconfiguring other existing sites. In MPLS VPN Service provider keeps separate routing tables per customer. It gives flexibility in customer addressing. In MPLS L3 VPN manual route and ACL filtering is not required in Service Providers. Customers can use default routing as needed [3].

How MPLS L3 VPN works

MPLS L3 VPN has two basic components. Separation of customer routing information.

- VRF - Virtual routing and forwarding instance.
- Different customers have different "Virtual routing tables".
- IGP/BGP run inside the VRF between the customer and SP.

Exchange of customer's routing information inside SP.

- It uses Multi-Protocol BGP through the SP network to share customer's route.
- Traffic destined for customer is label switched towards BGP next hop.

VPN Route Distribution-Route Targets.

- "Export" Route Target: Every VPN route is tagged with one or more route targets when it is exported from a VRF (to be offered to other VRFs).
- "Import" Route Target: A set of routes targets can be associated with a VRF, and all routes tagged with at least one of those route targets will be inserted into the VRF.

Transport label vs. VPN label

L3VPN needs at least 2 labels to deliver traffic can be more with applications like MPLS TE, FRR etc.

Transport label: It tells the SP core routers which PE Traffic is destined to. It is derived from LDP or we can say that it is the MPLS label which is swapped in MPLS core network. It is also called the IGP label.

VPN label: This label is below the MPLS label so it is exposed to PE routers only and based on these label PE routers can know which CE the traffic should go [4].

Controlling VPNv4 routes: Route distinguisher is used to make route unique. Rd allows for overlapping IPv4 addresses between customers. BGP extended community "route-target" is used to control what enters/exits into VRF table. "Export" route-target-what routes will go from VRF into BGP. "Import" route-target-what routes will go from BGP into VRF. These route-targets allow us to control what sites have what routes.

Configurations

VRF configurations on R2

Here in configuration we can see we have two VRFs, one is for cisco customers and one for Google customers and for these VRFs we have route-targets defined. Routes are being redistributed from BGP to VRF so that one site of company can get access to another (Figure 2).

MBGP configuration on R2

As mentioned before MBGP is used to share VPnv4 routes (Figure 3).

```
R2#sh run | s vrf
ip vrf cisco1
 rd 2.2.2.2:1
 route-target export 100:1
 route-target import 100:2
 route-target import 100:1
ip vrf google1
 rd 2.2.2.2:2
 route-target export 100:4
 route-target import 100:3
 ip vrf forwarding cisco1
 ip vrf forwarding google1
router ospf 1 vrf cisco1
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 10.0.0.0 0.255.255.255 area 0
 address-family ipv4 vrf google1
 address-family ipv4 vrf google1
 address-family ipv4 vrf cisco1
 redistribute ospf 1 vrf cisco1
```

Figure 2: VRF configurations on R2.

```
R2#sh run | s router bgp
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf google1
 redistribute rip
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf cisco1
 redistribute ospf 1 vrf cisco1
 no synchronization
 exit-address-family
```

Figure 3: MBGP configuration on R2.

Route-reflector configurations on R3

Route-Reflector is used for scalability purpose because when you have more PEs you can't establish sessions with all the PEs so to avoid this we have Route-Reflector so that each and every PE can establish iBGP session only VRF aware OSPF is used for PE-to-CE routing RR (Figure 4).

PE-to-CE routing configuration with VRF

Details mentioned in Figure 5.

Verification

Son R20 we have loopback0 with address 20.20.20.20/32 which is in vrf cisco1 so need to get this route to R1 which is also in same VRF (Figure 6).

As we can see 20.20.20.20/32 is highlighted in R1's routing table. Connectivity check between R1 and R20: I have initiated ping from R1's Loopback0 to R20's Loopback 0 which is 20.20.20.20/32 (Table 1 and Figure 7).

As we see in Table 1 when we sent first set of packets it is taking more time because first the destination is not available in CEF table so it builds when we first try to reach any destination and then uses that to forward packets so it take less time [5].

```
R03#sh run | s rou
R03#sh run | s router bgp
router bgp 100
 no bgp default ipv4-unicast
 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
 neighbor 5.5.5.5 remote-as 100
 neighbor 5.5.5.5 update-source Loopback0
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 neighbor 2.2.2.2 route-reflector-client
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 neighbor 4.4.4.4 route-reflector-client
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
 neighbor 5.5.5.5 route-reflector-client
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
 neighbor 19.19.19.19 route-reflector-client
 exit-address-family
```

Figure 4: Route-reflector configurations on R3.

```
R2#sh run | s router ospf
router ospf 1 vrf cisco1
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 10.0.0.0 0.255.255.255 area 0
```

Figure 5: PE-to-CE routing configuration with VRF.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     20.0.0.0/32 is subnetted, 1 subnets
O E2    20.20.20.20 [110/2] via 10.1.2.2, 00:01:58, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA    10.10.10.10/32 [110/3] via 10.1.2.2, 00:02:03, FastEthernet0/0
O IA    10.4.10.0/24 [110/2] via 10.1.2.2, 00:02:03, FastEthernet0/0
C       10.1.2.0/24 is directly connected, FastEthernet0/0
O E2    10.19.20.0/24 [110/1] via 10.1.2.2, 00:01:58, FastEthernet0/0
```

Figure 6: R1's routing table.

Testing Best Practices

Using RR for scaling BGP-Deploy RRs in pair for the redundancy. Keep RRs out of the forwarding paths and disable CEF (it saves memory).

Choose AS format for RT and RD i.e., ASN: X Reserve first few 100s of X for the internal purposes such as filtering.

Don't use customer names as the VRF names; difficult for NOC. Consider A101, A102, A201 etc. and use description for naming.

Consider unique RD per VRF per PE.

Source IP	Destination IP	No of packets	Min time	Avg time	Max time
1.1.1.1	20.20.20.20	10	232 ms	290 ms	404 ms
1.1.1.1	20.20.20.20	100	176 ms	246 ms	376
1.1.1.1	20.20.20.20	1000	140 ms	246 ms	376 ms

Table 1: R1's routing table.

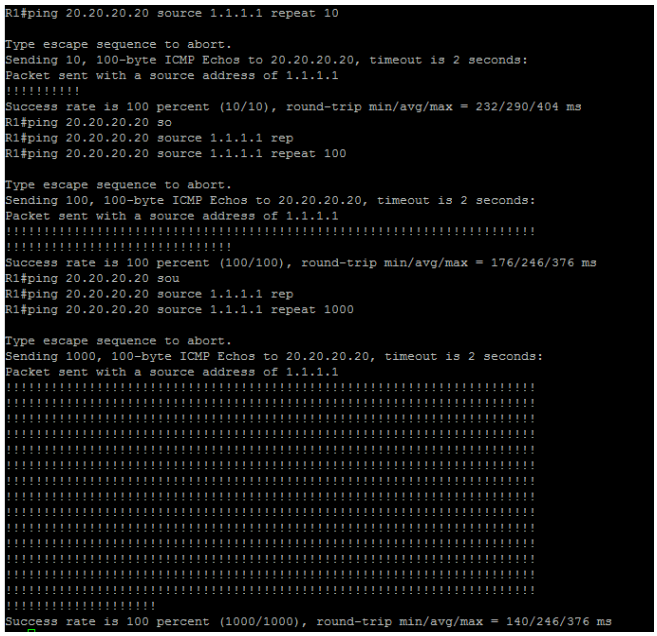

Figure 7: Connectivity check between R1 and R20.

Limit the number of prefixes per-VRF and/or per-neighbor on PE.

Utilize SP's public address space for PE-CE IP addressing.

Conclusion

Using this model of MPLS L3 VPN we can deploy a small size service provider network and scale it to a bigger. In this topology we have shown how to deploy a service provider network. For future work this topology can be taken as reference to deploy all kind of SP network and we have included some important configuration also those will help audience to understand the topology and network very easily. While deploying network in future people might need to configure on different platform but the basic of MPLS L3 VPN remains same and the scalability measures will remain same so you can adopt this method of deploying of SP network.

Acknowledgement

First of all I wish to give my gratitude to prof. Kala Praveen Bagadi who guided me to complete this paper and helped me a lot while configuring and testing this network. Secondly I would like to thank my colleagues who helped me and guided me all the way till the completion of this paper..

References

1. Pan J, Wang YH, Zhang K (2002) MPLS/VPN Technology Principle and Realization.
2. http://www.wtn.net/summit2010/
3. Introduction to Cisco MPLS VPN Technology.
4. Ravi Kumar CV, Bagadi KP (2016) Robust Neural Network based multiuser detector in MC-CDMA for multiple access interference mitigation. Indian Journal of Science And Technology 9: 1-7.
5. Ravi Kumar CV, Bagadi KP (2016) Performance analysis in layer3 gateway redundancy for corporate networks. Indian Journal of Science and Technology 9: 1-5.

Citation: Ravi Kumar CV, Dhanumjayulu C, Bagubali A, Bagadi KP (2017) Architecture for MPLS L3 VPN Deployment in Service Provider Network. J Telecommun Syst Manage 6: 152. doi: 10.4172/2167-0919.1000152