ISSN (online): 2320-9836
ISSN (Print): 2320-9828

Carrier Supporting Carrier – requirements and deployment

Merline Johndoss, T. Pramananda Perumal

Presidency College, Kamarajar Salai, Triplicane, Chennai-600 005, Tamil Nadu, India
merlinjohndoss@gmail.com, pramanandaperumal@yahoo.com

Abstract

Objectives: Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. Carrier Supporting Carrier (CSC) is implemented in circumstances in which one service provider needs to use the transport services provided by another service provider. The service provider providing the transport is called the backbone carrier and the service provider using the services provided by the backbone carrier is called a customer carrier. The customer carrier can either be an ISP provider or an MPLS VPN service provider. In my study, I have taken the case of the carrier customer is a service provider running MPLS VPN.
Methods/Analysis: In this project, we are giving interconnection between customer branches of ISP1. The POP locations of ISP1 are running with MPLS and ISP1 POP locations are interconnected via other ISP Backbone carrier ISP2 using MPLS network. Customers connected in POP sites 1 and POP sites 2 to ISP1, are using BGP protocol to send the network information to ISP1 in their respective location. ISP1 is also running BGP, collecting the information of Customers from both the POP sites using BGP protocol and sharing this information from POP1 site to POP2 site via backbone carrier ISP2.
Application: Backbone carrier ISP2 creates an MPLS link with both POP sites of ISP1 and carries customer network information via ISP2 network such that both the customer branches can share data across POP locations.
Results: The above network was simulated using GNS3 network simulation tools and the reach ability between the two customer sites of ISP2 the customer carrier was tested, with success.
***Keywords**:* MPLS Technology, VPN, Carrier Supporting Carriers, MPLS VPN, Private networks, MPLS VPN, VPN implementation, Service provider.

1. Introduction

A small service provider intends to connect its customers who are geographically apart. The service provider does not have direct connectivity between the locations. Normally internet is available in all the locations. But connecting the customer sites through internet has its own drawbacks. Internet is not very secure. The end customers want very secure, fast and scalable network connectivity. To fulfil the requirements of the end customers, internet may not be a workable solution. Also, if the user wants to have private IP connectivity, connecting through internet is not directly possible.

MPLS technology can be used to overcome the above. So the service provider takes the help of another bigger service provider, providing MPLS VPN network and has its presence in the geographically apart locations. Deployments of Multiprotocol Label Switching (MPLS) have become routine in large-scale global networks, which demand solutions to complex business and network problems. There are two primary components of the MPLS Inter-Domain Solution: Inter-AS and Carrier Supporting Carrier.

Inter-AS is a peer-to-peer type model that allows extension of VPNs through multiple provider or multi-domain networks. This solution enables Service Providers to peer up with one another and offer end-to-end VPN connectivity over extended geographical locations for those subscribers who may be out of reach for a single provider.

Carrier Supporting Carrier (CSC) is a hierarchical VPN model that allows small Service Providers, or customer carriers, to interconnect their IP or MPLS networks over an MPLS backbone. This eliminates the need for customer carriers to build and maintain their own MPLS backbone. Both Inter-AS and CSC can construct scalable networks that help maintain network segmentation based on internal organizational or operational boundaries.

2. Virtual private networks

A VPN is a network that emulates a private network over a common infrastructure. The private network requires that all customer sites are able to interconnect and are completely separate from other VPNs. In traditional router based networks; different sites belonging to the same customer were connected to each other using dedicated point-to-point links. A full mesh of connected sites would consequently imply an exponential increase in the cost associated. Frame Relay and ATM were the first technologies widely adopted to implement VPNs. These networks consisted of various devices, belonging to either the customer or the service provider, that were components of the VPN solution. Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following overlay model, peer-to-peer model. Overlay VPNs were initially implemented by the Service Provider by providing either Layer 1 (physical layer) connectivity or a Layer 2 transport circuit between customer sites. In the Layer 1 implementation, the service provider would provide physical layer connectivity between customer sites, and the customer was responsible for all other layers. In the Layer 2 implementation the Service Provider was responsible for transportation of Layer 2 frames (or cells) between customer sites, which was traditionally implemented using either frame relay or ATM switches as provider edge devices.

The peer-to-peer model was developed to overcome the drawbacks of the Overlay model and provide customers with optimal data transport via the service provider backbone. Hence, the service provider would actively participate in customer routing. In the peer-to-peer model, routing information is exchanged between the customer routers and the service provider routers, and customer data is transported across the service provider's core, optimally. Customer routing information is carried between routers in the provider network and customer network the peer-to-peer model, consequently, does not require the creation of virtual circuits.

3. Multi Protocol Label Switching – MPLS

Multiprotocol Label Switching (MPLS) [1] is a networking technology that uses labels attached to packets to forward them through the network. 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. The benefits of MPLS are, the use of one unified network infrastructure, better IP over ATM integration, Core network is BGP free, optimal traffic flow, peer-to-peer model for MPLS VPN, and traffic engineering. MPLS technology gives the customers the advantages of QoS.

4. MPLS VPN

MPLS VPNs [2] and [1] are made possible because the service provider runs MPLS in the backbone network, which supplies a decoupling of forwarding plane and control plane that IP does not. The privateness in MPLS VPN networks is achieved by using the concept of virtual routing/forwarding (VRF) and the data is forwarded in the backbone as labelled packets. The VRFs ensure that the routing information from the different customers is kept separate, and the MPLS in the backbone ensures that the packets are forwarding based on the label information and not the information in the IP header. MPLS VPN is more secure than IP VPN. The security threats of intrusions, DOS attacks are not possible in MPLS VPN.

5. Carrier Supporting Carrier network

Carrier Supporting Carriers (CSC) [3] is implemented in circumstances in which one service provider needs to use the transport services provided by another service provider. The service provider providing the transport is called the backbone carrier and the service provider using the services provided by the backbone carrier is called a customer carrier. The customer carrier can either be an ISP provider or an MPLS VPN service provider. Carrier Supporting Carrier (CSC), Carrier’s Carrier or Hierarchical MPLS is an architecture designed to expand the MPLS core in a hierarchical way. CSC defines a hierarchical architecture that is very similar to Tier levels in ISP architectures. If a SP has no extended coverage on a wide geographical area needs to purchase transport services from another SP.

5.1. Benefits of implementing Carrier Supporting Carrier network

CSC is where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

The backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier is not running MPLS in its network.

1. Benefits to the backbone carrier [4]

1. The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.
2. The MPLS VPN Carrier Supporting Carrier feature is scalable. Carrier Supporting Carrier can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The Carrier Supporting Carrier feature enables tens of thousands of VPNs to be set up over the same network and it allows the customer carrier to provide services.
3. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

2. Benefits to customer carriers [4]

1. The MPLS VPN Carrier Supporting Carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network, of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
2. Customer carriers who use the VPN services provided by the backbone carrier receives the same level of security that Frame relay or ATM based VPNs provide. Customer carriers can also sue IP sec in their VPNs for a higher level of security it is completely transparent to the backbone carrier.
3. Customer carriers can use any link layer technology SONET, DSL, Frame Relay and so on to connect the CE routers to the PE routers and PE routers to the P routers. The MPLS VPN Carrier Supporting Carrier feature is link layer independent. The CE routers and PE router use IP to communicate, and backbone carrier uses MPLS.
4. The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

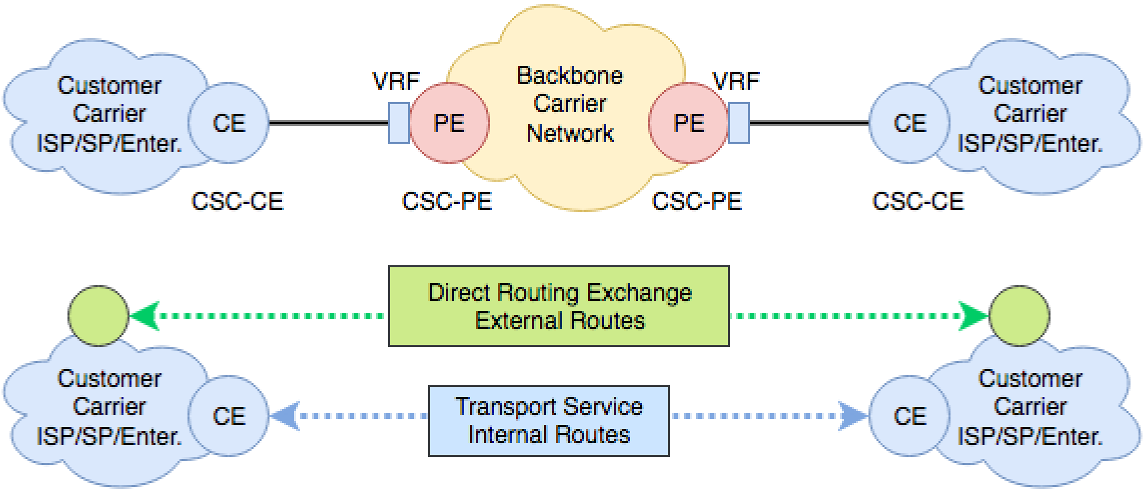
5.2. Architecture

The CSC architecture defines the following elements.

1. Backbone carrier
2. Customer carrier
3. CSC-CE: CE located in the customer carrier
4. CSC-PE: PE located in the backbone SP and carries customer SP routes (internal routes)
5. PE: PE located in the customer carrier and carries customer routes (external routes or
6. VPN routes)
7. RR: route reflectors located at the customer carrier

The Backbone Carrier joins Customer Carrier isolated locations. In case the Customer Carrier runs MPLS, transporting internal routes between sites allows for end-to-end LSPs between Customer Carrier sites. Once the LSP continuity is assured, VPN services (in case of Hierarchical VPN) can easily be extended between Customer Sites. The Backbone carrier is agnostic to the direct routing exchange of external routing information (VPN routing).

Figure 1. CSC Architecture


Customer Carrier ISP/SP/Enter.
CE
VRF
PE
Backbone Carrier Network
PE
VRF
CE
Customer Carrier ISP/SP/Enter.
CSC-CE
CSC-PE
CSC-PE
CSC-CE
Direct Routing Exchange External Routes
Transport Service Internal Routes
Customer Carrier ISP/SP/Enter.
CE
CE
Customer Carrier ISP/SP/Enter.

6. CSC deployment

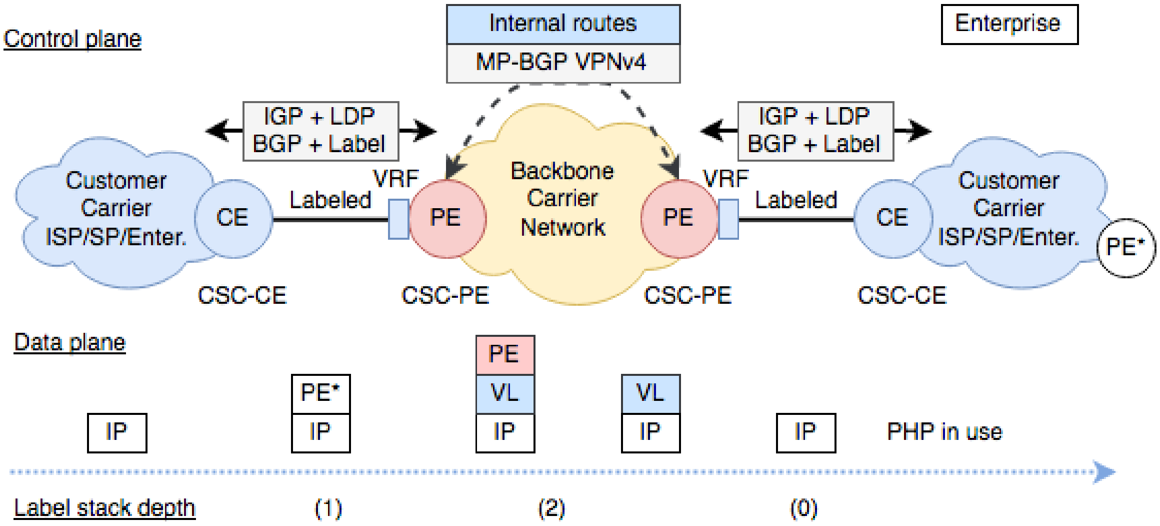
6.1. Label exchange methods in CSC

There are two ways of exchanging labels in MPLS VPN Network.

1. Using IGP for label exchange – LDP protocol.
2. Using BGP for label exchange – MPLS BGP forwarding

The protocols used in exchanging labels are given in Figure 2.

Figure 2. CSC protocols



The backbone carrier will transport internal routes between sites, allowing IP connectivity. If no further routing exchange is performed, the VRFs in the CSC-PE store all the exchanged routes as in the MPLS L3 VPN service.

6.2. Deployment scenarios with CSC [3]

Three deployment scenarios are possible with CSC architecture.

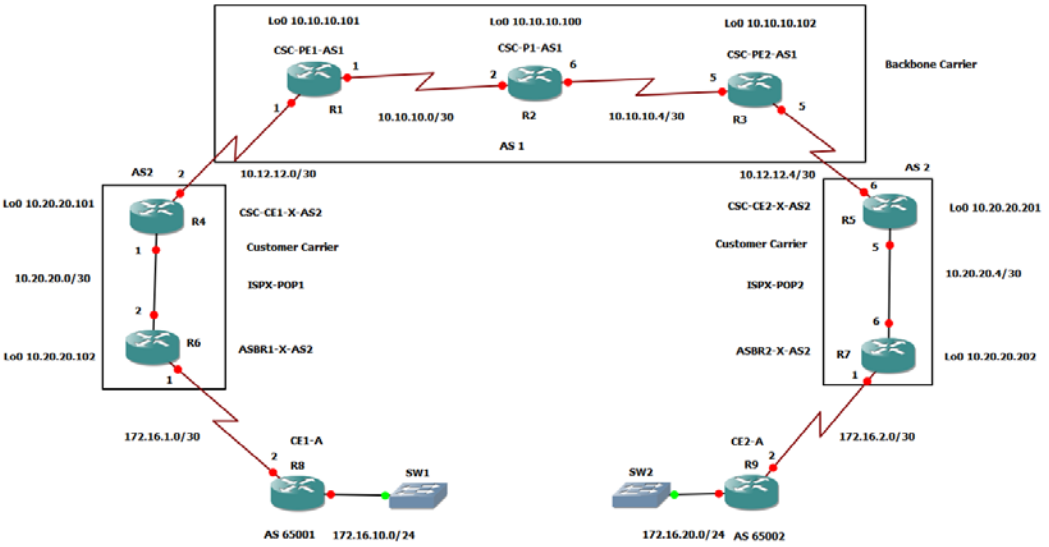
1. Customer carrier is not running MPLS inside its POP sites
2. Customer carrier is running MPLS inside its POP sites
3. Customer carrier is providing MPLS VPN services to user sites.

In this project, the third scenario where the customer carrier is not running MPLS inside its POP sites and transporting only IP traffic of its customers is deployed, using GNS3 simulation and the result tested. The network topology used to simulate is given below in Figure 3.

Let us consider that the customer carrier has two sitesCE1-A and another CE2-A.

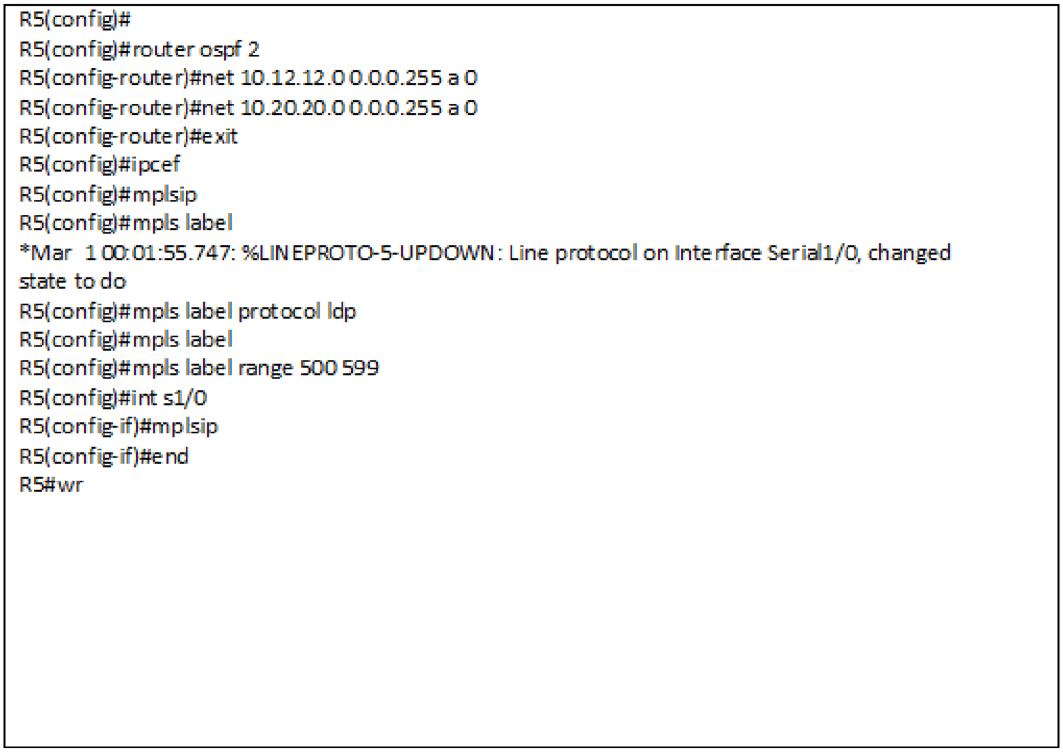
Each site is a point of presence for the customer carrier.

Figure 3. The GNS3 simulated network topology



In this topology, the backbone carrier uses MPLS VPN. The customer carrier also runs MPLS VPN. As a result, the backbone carrier must carry all the external routes of the customer carrier. To do so, the backbone carrier is configured with.

Figure 4. Router configuration of R5

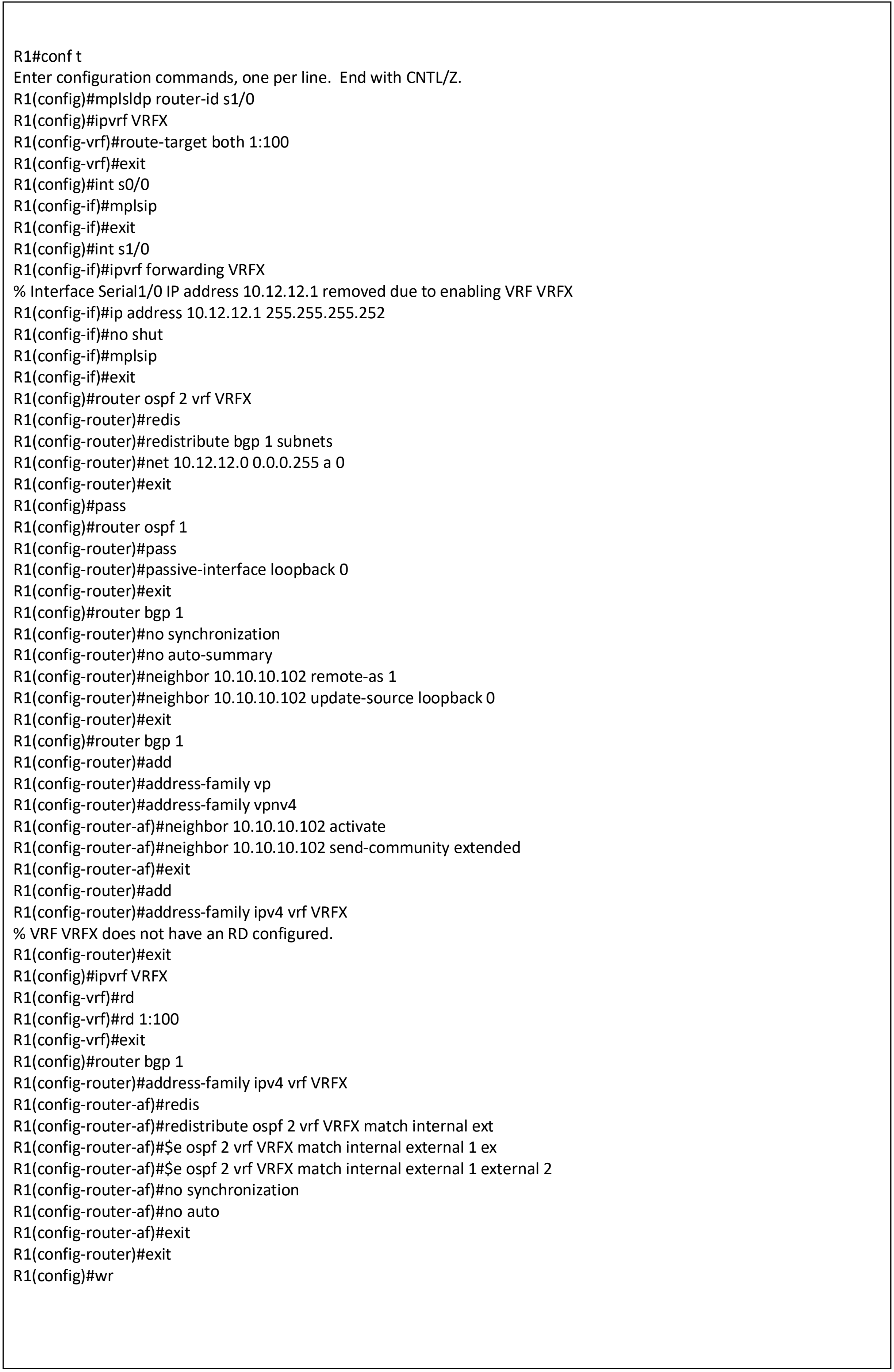


```
R5(config)#
R5(config)#router ospf 2
R5(config-router)#net 10.12.12.0 0.0.0.255 a 0
R5(config-router)#net 10.20.20.0 0.0.0.255 a 0
R5(config-router)#exit
R5(config)#ipcef
R5(config)#mplsip
R5(config)#mpls label
*Mar  1 00:01:55.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed
state to do
R5(config)#mpls label protocol ldp
R5(config)#mpls label
R5(config)#mpls label range 500 599
R5(config)#int s1/0
R5(config-if)#mplsip
R5(config-if)#end
R5#wr
```

1. The backbone carrier allows only internal routes of customer carrier’s IGP routes, between CE1 and PE1, and CE2 and PE2 [4].
2. MPLS is enabled in the interfaces between CE1 and PE1 and CE2 and PE2.

The configuration of customer carrier route is given in Figure 4. The running configuration of Backbone carrier router is given in Figure 5.

Figure 5. Router configuration of R1



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#mplsldp router-id s1/0
R1(config)#ipvrf VRFX
R1(config-vrf)#route-target both 1:100
R1(config-vrf)#exit
R1(config)#int s0/0
R1(config-if)#mplsip
R1(config-if)#exit
R1(config)#int s1/0
R1(config-if)#ipvrf forwarding VRFX
% Interface Serial1/0 IP address 10.12.12.1 removed due to enabling VRF VRFX
R1(config-if)#ip address 10.12.12.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#mplsip
R1(config-if)#exit
R1(config)#router ospf 2 vrf VRFX
R1(config-router)#redis
R1(config-router)#redistribute bgp 1 subnets
R1(config-router)#net 10.12.12.0 0.0.0.255 a 0
R1(config-router)#exit
R1(config)#pass
R1(config)#router ospf 1
R1(config-router)#pass
R1(config-router)#passive-interface loopback 0
R1(config-router)#exit
R1(config)#router bgp 1
R1(config-router)#no synchronization
R1(config-router)#no auto-summary
R1(config-router)#neighbor 10.10.10.102 remote-as 1
R1(config-router)#neighbor 10.10.10.102 update-source loopback 0
R1(config-router)#exit
R1(config)#router bgp 1
R1(config-router)#add
R1(config-router)#address-family vp
R1(config-router)#address-family vpnv4
R1(config-router-af)#neighbor 10.10.10.102 activate
R1(config-router-af)#neighbor 10.10.10.102 send-community extended
R1(config-router-af)#exit
R1(config-router)#add
R1(config-router)#address-family ipv4 vrf VRFX
% VRF VRFX does not have an RD configured.
R1(config-router)#exit
R1(config)#ipvrf VRFX
R1(config-vrf)#rd
R1(config-vrf)#rd 1:100
R1(config-vrf)#exit
R1(config)#router bgp 1
R1(config-router)#address-family ipv4 vrf VRFX
R1(config-router-af)#redis
R1(config-router-af)#redistribute ospf 2 vrf VRFX match internal ext
R1(config-router-af)#$e ospf 2 vrf VRFX match internal external 1 ex
R1(config-router-af)#$e ospf 2 vrf VRFX match internal external 1 external 2
R1(config-router-af)#no synchronization
R1(config-router-af)#no auto
R1(config-router-af)#exit
R1(config-router)#exit
R1(config)#wr
```

7. Results

The above topology was configured in the GNS3 simulator and the reach ability from customer site CE1-A to CE1-B and vice versa was tested.

8. Conclusion

CSC deployment has helped in scalability of networks with the already available backbone. Building a customer oriented network is cheaper for smaller service providers. With the exponential growth of global networks, and global reach ability of users, CSC is being implemented with several service providers. Not only for service providers some Government organisations are also using this technology to connect their offices geographically apart, as this is a secured and scalable solution to build their network.

9. References

1. MPLS Fundamentals, Luc De Ghein, CCIE, 2nd Edition. 2007.
2. https://tools.ietf.org/html/rfc4364. Date accessed: 02/2018.
3. https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fscsc23.html. Date accessed: 01/2018.
4. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ias_and_csc/configuration/xe-16/mp-ias-and-csc-xe-16-book/mpls-vpn-carrier-supporting-carrier-using-ldp-and-an-igp.pdf. Date accessed: 02/2018.

The Publication fee is defrayed by Indian Society for Education and Environment (www.iseeadyar.org)
Cite this article as:
Merline Johndoss, T. Pramananda Perumal. Carrier Supporting Carrier – requirements and deployment. *Indian Journal of Economics and Development.* Vol 6 (3), March 2018.