Advance Routing

FINAL PROYECT – MPLS

Luis Carlos Leaño Martin – 744732

Diego Gutiérrez Aldrete – 745359

ITESO, Universidad Jesuita de Guadalajara

November 28 of 2024

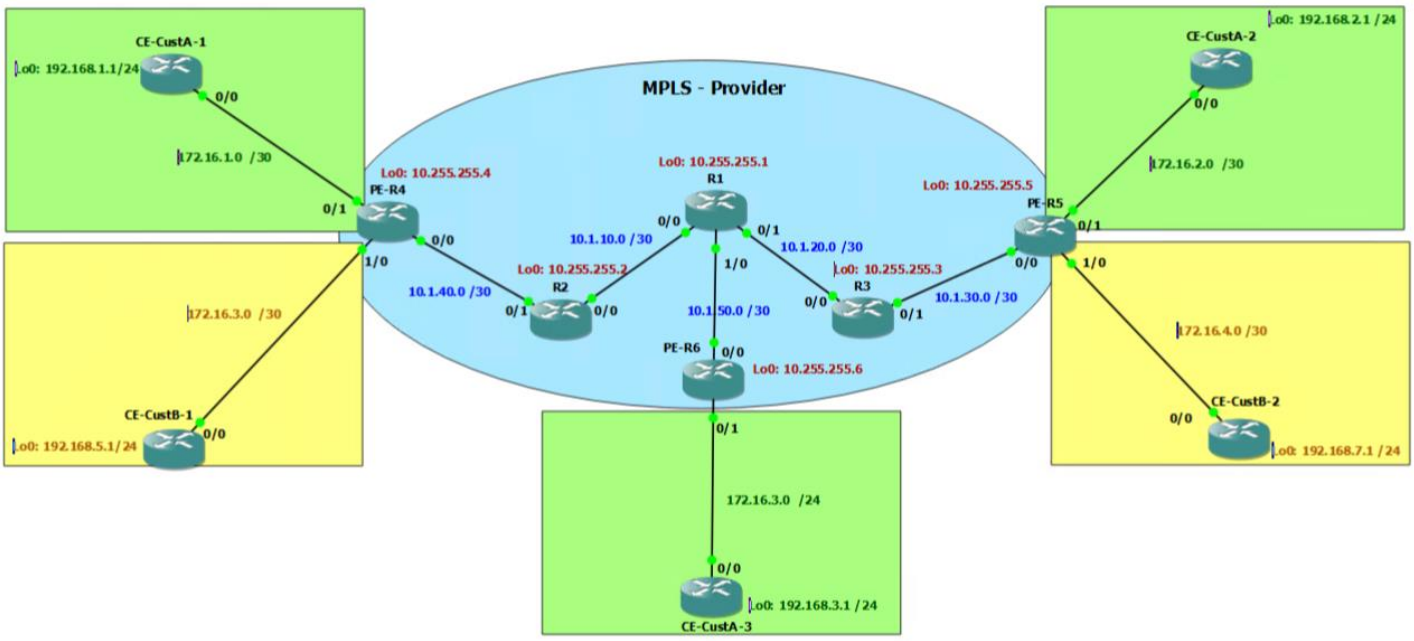
INTRODUCTION

Multiprotocol Label Switching (MPLS) represents a fundamental label switching technology in modern telecommunications networks, designed to optimize performance and routing efficiency across multi-protocol networks. Its operation is based on a labeling mechanism that enables predefined routes and packet switching more rapidly and precisely than traditional routing methods.

Labeling in MPLS is a process by which each packet receives a short numerical label indicating its forwarding route, allowing routers to make forwarding decisions based on these labels instead of performing complex IP header analysis. This method significantly reduces processing overhead and improves data transmission speed.

Virtual Private Networks (VPNs) implemented over MPLS, specifically Virtual Routing and Forwarding (VRF), provide a network segmentation mechanism that allows multiple clients to share a service provider's infrastructure while maintaining complete isolation of their data and routes. Each VRF functions as an independent routing domain, ensuring that one client's traffic cannot be accessed or viewed by others, which is critical for maintaining corporate information confidentiality and security.

In this practical exercise, an MPLS VPN network scenario will be implemented demonstrating the principles of labeling, client isolation, and efficient routing using protocols such as BGP, IGP, and VRF capabilities.



Advance Routing

DEVELOPTMENT

For the development of this project, the first thing we did was follow the project diagram to replicate it accurately and avoid logic errors. After that, we started with the IP addressing, following the diagram and verifying the ping to its nearest neighbor to ensure the addressing was correct. Once everything was functioning properly, we began configuring MPLS. We activated it on each router within the MPLS area and configured its internal routing protocol, which in this case was OSPF with area 0. We enabled MPLS within OSPF using the command `[mpls ldp autoconfig]`.

Next, we activated BGP within the MPLS zone, specifically on R1 and the Provider Edge routers. We set up R1 as a route reflector with its loopbacks. On the PE routers, we then configured their corresponding VRFs, named CUST_A and CUST_B, to ensure each had its own routing table. Afterward, we enabled BGP VPN to ensure that their networks were isolated from other routing tables while maintaining a direct connection between their different locations.

Finally, on the CE routers, we added a default route to allow them to reach their destinations and configured EBGP with a different autonomous system. Additionally, we configured and enabled their loopbacks. To have more security we enable the password to access to the terminal console, remote access (Telnet/SSH) and privileged mode, then we activate the encryption over the principal password.

EVIDENCE

Ping CA1 to CA2 and CA3

```
CE-CustA-1#ping 192.168.2.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/181/192 ms
CE-CustA-1#
```

```
CE-CustA-1#ping 192.168.3.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/150/156 ms
CE-CustA-1#
```

Advance Routing

Trace from CA1 to CA2 and CA3

```
CE-CustA-1#trace 192.168.2.1 source loopback 0

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 172.16.1.1 24 msec 32 msec 32 msec
  2 172.16.2.1 [MPLS: Label 25 Exp 0] 136 msec 152 msec 160 msec
  3 172.16.2.2 196 msec 168 msec 200 msec
CE-CustA-1#
```

```
CE-CustA-1#trace 192.168.3.1 source loopback 0

Type escape sequence to abort.
Tracing the route to 192.168.3.1

  1 172.16.1.1 24 msec 32 msec 36 msec
  2 172.16.3.1 [MPLS: Label 25 Exp 0] 100 msec 120 msec 124 msec
  3 172.16.3.2 156 msec 140 msec 168 msec
CE-CustA-1#
```

Ping CB1 to CB2:

```
CE-CustB-1#ping 192.168.7.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/184/200 ms
CE-CustB-1#
```

Trace from CB1 to CB2

```
CE-CustB-1#trace 192.168.7.1 source loopback 0

Type escape sequence to abort.
Tracing the route to 192.168.7.1

  1 172.16.3.1 20 msec 28 msec 32 msec
  2 172.16.4.1 [MPLS: Label 26 Exp 0] 148 msec 136 msec 144 msec
  3 172.16.4.2 212 msec 168 msec 184 msec
CE-CustB-1#
```

Advance Routing

VRF groups

```
PE-R4#show ip vrf
  Name                              Default RD          Interfaces
  CUST_A                            1:1                 Fa0/0
  CUST_B                            2:2                 Fa0/1
PE-R4#
```

Activate labels (MPLS) on OSPF

```
router ospf 7
 mpls ldp autoconfig
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet1/0
 network 10.1.40.0 0.0.0.3 area 0
 network 10.255.255.4 0.0.0.0 area 0
!
```

Hides the internal structure of MPLS

```
no mpls ip propagate-ttl
!
```

Password configuration

```
service password-encryption
!
hostname CE-CustA-1
!
boot-start-marker
boot-end-marker
!
enable password 7 104F0D140C19
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 020700560208
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password 7 045A0F0B062F
 login
```

CONCLUTIONS

Luis Carlos:
My conclusion about this practice is that it has been one of the coolest ones since we are using most of what we learned throughout the semester. With this new topic of MPLS, VRFs, and BGP VPN, it feels like one of the configurations that most closely resembles how many ISPs set up their networks to apply these protocols.

It allows them to provide their customers with maximum speed and security in their connections while ensuring they cannot see the internal structure of the network. This prevents customers from potentially exploiting that information to investigate or attack other customers.

Diego Gutiérrez:

We believe this is an excellent final project as it integrates several topics we covered throughout the semester. Moreover, understanding this type of communication with MPLS and the use of labels for routing is crucial. As we have explored in previous practical exercises, we can utilize different routing protocols, with the key consideration being to assess the specific needs before selecting the appropriate protocol. In this case, unlike Practice 7 where we only used VPN, we learned about a new type of technology: Virtual Routing and Forwarding (VRF), which enables us to segment routing tables, providing privacy between network links.

SOURCE

- Cisco Systems. (2021). *Cisco IOS IP Configuration Guide, Release 12.2*. Cisco Press.
- Doyle, J., & Carroll, D. (2005). *MPLS: Technology and Applications*. Morgan Kaufmann.
- Kompella, K., & Rekhter, Y. (2011). *RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)*. Internet Engineering Task Force (IETF).
- Pepelnjak, I. (2007). *MPLS and VPN Architectures*. Cisco Press.

- Rosen, E., & Viswanathan, A. (2006). *RFC 4761: Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*. Internet Engineering Task Force (IETF).