MPLS-enabled Network Services & Applications

PROJECT

Configuration and testing of three design options of internet access service to VPN customers

Authors: Aleksandra Mardaus, Jan Ściga, Michał Kurdziel

Spis treści

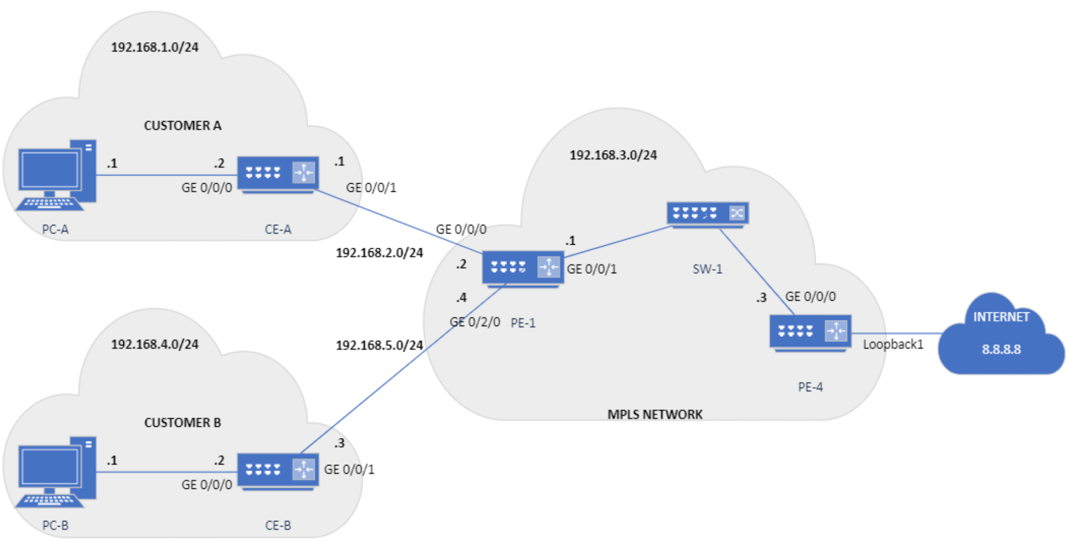
Introduction
The goal of the project is to configure and test three different design options for internet access service to VPN customers. The following types of design options for the mentioned service are considered:

- VRF Specific Default Route
- Separate PE-CE Sub-interfaces
- Extranet with Internet VRF

For each specific configuration, different topology will be built and configured to visualize the effect of each specific design option. Every subsection begins with short theoretical explanation of the presented feature. Then, the network topology built in the laboratory, required for the experiments is presented. Next, the configuration of the devices is given and finally the expected result and verification method. In the last paragraph, the conclusions from the conducted experiments are summarized.

VRF Specific Default Route
Theoretical Introduction
In this section, the configuration of Internet Access Service is provided with the use of VRF Specific Default Route. This solution acquires setting default route on PE-1 from Customer A and Customer B traffic to the router on which the Internet is available (PE-4). From backward traffic (Internet to Customer A and B), the static route pointing to the VRF interface is configured pointing to the neighbour on the internet access routers (PE-4). For the purpose of traffic capture and analysis, the switch SW-1 was added to the below configuration. The role of Internet is simulated by the Loopback1 interface on the PE-4 router visible in the below topology.

Topology
For configuring the kind of Internet Access Service introduced in the previous paragraph, the below topology was prepared in the laboratory.



Configuration

Basic configuration

In this section, the basic configuration should be made. This includes:

- interfaces (including loopbacks) addressing as shown in the *Topology* section
- OSPF configuration on each router (including advertising loopbacks)
- MPLS configuration in Core part of the network

Because of that the aforementioned points acquire only the fundamental configuration; these points are not included in the report.

Additionally, the VRFs and separate ospf processes for each VPN should be configured in the following way on PE-1.

```
ip vrf VPN-A
ip vrf VPN-B
!
router ospf 10 vrf VPN-A
 network 192.168.2.0 0.0.0.255 area 0
!
router ospf 20 vrf VPN-B
 network 192.168.5.0 0.0.0.255 area 0
!
interface GigabitEthernet0/2/0
 ip vrf forwarding VPN-B
!
interface GigabitEthernet0/0/0
 ip vrf forwarding VPN-A
```

Configuration 1 - Separate OSPF process for each VPN on PE-1

Finally, the monitor session should be configured to observe the traffic that is passing through the link between the PE-1 and PE-4.

```
monitor session 1 source interface Gi1/0/1
monitor session 1 destination interface Gi1/0/3
```

Configuration 2 - Monitor session configuration on SW-1

Default routes configuration

On the CE-A and CE-B routers, the default route for the Internet traffic should be configured. This route should redirect all the Internet traffic to the provider router.

```
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Configuration 3 - Default route configuration on CE-A

```
ip route 0.0.0.0 0.0.0.0 192.168.5.4
```

Configuration 4 - Default route configuration on CE-B

Additionally, on the PE-1 router, the VRF VPN-A and VPN-B default routes with *global* option should be enabled. This will inform router that it should look for the next hop in the global routing table.

```
ip route vrf VPN-A 0.0.0.0 0.0.0.0 192.168.3.3 global
ip route vrf VPN-B 0.0.0.0 0.0.0.0 192.168.3.3 global
```

Configuration 5 - Default route configuration on PE-1 in VRF tables

Last default route that is supposed to be configured is for the Internet traffic at the PE-4 router. It should redirect the traffic to the PE-1 router.

```
ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

Configuration 6 - Default route configuration on PE-4

Static route configuration

As the traffic from the Internet to the client will be passing through the PE-1, it should be aware of the route to the client routers. They should be added as thedefault routes on PE-1

```
ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0/0
ip route 192.168.4.0 255.255.255.0 GigabitEthernet0/2/0
```

Configuration 7 - Static route configuration on PE-1

Verification

For the purpose of appropriate verification of the configurations that we made, the inspection of the configured functionalities is divided into the following parts:

- Inspection on client computers
- Inspection on provider routers
- Inspection on client routers

Inspection on client computers

Ping from PC –A to the simulated Internet on *Loopback1* in PE-4

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::400:9cd9:a83:7124%14
   IPv4 Address. . . . . . . . . . . : 192.168.4.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.4.2

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c099:462b:5ca2:1882%8
   IPv4 Address. . . . . . . . . . . : 192.168.52.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=2ms TTL=253
Reply from 8.8.8.8: bytes=32 time=2ms TTL=253
Reply from 8.8.8.8: bytes=32 time=2ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\student>_
```

Verification 1 - Ping from PC-A to the Internet

Ping from PC-B to the simulated Internet on *Loopback1* in PE-4

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d29c:7633:238d:f2d3%9
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ccc8:fc30:9eb1:23b6%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.2

C:\Users\student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\student>
```

Verification 2 - Ping from PC-B to the Internet

Inspection on provider routers

Global routing table on PE-1:

```
PE1#show ip route

     10.0.0.0/32 is subnetted, 2 subnets
C       10.0.0.3 is directly connected, Loopback0
O       10.0.0.4 [110/2] via 192.168.3.3, 00:19:49, GigabitEthernet0/0/1
S    192.168.1.0/24 is directly connected, GigabitEthernet0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0/1
S    192.168.4.0/24 is directly connected, GigabitEthernet0/2/0
```

Verification 3 - Global routing table on PE-1

VRF VPN-A routing table on PE-1

```
PE1#show ip route vrf VPN-A

S*    0.0.0.0/0 [1/0] via 192.168.3.3
     10.0.0.0/32 is subnetted, 1 subnets
O       10.0.0.1 [110/2] via 192.168.2.1, 00:30:41, GigabitEthernet0/0/0
O    192.168.1.0/24 [110/2] via 192.168.2.1, 00:29:15, GigabitEthernet0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.2.2/32 is directly connected, GigabitEthernet0/0/0
```

Verification 4 - VRF VPN-A routing table on PE-1

VRF VPN-B routing table on PE-1

```
PE1#show ip route vrf VPN-B

S*    0.0.0.0/0 [1/0] via 192.168.3.3
     10.0.0.0/32 is subnetted, 1 subnets
O       10.0.0.2 [110/2] via 192.168.5.3, 00:30:09, GigabitEthernet0/2/0
O    192.168.4.0/24 [110/2] via 192.168.5.3, 00:30:09, GigabitEthernet0/2/0
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C       192.168.5.0/24 is directly connected, GigabitEthernet0/2/0
L       192.168.5.4/32 is directly connected, GigabitEthernet0/2/0
```

Verification 5 - VRF VPN-B routing table on PE-1

Global routing table on PE-4

```
PE-4#sh ip route
S*    0.0.0.0/0 [1/0] via 192.168.3.1
      8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        8.8.8.0/24 is directly connected, Loopback1
L        8.8.8.8/32 is directly connected, Loopback1
      10.0.0.0/32 is subnetted, 2 subnets
O        10.0.0.3 [110/2] via 192.168.3.1, 00:42:03, GigabitEthernet0/0/0
C        10.0.0.4 is directly connected, Loopback0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.3.3/32 is directly connected, GigabitEthernet0/0/0
```

Verification 6 - Global routing table on PE-4

Inspection on client routers

Global routing table on CE-A

```
R1#show ip route
S*    0.0.0.0/0 [1/0] via 192.168.2.2
                is directly connected, GigabitEthernet0/0/1
      10.0.0.0/32 is subnetted, 1 subnets
C        10.0.0.1 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0/1
```

Verification 7 - Global routing table on CE-A

Global routing table on CE-B

```
R2#show ip route

S*    0.0.0.0/0 [1/0] via 192.168.5.4
      10.0.0.0/32 is subnetted, 1 subnets
C        10.0.0.2 is directly connected, Loopback0
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.4.2/32 is directly connected, GigabitEthernet0/0/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.5.3/32 is directly connected, GigabitEthernet0/0/1
```

Verification 8 - Global routing table on CE-B

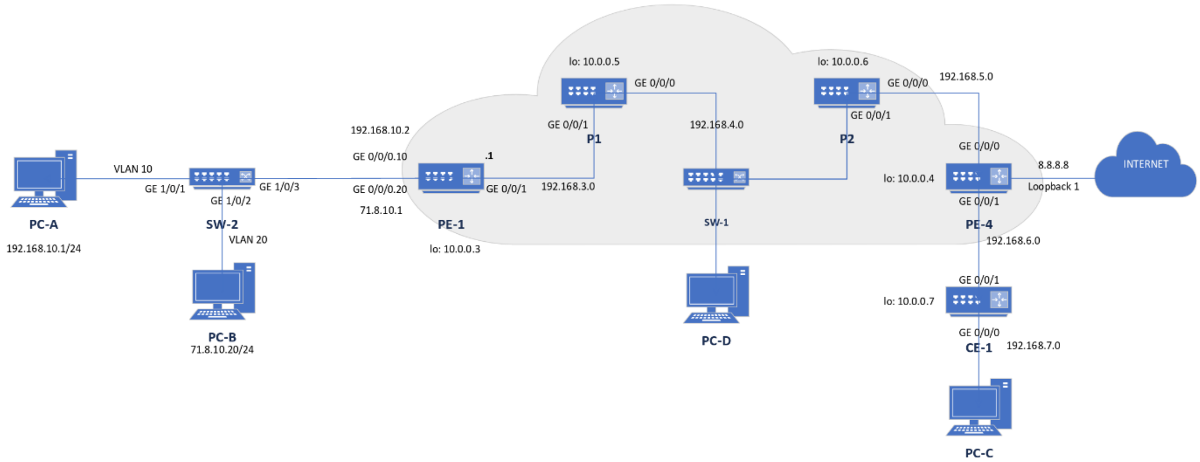
Separate PE-CE Sub-interfaces

Theoretical Introduction

We will create VPN connection between PC-A <=> PC-C and Internet access for PC-B. It will be done by separating above traffic via different VLAN tags on customer side and configuring two sub interfaces on PE-1:

- One for VPN traffic (VLAN 10)
- One for Internet access (VLAN 20)

Topology



Configuration

SW-2

- configure interfaces G1/0/1 (vlan 10), G1/0/2 (vlan 20) in access mode
- configure G1/0/3 as a trunk to forward vlan 10 and 20 traffic

PE-1

Create VRF to separate VPN related routes from global routing table:

```
ip vrf VPN-A
        rd 60000:11
        route-target export 60000:11
        route-target import 60000:12
```

Configuration 8 - VRF creation

Apply basic configuration for all physical interfaces (+ loopback). Enable MPLS on interface G0/0/1. Then create below sub interfaces:

```
interface GigabitEthernet0/0/0
        no ip address
        no sh

interface GigabitEthernet0/0/0.10                        # sub interface for VPN connection
        encapsulation dot1Q 10                           # match VLAN 10 traffic
        ip vrf forwarding VPN-A                          # bind VRF to sub interface
```

```
        ip address 192.168.10.2 255.255.255.0
        no sh

interface GigabitEthernet0/0/0.20                   # sub interface for Internet access
        encapsulation dot1Q 20
        ip address 71.8.10.1 255.255.255.0
        no sh
```

Configuration 9 - Subinterfaces creation

Configure core OSPF:

```
router ospf 1
        router-id 10.0.0.3
        network 10.0.0.3 0.0.0.0 area 0
        network 71.8.10.0 0.0.0.255 area 0
        network 192.168.3.0 0.0.0.255 area 0
```

Configuration 10 - OSPF core configuration

We must create MP-BGP session with PE-4 in order to advertise VPNv4 prefixes:

```
router bgp 60000
        neighbor 10.0.0.4 remote-as 60000             #PE-4 loopback address
        neighbor 10.0.0.4 update-source Loopback0

        address-family vpnv4
                neighbor 10.0.0.4 activate
                neighbor 10.0.0.4 send-community both
                exit-address-family
        address-family ipv4 vrf VPN-A
                redistribute connected         # which advertises also 192.168.10.0/24 network
                exit-address-family
```

Configuration 11 - BGP session creation

P1 and P2:

These routers are needed to observe MPLS labels in switch SW-1.

- address proper interfaces and enable MPLS
- advertise connected networks (+ loopback) using OSPF.

SW-1:

Configure monitor to observe traffic in PC-D. (Proper configuration has been given in previous scenario)

PE-4:

Create VRF:

```
ip vrf VPN-A
```

```
        rd 60000:12
        route-target export 60000:12
        route-target import 60000:11
```
Configuration 12 - VPN-A creation

Setup interfaces:

```
interface Loopback0
        ip address 10.0.0.4 255.255.255.255

interface Loopback1                    # for emulating Internet access
        ip address 8.8.8.8 255.255.255.0

interface GigabitEthernet0/0/0
        ip address 192.168.5.4 255.255.255.0
        mpls ip

interface GigabitEthernet0/0/1
        ip vrf forwarding VPN-A
        ip address 192.168.6.4 255.255.255.0
```
Configuration 13 - Interfaces setup

Next configure core OSPF:

```
router ospf 1
        router-id 10.0.0.4
        network 8.8.8.0 0.0.0.255 area 0
        network 10.0.0.4 0.0.0.0 area 0
        network 192.168.5.0 0.0.0.255 area 0
```
Configuration 14 - OSPF configuration

Configure OSPF under VRF:

```
router ospf 10 vrf VPN-A
        redistribute bgp 60000 metric 10 subnets
        network 10.0.0.4 0.0.0.0 area 0
        network 192.168.6.0 0.0.0.255 area 0
```
Configuration 15 - OSPF under VRF configuration

Next redistribute all VPNv4 prefixes to PE-1 using MP-BGP

```
router bgp 60000
        neighbor 10.0.0.3 remote-as 60000
        neighbor 10.0.0.3 update-source Loopback0
        address-family vpnv4
                neighbor 10.0.0.3 activate
                neighbor 10.0.0.3 send-community both
                exit-address-family

        address-family ipv4 vrf VPN-A
                redistribute connected
                redistribute ospf 10 metric 10 match internal external 1 external 2
                exit-address-family
```
Configuration 16 - VPNv4 prefixes redistribution using BGP

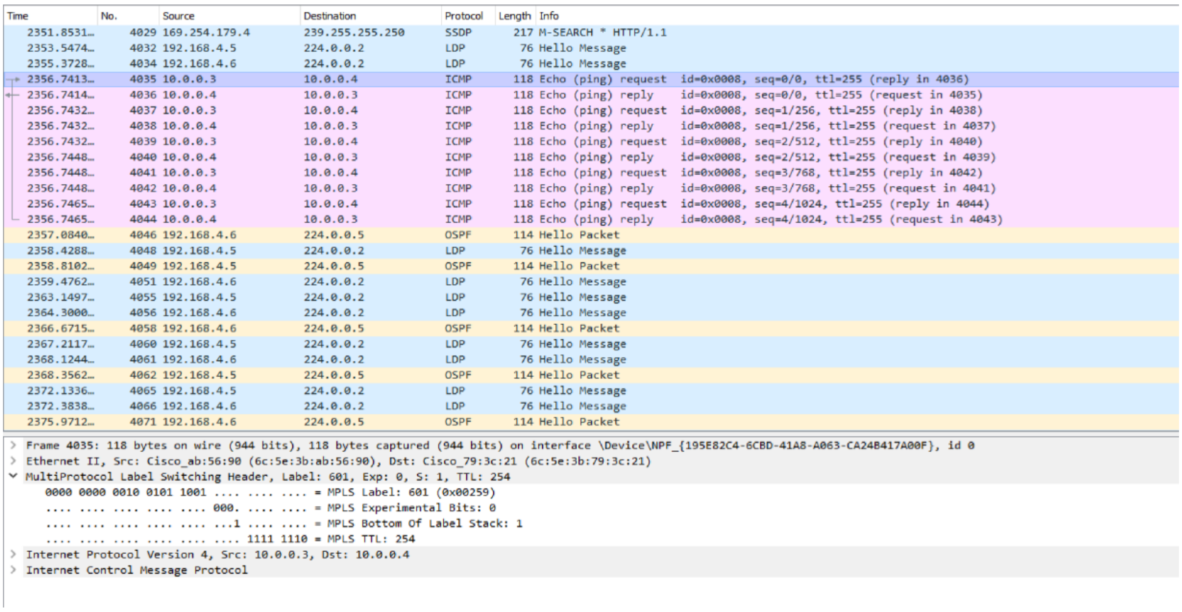
CE-1

Configure proper interfaces including Loopback 0, then setup basic OSPF configuration.

Verification

In order to check if MPLS core works properly do ping from PE-1 to PE-4 using Loopback address.

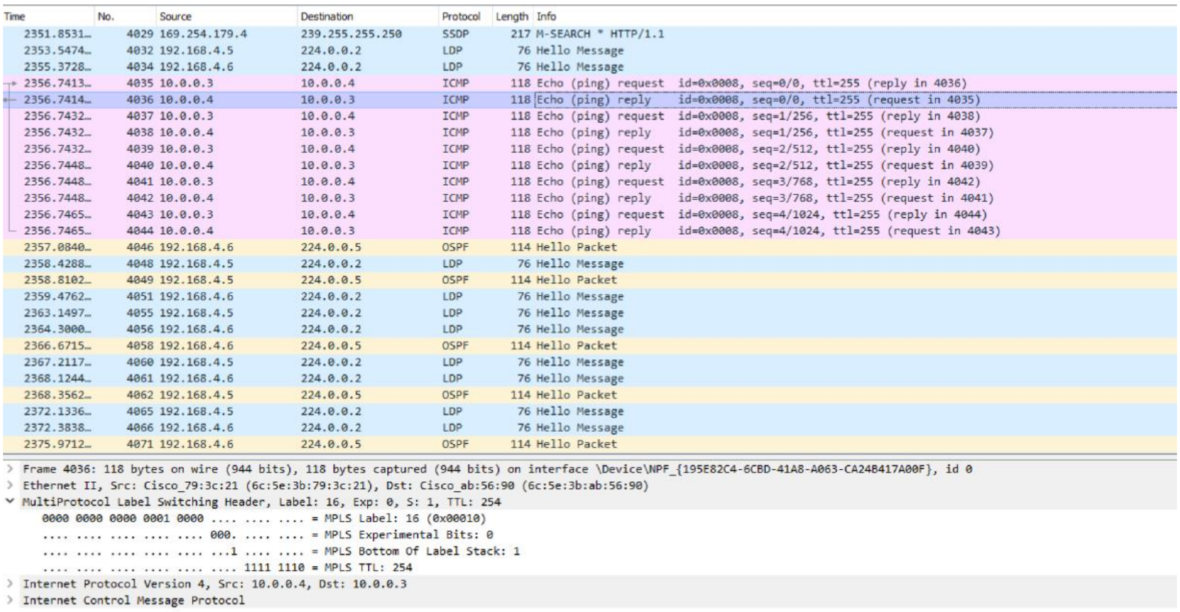
You should see similar results in Wireshark on PC-D.



Time	No.	Source	Destination	Protocol	Length	Info
2351.8531…	4029	169.254.179.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2353.5474…	4032	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2355.3728…	4034	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2356.7413…	4035	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=0/0, ttl=255 (reply in 4036)
2356.7414…	4036	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=0/0, ttl=255 (request in 4035)
2356.7432…	4037	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=1/256, ttl=255 (reply in 4038)
2356.7432…	4038	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=1/256, ttl=255 (request in 4037)
2356.7432…	4039	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=2/512, ttl=255 (reply in 4040)
2356.7448…	4040	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=2/512, ttl=255 (request in 4039)
2356.7448…	4041	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=3/768, ttl=255 (reply in 4042)
2356.7448…	4042	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=3/768, ttl=255 (request in 4041)
2356.7465…	4043	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=4/1024, ttl=255 (reply in 4044)
2356.7465…	4044	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=4/1024, ttl=255 (request in 4043)
2357.0840…	4046	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet
2358.4288…	4048	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2358.8102…	4049	192.168.4.5	224.0.0.5	OSPF	114	Hello Packet
2359.4762…	4051	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2363.1497…	4055	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2364.3000…	4056	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2366.6715…	4058	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet
2367.2117…	4060	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2368.1244…	4061	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2368.3562…	4062	192.168.4.5	224.0.0.5	OSPF	114	Hello Packet
2372.1336…	4065	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2372.3838…	4066	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2375.9712…	4071	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet

```
> Frame 4035: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{195E82C4-6CBD-41A8-A063-CA24B417A00F}, id 0
> Ethernet II, Src: Cisco_ab:56:90 (6c:5e:3b:ab:56:90), Dst: Cisco_79:3c:21 (6c:5e:3b:79:3c:21)
v MultiProtocol Label Switching Header, Label: 601, Exp: 0, S: 1, TTL: 254
    0000 0000 0010 0101 1001 .... .... .... = MPLS Label: 601 (0x00259)
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
> Internet Control Message Protocol
```

Verification 9- Ping request from PE-1



Time	No.	Source	Destination	Protocol	Length	Info
2351.8531…	4029	169.254.179.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2353.5474…	4032	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2355.3728…	4034	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2356.7413…	4035	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=0/0, ttl=255 (reply in 4036)
2356.7414…	4036	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=0/0, ttl=255 (request in 4035)
2356.7432…	4037	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=1/256, ttl=255 (reply in 4038)
2356.7432…	4038	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=1/256, ttl=255 (request in 4037)
2356.7432…	4039	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=2/512, ttl=255 (reply in 4040)
2356.7448…	4040	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=2/512, ttl=255 (request in 4039)
2356.7448…	4041	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=3/768, ttl=255 (reply in 4042)
2356.7448…	4042	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=3/768, ttl=255 (request in 4041)
2356.7465…	4043	10.0.0.3	10.0.0.4	ICMP	118	Echo (ping) request id=0x0008, seq=4/1024, ttl=255 (reply in 4044)
2356.7465…	4044	10.0.0.4	10.0.0.3	ICMP	118	Echo (ping) reply id=0x0008, seq=4/1024, ttl=255 (request in 4043)
2357.0840…	4046	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet
2358.4288…	4048	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2358.8102…	4049	192.168.4.5	224.0.0.5	OSPF	114	Hello Packet
2359.4762…	4051	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2363.1497…	4055	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2364.3000…	4056	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2366.6715…	4058	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet
2367.2117…	4060	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2368.1244…	4061	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2368.3562…	4062	192.168.4.5	224.0.0.5	OSPF	114	Hello Packet
2372.1336…	4065	192.168.4.5	224.0.0.2	LDP	76	Hello Message
2372.3838…	4066	192.168.4.6	224.0.0.2	LDP	76	Hello Message
2375.9712…	4071	192.168.4.6	224.0.0.5	OSPF	114	Hello Packet

```
> Frame 4036: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{195E82C4-6CBD-41A8-A063-CA24B417A00F}, id 0
> Ethernet II, Src: Cisco_79:3c:21 (6c:5e:3b:79:3c:21), Dst: Cisco_ab:56:90 (6c:5e:3b:ab:56:90)
v MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 1, TTL: 254
    0000 0000 0000 0001 0000 .... .... .... = MPLS Label: 16 (0x00010)
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Internet Control Message Protocol
```

Verification 10 - Ping reply from PE-4

We can check MPLS forwarding table on P1 and P2 to verify Wireshark output.

```
P1#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  10.0.0.3/32      10682         Gi0/0/1    192.168.3.1
500        601        10.0.0.4/32      12762         Gi0/0/0    192.168.4.6
501        Pop Label  192.168.5.0/24   3102          Gi0/0/0    192.168.4.6
502        Pop Label  10.0.0.6/32      0             Gi0/0/0    192.168.4.6
```

Verification 11 - MPLS forwarding table in P1

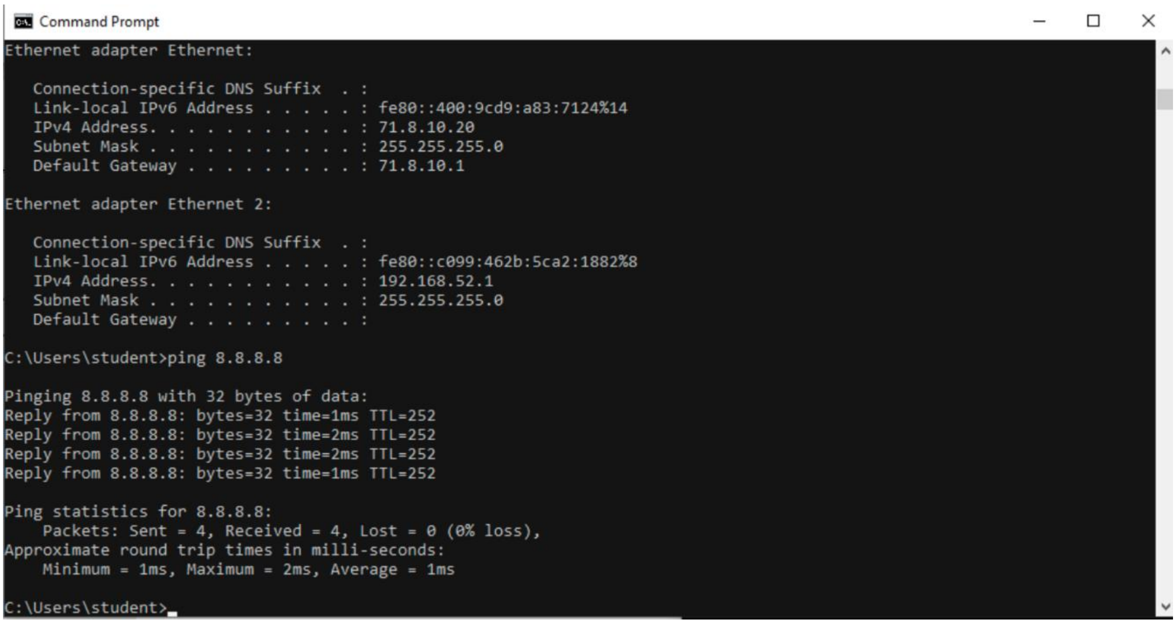
```
P2#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
600        16         10.0.0.3/32      10045         Gi0/0/1    192.168.4.5
601        Pop Label  10.0.0.4/32      10462         Gi0/0/0    192.168.5.4
602        Pop Label  10.0.0.5/32      0             Gi0/0/1    192.168.4.5
603        Pop Label  192.168.3.0/24   4184          Gi0/0/1    192.168.4.5
```

Verification 12 - MPLS forwarding table in P2

Now let’s verify connectivity between VPN sites (PC-A <=> PC-C) and Internet access for PC-B

```
Command Prompt
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : kt.agh.edu.pl
   Link-local IPv6 Address . . . . . : fe80::73a0:e418:2027:e79e%10
   IPv4 Address. . . . . . . . . . . : 192.168.7.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.7.7

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::239c:cafa:1f3:6810%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\student>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=123
Reply from 192.168.10.1: bytes=32 time=2ms TTL=123
Reply from 192.168.10.1: bytes=32 time=2ms TTL=123
Reply from 192.168.10.1: bytes=32 time=2ms TTL=123

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\student>
```

Verification 13 - Ping from PC-C to PC-A


```
Command Prompt
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::400:9cd9:a83:7124%14
   IPv4 Address. . . . . . . . . . . : 71.8.10.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 71.8.10.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c099:462b:5ca2:1882%8
   IPv4 Address. . . . . . . . . . . : 192.168.52.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252
Reply from 8.8.8.8: bytes=32 time=1ms TTL=252

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\student>
```

Verification 14 - Ping from PC-B to Internet

Extranet with Internet-VRF

Theoretical Introduction

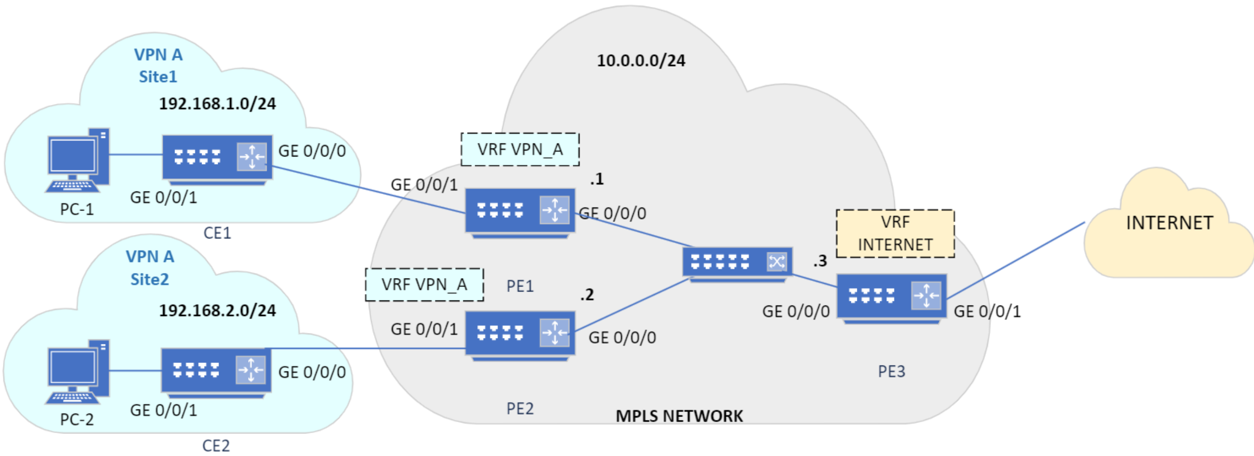
The last method of Internet Access Service to VPN Customer discussed in this paper is Extranet with Internet-VRF.

Virtual routing and forwarding (VRF) is a technology included in IP network routers that enables multiple instances of a routing table to exist in a virtual router and work simultaneously.

Route Targets are used to define which routes are exported and imported into a VRF routing table.

In order to make the customer able to access the Internet, we need to configure Route Targets on PE routers to enable VRF communication.

Topology



Configuration

Addressing + OSPF + MPLS

PE2
ip vrf VPNA rd 100:2 route-target export 1:10 route target import 1:10 route target import 100:10

PE3
ip vrf INTERNET rd 100:3 route target export 100:10 route target import 1:10 router bgp 100 address-family ipv4 vrf INTERNET network 0.0.0.0 0.0.0.0 ip route vrf INTERNET 0.0.0.0 0.0.0.0

Verification

PC-1: ping 8.8.8.8
PC-2: ping 8.8.8.8
(Clients should be able to access Internet)

show ip route vrf [vrf-name]

NOTE: This section is not widely expanded because of lack of access to the laboratory as well as internal arrangements with the laboratory instructor

Conclusions

Internet Access Service is a common and widely deployed service carried out by telecommunications operators. In this project, three design options of its configuration has been described, configured, tested and verified. Completing these tasks gave us opportunity to broaden our knowledge about modern MPLS services as well as expanded our practical skills in building, configuring and verifying MPLS-based L3 services in laboratory.