CCIE Service Provider Lab Workbook v4.0 - How to Use This Workbook v4

Overview (pending update)

INE's CCIE Service Provider Lab Workbook Version 3.0 is designed to be used as a supplement to other self-paced and instructor-led training materials in preparation for Cisco's CCIE Service Provider Lab Exam Version 3.0. This workbook is divided into two main sections, Advanced Technology Labs and Full-Scale Labs.

The Advanced Technology Labs are your hands-on practice companion to the CCIE Service Provider Advanced Technologies Video Course. These are individually-focused advanced technology labs that present topics in an easy-to-follow, goal-oriented, and step-by-step manner. The purpose of these labs is to isolate each topic on its own to give you firsthand experience with the various ways to configure each technology. By understanding these fundamental technologies, you will be able to predict advanced and sometimes subtle interactions when configuring multiple technologies together.

The Full-Scale Labs are 8-hour lab scenarios designed to simulate the actual CCIE Service Provider Lab Exam while also illustrating the principles behind the technologies they cover.

The recommended approach for using this workbook is as follows:

- Watch the videos in the CCIE Service Provider Advanced Technologies Video Course .
- Follow the recommended readings from class, including the Cisco documentation.
- Configure the associated labs in the Advanced Technology Labs section.
- Revisit the videos and readings for further clarification.
- Configure the labs in the Full-Scale Labs section.
- Take and pass the CCIE SPv3 Lab Exam!

CCIE Service Provider Lab Workbook v4.0 - How to Use This Workbook v4

Topology Information (pending update)

The physical topology for INE's CCIE Service Provider Lab Workbook Version 3.0 uses 10 routers and 2 switches, which include a mix of 7200s, 2600s, XR 12000s, Catalyst ME3400s, and Catalyst 3550s. This topology has the flexibility to mimic the requirements of Cisco's actual CCIE Service Provider Version 3.0 hardware blueprint, while minimizing the cost for users building their own lab at home or work and allowing users to run the regular IOS portion of the topology in GNS3/Dynamips.

Specifically, the platforms used in the development of this workbook are as follows:

Device	Platform	RAM	Flash	Modules
R1	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX, PA-4T+
R2	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX, PA-4T+
R3	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX
R4	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX
R5	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX
R6	7204VXR	256 MB	32 MB	C7200-IO-FE, PA-FE-TX

Device	Platform	RAM	Flash	Modules
R7	2611XM	128 MB	32 MB	WIC-1T
R8	2611XM	128 MB	32 MB	WIC-1T
XR1	XR 12000	2 GB	1 GB	PRP-2, 4GE-SFP-LC, 4OC3X/POS-IR-LC-B
XR2	XR 12000	2 GB	1 GB	PRP-2, 4GE-SFP-LC, 4OC3X/POS-IR-LC-B
SW1	ME3400	N/A	N/A	N/A
SW2	3550	N/A	N/A	N/A

CCIE Service Provider Lab Workbook v4.0 - How to Use This Workbook v4

IOS Version Information (pending update)

The IOS code versions used in the development of this workbook are as follows:

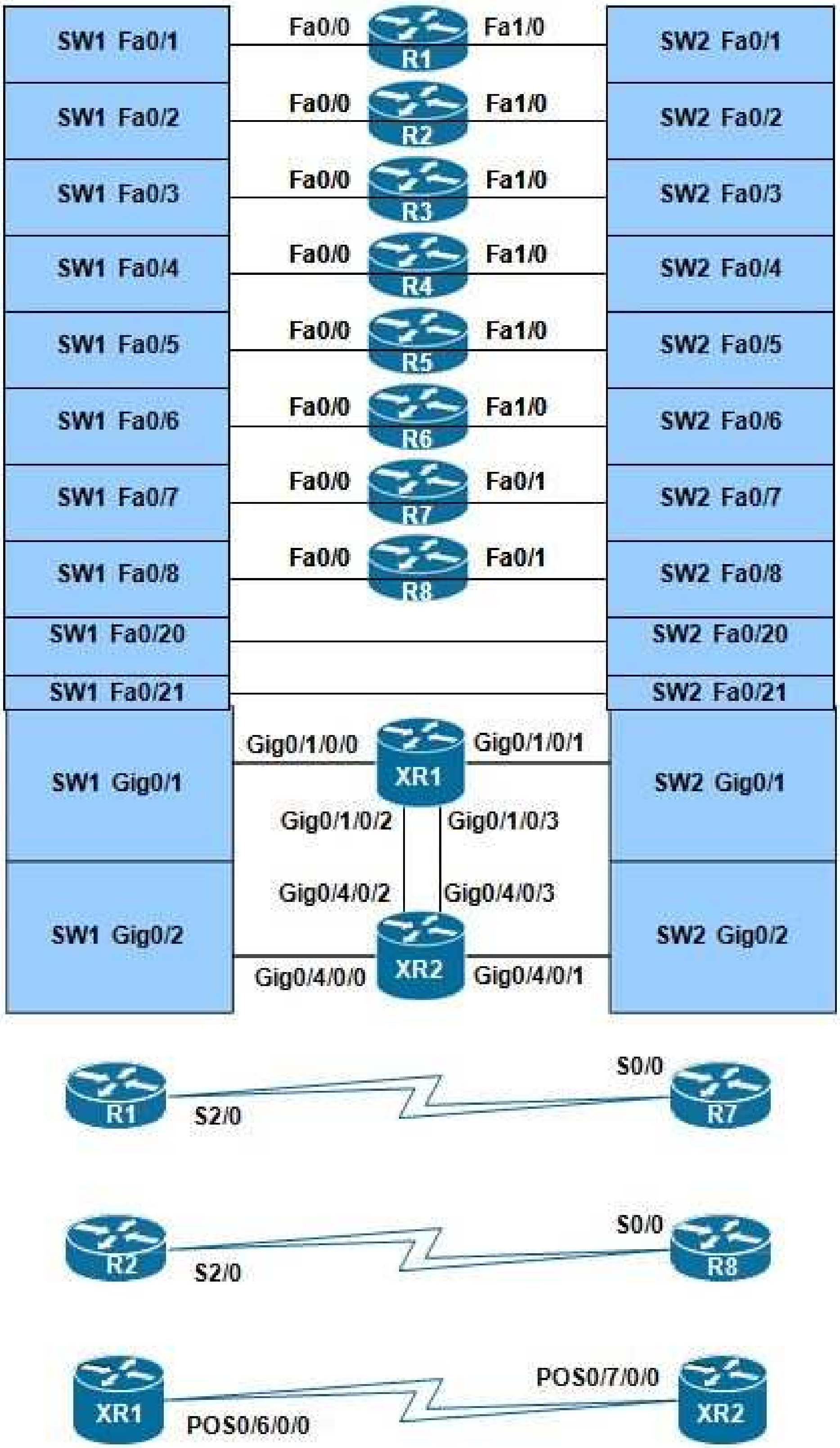
Device	IOS	Feature Set	Filename
R1	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R2	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R3	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R4	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R5	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R6	12.2(33)SRE3	Adv. IP Services	c7200-advipservicesk9-mz.122-33.SRE3.bin
R7	12.3(26)	Adv. Ent. Services	c2600-adventerprisek9-mz.123-26.bin
R8	12.3(26)	Adv. Ent. Services	c2600-adventerprisek9-mz.123-26.bin

Device	IOS	Feature Set	Filename
XR1	3.9.1	N/A	c12k-os-mbi-3.9.1/mbiprp-rp.vm
XR2	3.9.1	N/A	c12k-os-mbi-3.9.1/mbiprp-rp.vm
SW1	12.2(44)SE5	Metro IP Access	me340x-metroipaccessk9-mz.122-54.SE.bin
SW2	12.2(50)SE	IP Services	c3550-ipservicesk9-mz.122-50.SE.bin

CCIE Service Provider Lab Workbook v4.0 - How to Use This Workbook v4

Physical Wiring Diagram (pending update)

Physical Wiring Diagram



CCIE Service Provider Lab Workbook v4.0 - How to Use This Workbook v4

CCIE SPv4 Topology Diagrams & Initial Configs

Although the physical topology always remains the same throughout the workbook, there are multiple logical network diagrams that must be referenced to complete the tasks in both the Advanced Technology Labs and the Full-Scale Labs. Logical diagrams provide additional information about the network that is needed for a particular task, such as IPv4 addressing, IPv6 addressing, interface numbering, etc. Additionally, these logical diagrams include one or more sets of initial configurations that must be loaded on the network devices before beginning work on the associated tasks.

For the Advanced Technology Labs, each task will generally indicate which logical diagram to reference and which set of initial configurations to load. A few of the earlier labs have configurations that cumulatively build on each other, so it’s not required to reset the initial configurations or use a different diagram for those tasks. For tasks that do require a new diagram and reset of the initial configurations, you can find this information by clicking the **Resources** button at the top of the page.

Full-Scale Labs have one diagram and initial configuration set per lab. For example, for Full-Scale Lab 2, you simply load the Full-Scale Lab 2 initial configurations and reference the Full-Scale Lab 2 Diagram. These can be found in the **Tasks** section for each lab, by clicking the **Resources** button at the top of the page.

GNS3 Version 3 configurations and the GNS3 .NET file can be downloaded by clicking the **Resources** button above.

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 1: Bridging & Switching v4

1.1 Catalyst ME 3400 Port Types (pending update)

- Per the diagram, all routers are preconfigured with IP addresses in the 10.0.0.0/24 subnet. SW2 is configured with the links to R5, R6, R7, R8, and XR2 as access ports in VLAN 100, and its link Fa0/20 connecting to SW1 is configured as an 802.1q trunk link.
- Configure SW1 as follows:
  - Links connecting to R1, R2, R3, and R4 should be statically set to full duplex.
  - The link connecting to XR1 should be statically set to not negotiate the speed of the link.
  - Links connecting to R1, R2, R3, R4, and XR1 should all be access ports in VLAN 100.
  - Links connecting to R3, R4, and XR1 should be Enhanced Network Interface (ENI) port types and have CDP enabled.
  - The link connecting to SW2 should be a Network Node Interface (NNI) port type and an 802.1q trunk link.
- When complete, the following reachability should be achieved:
  - SW1 should see R3, R4, XR1, and SW2 as CDP neighbors.
  - All devices connected to SW2 should have full IP reachability to all routers in VLAN 100.
  - Devices connected to SW1 should only have IP reachability to the routers in VLAN 100 that are connected to SW2.

Configuration

```
SW1:
vlan 100
!
interface FastEthernet0/1
switchport access vlan 100 duplex full
!
interface FastEthernet0/2
```

```
switchport access vlan 100
duplex full
!
interface FastEthernet0/3
port-type eni
switchport access vlan 100
duplex full cdp enable
!
interface FastEthernet0/4
port-type eni
switchport access vlan 100 duplex full
cdp enable
!
interface FastEthernet0/20
port-type nni switchport mode trunk
!
interface GigabitEthernet0/1
port-type eni
switchport access vlan 100 speed nonegotiate
cdp enable
```

Verification

By default, all ports of the Catalyst ME3400 are User Network Interfaces (UNIs) with the exception of the uplink ports, which are Network Node Interfaces (NNIs). The configured or default port type can be verified as follows.

```
SW1#show port-type
Port      Name                 Vlan       Port Type
--------- ------------------ ---------- ---------------------------
Fa0/1                          100       User Network Interface      (uni)
Fa0/2                          100       User Network Interface      (uni)
 Fa0/3                          100       Enhanced Network Interface  (eni)
Fa0/4                          100       Enhanced Network Interface  (eni)
Fa0/5                          1           User Network Interface    (uni)
Fa0/6                          1           User Network Interface    (uni)
Fa0/                           1           User Network Interface    (uni)
Fa0/8                          1           User Network Interface    (uni)
Fa0/9                          1           User Network Interface    (uni)
Fa0/10                         1           User Network Interface    (uni)
Fa0/11                         1           User Network Interface    (uni)
Fa0/12                         1           User Network Interface    (uni)
Fa0/13                         1           User Network Interface    (uni)
Fa0/14                         1           User Network Interface    (uni)
```

```
Fa0/15                     1          User Network Interface    (uni)
Fa0/16                     1          User Network Interface    (uni)
Fa0/17                     1          User Network Interface    (uni)
Fa0/18                     1          User Network Interface    (uni)
Fa0/19                     1          User Network Interface    (uni)
Fa0/20                     trunk      Network Node Interface    (nni)
Fa0/21                     1          User Network Interface    (uni)
Fa0/22                     1          User Network Interface    (uni)
Fa0/23                     1          User Network Interface    (uni)
Fa0/24                     1          User Network Interface    (uni)
Gi0/1                      100      Enhanced Network Interface  (eni)

Gi0/2                      1          Network Node Interface    (nni)
```

By default, both UNI and ENI ports are only allowed to send traffic to NNI ports that are in the same VLAN, because the default UNI-VLAN mode is *isolated*, as shown below.

```
SW1#show vlan uni-vlan type

Vlan Type
---- -----------------
1   UNI isolated100 UNI isolated
```

The ENI ports can be configured with additional services that UNI ports do not support, such as CDP, LACP, or STP. Below we see that CDP is enabled on the ENI and NNI ports, but not UNI ports.

```
SW1#show cdp interface
FastEthernet0/3 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
FastEthernet0/4 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
FastEthernet0/20 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
```

```
    Holdtime is 180 seconds
GigabitEthernet0/2 is down, line protocol is down
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
SW1#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID    Local Intrfce    Holdtme Capability  Platform    Port ID
SW2          Fas 0/20         125     S I         WS-C3550-   Fas 0/20
XR1          Gig 0/1          155     R           12008/PRP   Gig 0/1/0/0
R3           Fas 0/3          145     R           7204VXR     Fas 0/0
R4           Fas 0/4          143     R           7204VXR     Fas 0/0
```

The final result of this configuration is that when traffic comes in a UNI or ENI port on SW1, it can only be sent to an NNI port. This means that R1, R2, R3, R4, and XR1 will not have reachability to each other, but will have reachability to R5, R6, R7, R8, and XR2. This can be quickly verified with ICMP PINGs sent to the broadcast address.

```
R1#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 1 ms
Reply to request 0 from 10.0.0.20, 1 ms
Reply to request 0 from 10.0.0.7, 1 ms
Reply to request 0 from 10.0.0.8, 1 ms
Reply to request 0 from 10.0.0.6, 1 ms

R2#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 1 ms
Reply to request 0 from 10.0.0.7, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.8, 4 ms
Reply to request 0 from 10.0.0.6, 1 ms
R3#ping 255.255.255.255 repeat 1
```

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.7, 4 ms
Reply to request 0 from 10.0.0.8, 4 ms
Reply to request 0 from 10.0.0.6, 4 ms
R4#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 1 ms
Reply to request 0 from 10.0.0.7, 1 ms
Reply to request 0 from 10.0.0.8, 1 ms
Reply to request 0 from 10.0.0.20, 1 ms
Reply to request 0 from 10.0.0.6, 1 ms
R5#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.4, 1 ms
Reply to request 0 from 10.0.0.7, 4 ms
Reply to request 0 from 10.0.0.8, 1 ms
Reply to request 0 from 10.0.0.20, 1 ms
Reply to request 0 from 10.0.0.19, 1 ms
Reply to request 0 from 10.0.0.6, 1 ms
Reply to request 0 from 10.0.0.2, 1 ms
Reply to request 0 from 10.0.0.1, 1 ms
Reply to request 0 from 10.0.0.3, 1 ms
R6#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.1, 4 ms
Reply to request 0 from 10.0.0.7, 4 ms
Reply to request 0 from 10.0.0.8, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.19, 4 ms
Reply to request 0 from 10.0.0.2, 4 ms
Reply to request 0 from 10.0.0.5, 4 ms
Reply to request 0 from 10.0.0.4, 4 ms
```

```
Reply to request 0 from 10.0.0.3, 4 ms
R7#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 4 ms
Reply to request 0 from 10.0.0.8, 8 ms
Reply to request 0 from 10.0.0.19, 8 ms
Reply to request 0 from 10.0.0.20, 8 ms
Reply to request 0 from 10.0.0.2, 8 ms
Reply to request 0 from 10.0.0.4, 8 ms
Reply to request 0 from 10.0.0.6, 4 ms
Reply to request 0 from 10.0.0.3, 4 ms
Reply to request 0 from 10.0.0.1, 4 ms
R8#ping 255.255.255.255 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.6, 4 ms
Reply to request 0 from 10.0.0.7, 8 ms
Reply to request 0 from 10.0.0.20, 8 ms
Reply to request 0 from 10.0.0.19, 4 ms
Reply to request 0 from 10.0.0.2, 4 ms
Reply to request 0 from 10.0.0.3, 4 ms
Reply to request 0 from 10.0.0.1, 4 ms
Reply to request 0 from 10.0.0.4, 4 ms
Reply to request 0 from 10.0.0.5, 4 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 1: Bridging & Switching v4

1.2 Catalyst ME 3400 UNI VLANS (pending update)

- Per the diagram, all routers are preconfigured with IP addresses in the 10.0.0.0/24 subnet. SW2 is configured with the links to R5, R6, R7, R8, and XR2 as access ports in VLAN 100, and its link Fa0/20 connecting to SW1 is configured as an 802.1q trunk link.
- Configure SW1 as follows:
  - Links connecting to R1, R2, R3, and R4 should be statically set to full duplex.
  - The link connecting to XR1 should be statically set to not negotiate the speed of the link.
  - Configure VLAN 100 as a UNI Community VLAN.
  - Links connecting to R1, R2, R3, R4, and XR1 should all be access ports in VLAN 100.
  - Links connecting to R3, R4, and XR1 should be Enhanced Network Interface (ENI) port types and have CDP enabled.
  - The link connecting to SW2 should be a Network Node Interface (NNI) port type and an 802.1q trunk link.
- When complete, the following reachability should be achieved:
  - SW1 should see R3, R4, XR1, and SW2 as CDP neighbors.
  - All routers in VLAN 100 should have full IP reachability to each other.

Configuration

```
SW1:
vlan 100
uni-vlan community
!
interface FastEthernet0/1
switchport access vlan 100 duplex full
!
interface FastEthernet0/2
switchport access vlan 100
```

```
duplex full
!
interface FastEthernet0/3
port-type eni
switchport access vlan 100
duplex full cdp enable
!
interface FastEthernet0/4
port-type eni
switchport access vlan 100 duplex full
cdp enable




!
interface FastEthernet0/20
port-type nni
switchport mode trunk
!
interface GigabitEthernet0/1
port-type eni
switchport access vlan 100
speed nonegotiate cdp enable
```

Verification

The behavior of UNI Community VLANs is similar to normal VLAN behavior on other Catalyst IOS platforms. UNI ports still do not support features such as CDP or STP, but if the VLAN is in Community mode, packets can be exchanged between local UNI or ENI ports. Verification of this task is similar to the previous task, with the exception that now all routers have full IP reachability to each other.

```
SW1#show vlan uni-vlan type

Vlan Type
---- -----------------
1   UNI isolated 100 UNI community
SW1#show port-type
Port    Name    Vlan    Port Type
--------- ----------------- ---------- ---------------------------
Fa0/1 100 User Network Interface  (uni)
Fa0/2 100 User Network Interface  (uni)
Fa0/3 100 Enhanced Network Interface  (eni)
Fa0/4 100 Enhanced Network Interface  (eni)
```

```
Fa0/5   1   User    Network Interface   (uni)
Fa0/6   1   User    Network Interface   (uni)
Fa0/7   1   User    Network Interface   (uni)
Fa0/8   1   User    Network Interface   (uni)
Fa0/9   1   User    Network Interface   (uni)
Fa0/10  1   User    Network Interface   (uni)
Fa0/11  1   User    Network Interface   (uni)
Fa0/12  1   User    Network Interface   (uni)
Fa0/13  1   User    Network Interface   (uni)
Fa0/14  1   User    Network Interface   (uni)
Fa0/15  1   User    Network Interface   (uni)
Fa0/16  1   User    Network Interface   (uni)
Fa0/17  1   User    Network Interface   (uni)
Fa0/18  1   User    Network Interface   (uni)
Fa0/19  1   User    Network Interface   (uni) Fa0/20    trunk   Network Node    Interface   (nni)
Fa0/21  1   User    Network Interface   (uni)
Fa0/22  1   User    Network Interface   (uni)
Fa0/23  1   User    Network Interface   (uni)
Fa0/24  1   User    Network Interface   (uni)  Gi0/1 100 Enhanced Network Interface  (eni)
Gi0/2   1   Network Node Interface  (nni)
SW1#show cdp interface
FastEthernet0/3 is up, line protocol is up
    Encapsulation ARPA
Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
FastEthernet0/4 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
FastEthernet0/20 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
GigabitEthernet0/2 is down, line protocol is down
    Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
SW1#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

```
Device ID       Local Intrfce      Holdtme     Capability      Platform    Port ID
SW2             Fas 0/20           145               S I       WS-C3550-   Fas 0/20
XR1             Gig 0/1            179                R        12008/PRP   Gig 0/1/0/0
R3              Fas 0/3            164                R        7204VXR     Fas 0/0
R4              Fas 0/4            163                R        7204VXR     Fas 0/0
```

In this case, devices on SW1 have full reachability everywhere.

```
R1#ping 255.255.255.255 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.3, 4 ms
Reply to request 0 from 10.0.0.19, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.8, 4 ms
Reply to request 0 from 10.0.0.7, 4 ms
Reply to request 0 from 10.0.0.4, 4 ms
Reply to request 0 from 10.0.0.6, 4 ms
Reply to request 0 from 10.0.0.2, 4 ms
Reply to request 0 from 10.0.0.5, 4 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 1: Bridging & Switching v4

1.3 Catalyst ME 3400 Private VLANS (pending update)

- Per the diagram, all routers are preconfigured with IP addresses in the 10.0.0.0/24 subnet.
- Configure SW1 as follows:
  - Links connecting to R1, R2, R3, R4, R5, and R6 should be statically set to full duplex.
  - The links connecting to XR1 and XR2 should be statically set to not negotiate the speed of the link.
  - Configure VLAN 100 as a Private VLAN Primary VLAN.
  - Configure VLAN 1000 as a Private VLAN Secondary Isolated VLAN.
  - Configure VLANs 2000 and 3000 as Private VLAN Secondary Community VLANs.
  - The links connecting to R1 and R2 should be Private VLAN Host Ports in the Secondary Private VLAN 1000.
  - The links connecting to R3 and R4 should be Private VLAN Host Ports in the Secondary Private VLAN 2000.
  - The links connecting to R5 and R6 should be Private VLAN Host Ports in the Secondary Private VLAN 3000.
  - The links connecting to XR1 and XR2 should be NNI ports and Private VLAN Promiscuous Ports.
- When complete, the following reachability should be achieved:
  - R1 should have IP reachability only to XR1 and XR2.
  - R2 should have IP reachability only to XR1 and XR2.
  - R3 and R4 should have reachability to each other and to XR1 and XR2.
  - R5 and R6 should have reachability to each other and to XR1 and XR2.
  - XR1 and XR2 should have reachability to all routers.

Configuration

```
SW1:
vlan 100
   private-vlan primary
   private-vlan association 1000,2000,3000
!
vlan 1000
   private-vlan isolated
!
vlan 2000
   private-vlan community
!
vlan 3000
   private-vlan community
!
interface FastEthernet0/1
 switchport private-vlan host-association   100 1000
 switchport mode private-vlan host
 duplex full
 no shutdown
!
interface FastEthernet0/2
 switchport private-vlan host-association   100 1000
 switchport mode private-vlan host
 duplex full
 no shutdown
!
interface FastEthernet0/3
 switchport private-vlan host-association   100 2000
 switchport mode private-vlan host
 duplex full
 no shutdown
!
interface FastEthernet0/4
 switchport private-vlan host-association   100 2000
 switchport mode private-vlan host
 duplex full
 no shutdown
!
interface FastEthernet0/5
 switchport private-vlan host-association   100 3000
 switchport mode private-vlan host
 duplex full
 no shutdown
!
interface FastEthernet0/6
 switchport private-vlan host-association 100 3000
```

```
 switchport mode private-vlan host
 no shutdown
!
interface GigabitEthernet0/1
 port-type nni
 switchport private-vlan mapping 100 1000,2000,3000
 switchport mode private-vlan promiscuous
 speed nonegotiate
 no shutdown
!
interface GigabitEthernet0/2
 port-type nni
 switchport private-vlan mapping 100 1000,2000,3000
 switchport mode private-vlan promiscuous
 speed nonegotiate
 no shutdown
```

Verification

Private VLANs on the ME3400 work similar to other Catalyst IOS platforms, with one minor exception. Promiscuous Ports can only be of port type Network Node Interface (NNI), not UNI or ENI. With Private VLANs, a single Primary VLAN is broken down into smaller Secondary VLANs. Secondary VLANs can either be of type Isolated or Community. Ports that are assigned to Isolated VLANs can only talk to Promiscuous Ports. Ports that are assigned to Community VLANs can talk to other ports in the same Community VLAN, and to the Promiscuous Ports.

Private VLAN types and assignments can be verified as follows.

```
SW1#show vlan private-vlan


Primary Secondary Type  Ports
------- --------- ----------------- -----------------------------------------
100 1000    isolated    Fa0/1,  Fa0/2,  Gi0/1,  Gi0/2
100 2000    community   Fa0/3,  Fa0/4,  Gi0/1,  Gi0/2
100 3000    community   Fa0/5,  Fa0/6,  Gi0/1,  Gi0/2
SW1#show vlan private-vlan type


Vlan Type
---- -----------------
100 primary
1000 isolated
2000 community
3000 community
```

Note that Gig0/1 and Gig0/2, the Promiscuous Ports, are assigned to all Secondary VLANs, both Isolated and Community. The final result can be verified with basic ICMP PING connectivity checks as follows.

R1 and R2 should only be able to reach XR1 and XR2, because R1 and R2 are in the Isolated VLAN.

```
R1#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.19, 4 ms
R2#ping 255.255.255.255 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.19, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
```

R3 and R4 should be able to reach each other, along with XR1 and XR2, because they are in the same Community VLAN.

```
R3#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.4, 4 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.19, 4 ms
R4#ping 255.255.255.255 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.3, 1 ms
Reply to request 0 from 10.0.0.20, 1 ms
Reply to request 0 from 10.0.0.19, 1 ms
```

Likewise R5 and R6 should be able to reach each other, along with XR1 and XR2, because they are in the same Community VLAN.

```
R5#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.6, 1 ms
Reply to request 0 from 10.0.0.20, 1 ms
Reply to request 0 from 10.0.0.19, 1 ms
R6#ping 255.255.255.255 repeat 1


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.0.0.5, 1 ms
Reply to request 0 from 10.0.0.20, 4 ms
Reply to request 0 from 10.0.0.19, 4 ms
```

XR1 and XR2 should be able to reach everyone, because they are both

Promiscuous Ports.

```
RP/0/0/CPU0:XR1#ping 10.0.0.1
Thu Mar 29 20:05:32.514 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/45/222 ms
RP/0/0/CPU0:XR1#ping 10.0.0.2
Thu Mar 29 20:05:34.300 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
RP/0/0/CPU0:XR1#ping 10.0.0.3
Thu Mar 29 20:05:35.672 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
RP/0/0/CPU0:XR1#ping 10.0.0.4
Thu Mar 29 20:05:36.954 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
RP/0/0/CPU0:XR1#ping 10.0.0.5
Thu Mar 29 20:05:38.168 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
RP/0/0/CPU0:XR1#ping 10.0.0.6

Thu Mar 29 20:05:39.315 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv2

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IPv4**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Using the Base IPv4 Diagram, configure OSPFv2 Area 0 on all interfaces of all devices.
- Statically set the OSPF Router IDs of all devices to their Loopback0 interface address.

Configuration

```
R1:
router ospf 1
 router-id 1.1.1.1
 network 0.0.0.0 255.255.255.255 area 0

R2:
router ospf 1
 router-id 2.2.2.2
 network 0.0.0.0 255.255.255.255 area 0

R3:
router ospf 1
 router-id 3.3.3.3
 network 0.0.0.0 255.255.255.255 area 0

R4:
router ospf 1
 router-id 4.4.4.4
 network 0.0.0.0 255.255.255.255 area 0

R5:
router ospf 1
```

```
 router-id 5.5.5.5
 network 0.0.0.0 255.255.255.255 area 0

R6:
router ospf 1
 router-id 6.6.6.6
 network 0.0.0.0 255.255.255.255 area 0

XR1:
router ospf 1
 router-id 19.19.19.19
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0.519
  !
  interface GigabitEthernet0/0/0/0.619
  !
  interface GigabitEthernet0/0/0/0.1920
  !
 !
!

XR2:
router ospf 1
 router-id 20.20.20.20
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0.1920
  !
 !
!
```

Verification

All devices should be adjacent with their directly connected neighbors.

```
R6#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
19.19.19.19       1   FULL/BDR        00:00:34    20.6.19.19      GigabitEthernet1.619
5.5.5.5           1   FULL/BDR        00:00:36    20.5.6.5        GigabitEthernet1.56
4.4.4.4           1   FULL/BDR        00:00:32    20.4.6.4        GigabitEthernet1.46
3.3.3.3           1   FULL/BDR        00:00:32    20.3.6.3        GigabitEthernet1.36
```

```
RP/0/0/CPU0:XR1#show ospf neighbor

Sun Apr 19 17:04:42.146 UTC

* Indicates MADJ interface

Neighbors for OSPF 1

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5         1     FULL/DR         00:00:34    20.5.19.5       GigabitEthernet0/0/0/0.519
    Neighbor is up for 00:02:48
6.6.6.6         1     FULL/DR         00:00:34    20.6.19.6       GigabitEthernet0/0/0/0.619
    Neighbor is up for 00:02:46
20.20.20.20     1     FULL/DR         00:00:38    10.19.20.20     GigabitEthernet0/0/0/0.1920
    Neighbor is up for 00:02:32

Total neighbor count: 3
```

All routers generate a Router LSA (LSA Type 1) and the DR for Ethernet links generates a Network LSA (LSA Type 2). The view of the OSPF database should be identical from all routers, both regular IOS and IOS XR.

```
R6#show ip ospf database

            OSPF Router with ID (6.6.6.6) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         630         0x80000002 0x00B542 2
2.2.2.2         2.2.2.2         527         0x80000005 0x00E76E 4
3.3.3.3         3.3.3.3         608         0x80000004 0x00041E 4
4.4.4.4         4.4.4.4         608         0x80000004 0x008238 5
5.5.5.5         5.5.5.5         233         0x80000004 0x005A78 4
6.6.6.6         6.6.6.6         230         0x80000003 0x003A2E 5
19.19.19.19     19.19.19.19     187         0x80000004 0x00426A 4
20.20.20.20     20.20.20.20     188         0x80000002 0x006C39 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        2.2.2.2         629         0x80000001 0x0021F5
10.19.20.20     20.20.20.20     189         0x80000001 0x00AC5B
20.2.3.3        3.3.3.3         623         0x80000001 0x00B34A
```

```
20.2.4.4        4.4.4.4         618         0x80000001 0x00A251
20.3.4.4        4.4.4.4         618         0x80000001 0x00C826
20.3.6.6        6.6.6.6         607         0x80000001 0x00A634
20.4.5.5        5.5.5.5         613         0x80000001 0x00DD02
20.4.6.6        6.6.6.6         607         0x80000001 0x00CC09
20.5.6.6        6.6.6.6         607         0x80000001 0x00F2DD
20.5.19.5       5.5.5.5         233         0x80000001 0x00286C
20.6.19.6       6.6.6.6         230         0x80000001 0x001674

RP/0/0/CPU0:XR1#show ospf database

Sun Apr 19 17:06:25.479 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         669         0x80000002 0x00b542 2
2.2.2.2         2.2.2.2         566         0x80000005 0x00e76e 4
3.3.3.3         3.3.3.3         648         0x80000004 0x00041e 4
4.4.4.4         4.4.4.4         647         0x80000004 0x008238 5
5.5.5.5         5.5.5.5         272         0x80000004 0x005a78 4
6.6.6.6         6.6.6.6         270         0x80000003 0x003a2e 5
19.19.19.19     19.19.19.19     225         0x80000004 0x00426a 4
20.20.20.20     20.20.20.20     226         0x80000002 0x006c39 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        2.2.2.2         668         0x80000001 0x0021f5
10.19.20.20     20.20.20.20     226         0x80000001 0x00ac5b
20.2.3.3        3.3.3.3         662         0x80000001 0x00b34a
20.2.4.4        4.4.4.4         656         0x80000001 0x00a251
20.3.4.4        4.4.4.4         656         0x80000001 0x00c826
20.3.6.6        6.6.6.6         647         0x80000001 0x00a634
20.4.5.5        5.5.5.5         650         0x80000001 0x00dd02
20.4.6.6        6.6.6.6         647         0x80000001 0x00cc09
20.5.6.6        6.6.6.6         647         0x80000001 0x00f2dd
20.5.19.5       5.5.5.5         272         0x80000001 0x00286c
20.6.19.6       6.6.6.6         270         0x80000001 0x001674
```

All devices should have full routing information about the network.

```
R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 10.1.2.2, 00:11:46, GigabitEthernet1.12
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/3] via 10.1.2.2, 00:11:36, GigabitEthernet1.12
      4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/3] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
      5.0.0.0/32 is subnetted, 1 subnets
O        5.5.5.5 [110/4] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/4] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.19.20.0/24 [110/5] via 10.1.2.2, 00:04:25, GigabitEthernet1.12
      19.0.0.0/32 is subnetted, 1 subnets
O        19.19.19.19 [110/5] via 10.1.2.2, 00:05:12, GigabitEthernet1.12
      20.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O        20.2.3.0/24 [110/2] via 10.1.2.2, 00:11:36, GigabitEthernet1.12
O        20.2.4.0/24 [110/2] via 10.1.2.2, 00:11:36, GigabitEthernet1.12
O        20.3.4.0/24 [110/3] via 10.1.2.2, 00:11:36, GigabitEthernet1.12
O        20.3.6.0/24 [110/3] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.4.5.0/24 [110/3] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.4.6.0/24 [110/3] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.5.6.0/24 [110/4] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.5.19.0/24 [110/4] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.6.19.0/24 [110/4] via 10.1.2.2, 00:11:26, GigabitEthernet1.12
O        20.20.20.20/32 [110/6] via 10.1.2.2, 00:04:15, GigabitEthernet1.12
RP/0/0/CPU0:XR2#show route ipv4 ospf

Sun Apr 19 17:07:44.974 UTC

O    1.1.1.1/32 [110/6] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    2.2.2.2/32 [110/5] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
```

```
O    3.3.3.3/32 [110/4] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    4.4.4.4/32 [110/4] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    5.5.5.5/32 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    6.6.6.6/32 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    10.1.2.0/24 [110/5] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    19.19.19.19/32 [110/2] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.2.3.0/24 [110/4] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.2.4.0/24 [110/4] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.3.4.0/24 [110/4] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.3.6.0/24 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.4.5.0/24 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.4.6.0/24 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.5.6.0/24 [110/3] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.5.19.0/24 [110/2] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
O    20.6.19.0/24 [110/2] via 10.19.20.19, 00:05:04, GigabitEthernet0/0/0/0.1920
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv2 Network Types

- Change the OSPF Network Type of the link between R5 and XR1 to Point-to-Point.

Configuration

```
R5:
interface GigabitEthernet1.519
  ip ospf network point-to-point

XR1:
router ospf 1
area 0
  interface GigabitEthernet0//0/0.519
  network point-to-point
```

Verification

The link between R5 and XR1 now runs in OSPF Point-to-Point Network Type as opposed to the default Broadcast Network Type.

```
R5#show ip ospf interface GigabitEthernet1.519
GigabitEthernet1.519 is up, line protocol is up
  Internet Address 20.5.19.5/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 5.5.5.5, Network Type POINT_TO_POINT
, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
```

```
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 19.19.19.19
  Suppress hello for 0 neighbor(s)
RP/0/0/CPU0:XR1#show ospf interface GigabitEthernet0/0/0/0.519
Sun Apr 19 17:16:58.396 UTC

GigabitEthernet0/0/0/0.519 is up, line protocol is up
  Internet Address 20.5.19.19/24, Area 0   Process ID 1, Router ID 19.19.19.19,
Network Type POINT_TO_POINT
, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT, MTU 1500, MaxPktSz 1500
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05:707
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 16
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
```

A Network LSA (LSA Type 2) is no longer generated for the Ethernet link between R5 and XR1. Since there are only two routers on the segment, using network type Point-to-Point simplifies the OSPF database lookup. The most efficient design for this topology would then be to run Network Type Point-to-Point on all router to router Ethernet links.

```
R5#show ip ospf database

            OSPF Router with ID (5.5.5.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1354        0x80000002 0x00B542 2
2.2.2.2         2.2.2.2         1251        0x80000005 0x00E76E 4
3.3.3.3         3.3.3.3         1333        0x80000004 0x00041E 4
4.4.4.4         4.4.4.4         1332        0x80000004 0x008238 5
```

```
5.5.5.5         5.5.5.5         144         0x80000006 0x00A3D5 5
6.6.6.6         6.6.6.6         955         0x80000003 0x003A2E 5
19.19.19.19     19.19.19.19     142         0x80000007 0x004248 5
20.20.20.20     20.20.20.20     911         0x80000002 0x006C39 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        2.2.2.2         1353        0x80000001 0x0021F5
10.19.20.20     20.20.20.20     912         0x80000001 0x00AC5B
20.2.3.3        3.3.3.3         1347        0x80000001 0x00B34A
20.2.4.4        4.4.4.4         1341        0x80000001 0x00A251
20.3.4.4        4.4.4.4         1341        0x80000001 0x00C826
20.3.6.6        6.6.6.6         1332        0x80000001 0x00A634
20.4.5.5        5.5.5.5         1336        0x80000001 0x00DD02
20.4.6.6        6.6.6.6         1332        0x80000001 0x00CC09
20.5.6.6        6.6.6.6         1332        0x80000001 0x00F2DD
20.6.19.6       6.6.6.6         955         0x80000001 0x001674
```

RP/0/0/CPU0:XR1#show ospf database

```
Sun Apr 19 17:18:46.498 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1410        0x80000002 0x00b542 2
2.2.2.2         2.2.2.2         1307        0x80000005 0x00e76e 4
3.3.3.3         3.3.3.3         1389        0x80000004 0x00041e 4
4.4.4.4         4.4.4.4         1388        0x80000004 0x008238 5
5.5.5.5         5.5.5.5         201         0x80000006 0x00a3d5 5
6.6.6.6         6.6.6.6         1011        0x80000003 0x003a2e 5
19.19.19.19     19.19.19.19     197         0x80000007 0x004248 5
20.20.20.20     20.20.20.20     967         0x80000002 0x006c39 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        2.2.2.2         1409        0x80000001 0x0021f5
10.19.20.20     20.20.20.20     967         0x80000001 0x00ac5b
20.2.3.3        3.3.3.3         1403        0x80000001 0x00b34a
20.2.4.4        4.4.4.4         1397        0x80000001 0x00a251
20.3.4.4        4.4.4.4         1397        0x80000001 0x00c826
20.3.6.6        6.6.6.6         1388        0x80000001 0x00a634
```

```
20.4.5.5        5.5.5.5         1391        0x80000001 0x00dd02
20.4.6.6        6.6.6.6         1388        0x80000001 0x00cc09
20.5.6.6        6.6.6.6         1388        0x80000001 0x00f2dd
20.6.19.6       6.6.6.6         1011        0x80000001 0x001674
```

RP/0/0/CPU0:XR1#show ospf database router self-originate

```
Sun Apr 19 17:19:15.136 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 1)

                Router Link States (Area 0)

  LS age: 226
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 19.19.19.19
  Advertising Router: 19.19.19.19
  LS Seq Number: 80000007
  Checksum: 0x4248
  Length: 84
   Number of Links: 5

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 19.19.19.19
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1
 Link connected to: another Router (point-to-point)
     (Link ID) Neighboring Router ID: 5.5.5.5
     (Link Data) Router Interface address: 20.5.19.19

      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 20.5.19.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.6.19.6
     (Link Data) Router Interface address: 20.6.19.19
      Number of TOS metrics: 0
```

```
      TOS 0 Metrics: 1

   Link connected to: a Transit Network
    (Link ID) Designated Router address: 10.19.20.20
    (Link Data) Router Interface address: 10.19.20.19
     Number of TOS metrics: 0
      TOS 0 Metrics: 1
```

Prior to making the change, XR1 was originating the Type-2 LSA for the LAN segment between R5 and XR1.

```
RP/0/0/CPU0:XR1#show ospf database network self-originate
Sun Apr 19 17:20:25.522 UTC
            OSPF Router with ID (19.19.19.19) (Process ID 1)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv2 Path Selection

- Change the OSPF cost on the link between R6 and XR1 so that bidirectional traffic between R1 and XR2 prefers to use the link between R5 and XR1.

Configuration

```
R6:
interface GigabitEthernet1.619
 ip ospf cost 100

XR1:
router ospf 1
 area 0
 !
 interface GigabitEthernet0/0/0/0.619
  cost 100
  !
 !
!
```

Verification

Prior to making a change, review the forwarding state of the network. XR1 has two equal cost paths to reach R1.

```
RP/0/0/CPU0:XR1#show route ipv4 1.1.1.1/32
Sun Apr 19 17:49:17.723 UTC
Routing entry for 1.1.1.1/32
  Known via "ospf 1", distance 110, metric 5, type intra area
  Installed Apr 19 17:48:57.484 for 00:00:20
  Routing Descriptor Blocks 20.5.19.5, from 1.1.1.1, via GigabitEthernet0/0/0/0.519
      Route metric is 5 20.6.19.6, from 1.1.1.1, via GigabitEthernet0/0/0/0.619

      Route metric is 5
```

```
No advertising protos.
```

This can also be verified by looking at the FIB.

```
RP/0/0/CPU0:XR1#show cef ipv4 1.1.1.1/32 detail

Sun Apr 19 17:55:16.468 UTC 1.1.1.1/32
, version 131, internal 0x4000001 0x0 (ptr 0xa0edc074) [1], 0x0 (0xa0ea75a8), 0x0 (0x0)
 Updated Apr 19 17:48:57.504
 local adjacency 20.5.19.5
 Prefix Len 32, traffic index 0, precedence n/a, priority 1
  gateway array (0xa0d30130) reference count 7, flags 0x0, source rib (6), 0 backups
                [8 type 3 flags 0x8081 (0xa0df180c) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0xa0ea75a8, sh-ldi=0xa0df180c] via 20.5.19.5, GigabitEthernet0/0/0/0.519
, 7 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0xa15365c8 0x0] next hop 20.5.19.5
    tx adjacency via 20.6.19.6, GigabitEthernet0/0/0/0.619
, 7 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 1 NHID 0x0 [0xa153663c 0x0] next hop 20.6.19.6
    tx adjacency


    Load distribution: 0 1 (refcount 8)

    Hash  OK  Interface                 Address 0      Y   GigabitEthernet0/0/0/0.519 20.5.19.5
      1      Y   GigabitEthernet0/0/0/0.619 20.6.19.6
```

Similarly, R2 has two equal cost paths to reach XR2.

```
R2#show ip route 20.20.20.20
Routing entry for 20.20.20.20/32
  Known via "ospf 1", distance 110, metric 5, type intra area
  Last update from 20.2.3.3 on GigabitEthernet1.23, 00:07:59 ago
  Routing Descriptor Blocks:  * 20.2.4.4, from 20.20.20.20, 00:54:17 ago, via GigabitEthernet1.24
      Route metric is 5, traffic share count is 1
 20.2.3.3, from 20.20.20.20, 00:07:59 ago, via GigabitEthernet1.23
      Route metric is 5, traffic share count is 1
R2#show ip cef 20.20.20.20/32 detail
20.20.20.20/32, epoch 2, per-destination sharing nexthop 20.2.3.3 GigabitEthernet1.23
 nexthop 20.2.4.4 GigabitEthernet1.24
```

After making the change, the link between R6 and XR1 has its OSPF Cost increased from 1 to 100, making it less preferred.

```
R6#show ip ospf interface | include line protocol|Cost:
Loopback0 is up, line protocol is up
  Process ID 1, Router ID 6.6.6.6, Network Type LOOPBACK, Cost: 1 GigabitEthernet1.619
 is up, line protocol is up   Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 100
GigabitEthernet1.56 is up, line protocol is up
  Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 1
GigabitEthernet1.46 is up, line protocol is up
  Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 1
GigabitEthernet1.36 is up, line protocol is up
  Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 1
RP/0/0/CPU0:XR1#show ospf interface | include "line protocol|Cost"
Sun Apr 19 17:42:15.732 UTC
Loopback0 is up, line protocol is up
  Process ID 1, Router ID 19.19.19.19, Network Type LOOPBACK, Cost: 1
GigabitEthernet0/0/0/0.519 is up, line protocol is up
  Process ID 1, Router ID 19.19.19.19, Network Type POINT_TO_POINT, Cost: 1 GigabitEthernet0/0/0/0.619
 is up, line protocol is up   Process ID 1, Router ID 19.19.19.19, Network Type BROADCAST, Cost: 100

GigabitEthernet0/0/0/0.1920 is up, line protocol is up
  Process ID 1, Router ID 19.19.19.19, Network Type BROADCAST, Cost: 1
```

The forwarding tables on R2 and XR1 reflect the change.

```
RP/0/0/CPU0:XR1#show cef ipv4 1.1.1.1/32 detail

Sun Apr 19 17:59:50.260 UTC
1.1.1.1/32, version 149, internal 0x4000001 0x0 (ptr 0xa0edc074) [1], 0x0 (0xa0ea75a8), 0x0 (0x0)
 Updated Apr 19 17:59:45.690
 local adjacency 20.5.19.5
 Prefix Len 32, traffic index 0, precedence n/a, priority 1
  gateway array (0xa0d300b8) reference count 14, flags 0x0, source rib (6), 0 backups
              [15 type 3 flags 0x8081 (0xa0df17d0) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0xa0ea75a8, sh-ldi=0xa0df17d0] via 20.5.19.5, GigabitEthernet0/0/0/0.519
, 5 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0xa15365c8 0x0] next hop 20.5.19.5
    tx adjacency



    Load distribution: 0 (refcount 15)

    Hash  OK  Interface                 Address 0     Y   GigabitEthernet0/0/0/0.519 20.5.19.5
```

```
R2#show ip cef 20.20.20.20/32 detail

20.20.20.20/32, epoch 2 nexthop 20.2.4.4 GigabitEthernet1.24
```

Traffic from R1 to XR2 avoids the link between R6 and XR1 due to its higher cost.

```
R1#traceroute 20.20.20.20
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 1 msec 2 msec 1 msec
  2 20.2.4.4 1 msec 1 msec 1 msec
  3 20.4.5.5 2 msec 1 msec 5 msec 4 20.5.19.19 10 msec 12 msec 13 msec
  5 10.19.20.20 62 msec *  3 msec

RP/0/0/CPU0:XR2#traceroute 1.1.1.1
Sun Apr 19 17:43:41.216 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

1  10.19.20.19 0 msec  0 msec  0 msec 2  20.5.19.5 0 msec  0 msec  0 msec

3  20.4.5.4 0 msec  0 msec  0 msec
4  20.2.4.2 0 msec  0 msec  0 msec
5  10.1.2.1 0 msec  *  0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv2 BFD

- Configure BFD for OSPF between R2 and R4 so that if there is a failure of the link between them, they begin reconvergence in less than one second.

Configuration

> Note: BFD is not supported on the current releases of the XRv platform.

```
R2:
interface GigabitEthernet1.24
 ip ospf bfd
 bfd interval 250 min_rx 250 multiplier 3

R4:
interface GigabitEthernet1.24
 ip ospf bfd
 bfd interval 250 min_rx 250 multiplier 3
```

Verification

R2 and R4 are BFD adjacent, and will detect a failure in less than one second.

```
R2#show bfd neighbors detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
20.2.4.4                             4097/4097       Up        Up        Gi1.24
Session state is UP and using echo function with 250 ms interval.
Session Host: Software
OurAddr: 20.2.4.2
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
```

```
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(21)
Rx Count: 17, Rx Interval (ms) min/max/avg: 1/992/799 last: 713 ms ago
Tx Count: 22, Tx Interval (ms) min/max/avg: 1/971/825 last: 201 ms ago
Elapsed time watermarks: 0 0 (last: 0) Registered protocols: OSPF CEF

Uptime: 00:00:13
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 4097             - Your Discr.: 4097
             Min tx interval: 1000000    - Min rx interval: 1000000 Min Echo interval: 250000



R4#show bfd neighbors detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
20.2.4.2                             4097/4097       Up        Up        Gi1.24
Session state is UP and using echo function with 250 ms interval.
Session Host: Software
OurAddr: 20.2.4.4
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(125)
Rx Count: 124, Rx Interval (ms) min/max/avg: 1/1001/867 last: 684 ms ago
Tx Count: 127, Tx Interval (ms) min/max/avg: 1/1001/849 last: 405 ms ago
Elapsed time watermarks: 0 0 (last: 0) Registered protocols: OSPF CEF

Uptime: 00:01:47
Last packet: Version: 1                  - Diagnostic: 0
            State bit: Up               - Demand bit: 0
            Poll bit: 0                 - Final bit: 0
            C bit: 0
            Multiplier: 3               - Length: 24
            My Discr.: 4097             - Your Discr.: 4097
            Min tx interval: 1000000    - Min rx interval: 1000000 Min Echo interval: 250000
```

When R2's link goes down, R4 detects this within one second. Notice the timestamps on the logs indicating reconvergence within 1 second.

```
R4#debug bfd event

 BFD event debugging is on

 R2#conf t
 Enter configuration commands, one per line.  End with CNTL/Z.R2(config)#interface GigabitEthernet1.24
R2(config-subif)#shutdown
R2(config-subif)#end
 R2#*Apr 19 20:32:20 : %OSPF-5-ADJCHG: Process 1,
 Nbr 4.4.4.4 on GigabitEthernet1.24 from FULL to DOWN, Neighbor Down: Interface down or detached

 R4#
 *Apr 19 20:32:21 : BFD-DEBUG Event: V1 FSM ld:4097 handle:1 event:ECHO FAILURE
  state:UP (0)*Apr 19 20:32:21 : BFD-DEBUG EVENT: bfd_session_destroyed, proc:OSPF
, handle:1 act*Apr 19 20:32:21 : %OSPF-5-ADJCHG: Process 1,
 Nbr 2.2.2.2 on GigabitEthernet1.24 from FULL to DOWN, Neighbor Down: BFD node down

 R4#
 *Apr 19 20:32:21: BFD-DEBUG Event: notify client(CEF) IP:20.2.4.2, ld:4097, handle:1, event:DOWN, cp independent fai
 *Apr 19 20:32:21: BFD-DEBUG Event: notify client(OSPF) IP:20.2.4.2, ld:4097, handle:1, event:DOWN, cp independent fa
 *Apr 19 20:32:21: BFD-DEBUG Event: notify client(CEF) IP:20.2.4.2, ld:4097, handle:1, event:DOWN, cp independent fai
```

Traffic between R1 and XR2 now uses the link between R2 and R3.

```
R1#traceroute 20.20.20.20
 Type escape sequence to abort.
 Tracing the route to 20.20.20.20
 VRF info: (vrf in name/id, vrf out name/id)
   1 10.1.2.2 4 msec 1 msec 1 msec 2 20.2.3.3 1 msec 1 msec 1 msec

   3 20.3.4.4 2 msec 1 msec 4 msec
   4 20.4.5.5 10 msec 8 msec 10 msec
   5 20.5.19.19 9 msec 13 msec 13 msec
   6 10.19.20.20 13 msec *  4 msec
```

Note: previous to the failure, the traceroute output took the following path:

```
R1#traceroute 20.20.20.20
 Type escape sequence to abort.
 Tracing the route to 20.20.20.20
 VRF info: (vrf in name/id, vrf out name/id)
   1 10.1.2.2 1 msec 2 msec 1 msec
```

```
2 20.2.4.4 1 msec 1 msec 1 msec

  3 20.4.5.5 2 msec 1 msec 5 msec
  4 20.5.19.19 10 msec 12 msec 13 msec
  5 10.19.20.20 62 msec *  3 msec
```

Accordingly, XR2 also follows the new path via R3:

```
RP/0/0/CPU0:XR2#traceroute 1.1.1.1
Sun Apr 19 20:20:36.431 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.5.6.6 0 msec  0 msec  0 msec  4  20.3.6.3 0 msec  0 msec  0 msec

 5  20.2.3.2 0 msec  0 msec  0 msec
 6  10.1.2.1 0 msec  *  0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv2 Authentication

- Configure clear text OSPF Authentication between R6 and XR1 using the password “INECLEAR”.
- Configure MD5 OSPF Authentication between R5 and XR1 using the password “INEMD5”.

Configuration

```
R5:
interface GigabitEthernet1.519
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 INEMD5

R6:
interface GigabitEthernet1.619
 ip ospf authentication
 ip ospf authentication-key INECLEAR

XR1:
router ospf 1
 area 0
  !
  interface GigabitEthernet0/0/0/0.519
   authentication message-digest
   message-digest-key 1 md5 INEMD5
  !
  interface GigabitEthernet0/0/0/0.619
   authentication-key INECLEAR
   authentication
  !
 !
!
```

Verification

R5 and XR1 have MD5 authentication enabled using Key ID 1, and are adjacent with each other.

```
R5#show ip ospf interface GigabitEthernet1.519
GigabitEthernet1.519 is up, line protocol is up
  Internet Address 20.5.19.5/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 5.5.5.5, Network Type POINT_TO_POINT, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1  Adjacent with neighbor 19.19.19.19
  Suppress hello for 0 neighbor(s) Cryptographic authentication enabled
 Youngest key id is 1

RP/0/0/CPU0:XR1#show ospf interface GigabitEthernet0/0/0/0.519
Sun Apr 19 20:44:49.371 UTC

GigabitEthernet0/0/0/0.519 is up, line protocol is up
  Internet Address 20.5.19.19/24, Area 0
  Process ID 1, Router ID 19.19.19.19, Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT, MTU 1500, MaxPktSz 1500
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01:093
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 16
  Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with neighbor 5.5.5.5
```

```
  Suppress hello for 0 neighbor(s) Message digest authentication enabled
 Youngest key id is 1
  Multi-area interface Count is 0
RP/0/0/CPU0:XR1#debug ospf 1 packet GigabitEthernet0/0/0/0.519
Sun Apr 19 20:49:06.944 UTC RP/0/0/CPU0:Apr 19 20:49:29.942 : ospf[1014]: Send: HLO  l:48 rid:19.19.19.19
 aut:2 auk: from 20.5.19.19 to 224.0.0.5 on GigabitEthernet0/0/0/0.519
, vrf default vrfid 0x60000000 RP/0/0/CPU0:Apr 19 20:49:32.162 : ospf[1014]: Recv: HLO  l:48 rid:5.5.5.5
 aut:2 auk: from 20.5.19.5 to 224.0.0.5 on GigabitEthernet0/0/0/0.519
, vrf default vrfid 0x60000000
```

R6 and XR1 have use clear text authentication and are adjacent with each other.

```
R6#show ip ospf interface GigabitEthernet1.619
GigabitEthernet1.619 is up, line protocol is up
  Internet Address 20.6.19.6/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 100
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           100       no          no            Base
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 19.19.19.19, Interface address 20.6.19.19
  Backup Designated router (ID) 6.6.6.6, Interface address 20.6.19.6
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 19.19.19.19  (Designated Router)
  Suppress hello for 0 neighbor(s) Simple password authentication enabled

RP/0/0/CPU0:XR1#show ospf interface GigabitEthernet0/0/0/0.619
Sun Apr 19 20:46:18.715 UTC

GigabitEthernet0/0/0/0.619 is up, line protocol is up
  Internet Address 20.6.19.19/24, Area 0
  Process ID 1, Router ID 19.19.19.19, Network Type BROADCAST, Cost: 100
  Transmit Delay is 1 sec, State DR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 19.19.19.19, Interface address 20.6.19.19
```

```
  Backup Designated router (ID) 6.6.6.6, Interface address 20.6.19.6
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07:113
  Index 3/3, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 6
  Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 6.6.6.6  (Backup Designated Router)
  Suppress hello for 0 neighbor(s) Clear text authentication enabled
  Multi-area interface Count is 0
```

```
RP/0/0/CPU0:XR1#debug ospf 1 packet GigabitEthernet0/0/0/0.619

Sun Apr 19 20:47:28.721 UTC
RP/0/0/CPU0:Apr 19 20:48:01.358 : ospf[1014]: Send: HLO  l:48 rid:19.19.19.19
aut:1 auk:INECLEAR^?^?^? from 20.6.19.19 to 224.0.0.5 on GigabitEthernet0/0/0/0.619
, vrf default vrfid 0x60000000 RP/0/0/CPU0:Apr 19 20:48:01.688 : ospf[1014]: Recv: HLO  l:48 rid:6.6.6.6
aut:1 auk: from 20.6.19.6 to 224.0.0.5 on GigabitEthernet0/0/0/0.619
, vrf default vrfid 0x60000000
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv3

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IPv6**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv6 Diagram** in order to complete this task.

- Using the Base IPv6 Diagram, configure OSPFv3 Area 0 on all interfaces of all devices.
- Statically set the OSPF Router IDs of all devices to be Y.Y.Y.Y, where Y is the router number.

Configuration

```
R1:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
interface Loopback0
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.12
 ipv6 ospf 1 area 0


R2:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 2.2.2.2
!
interface Loopback0
 ipv6 ospf 1 area 0
!
```

```
interface GigabitEthernet1.23
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.24
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.12
 ipv6 ospf 1 area 0


R3:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 3.3.3.3
!
interface Loopback0
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.23
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.34
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.36
 ipv6 ospf 1 area 0


R4:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 4.4.4.4
!
interface Loopback0
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.24
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.34
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.45
 ipv6 ospf 1 area 0
```

```
!
interface GigabitEthernet1.46
 ipv6 ospf 1 area 0


R5:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 5.5.5.5
!
interface Loopback0
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.45
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.56
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.519
 ipv6 ospf 1 area 0


R6:
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 6.6.6.6
!
interface Loopback0
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.36
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.46
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.56
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1.619
 ipv6 ospf 1 area 0
```

```
XR1:
router ospfv3 1
 router-id 19.19.19.19
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0.519
  !
  interface GigabitEthernet0/0/0/0.619
  !
  interface GigabitEthernet0/0/0/0.1920
  !
 !
!

XR2:
router ospfv3 1
 router-id 20.20.20.20
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0.1920
  !
 !
!
```

Verification

Even though it is used to route IPv6 traffic, OSPFv3 uses an IPv4 formatted Router-ID. If there is not an interface in the up/up state with an IPv4 address assigned to it, the OSPFv3 process cannot assign a Router-ID, and cannot start, as seen below. The fix for this is to manually define a Router-ID in the 32-bit dotted decimal format under the OSPFv3 process, similar to OSPFv2.

```
R1(config)#    ipv6 unicast-routing
R1(config)#    !
R1(config)#    interface Loopback0
R1(config-if)#     ipv6 ospf 1 area 0
%OSPFv3-4-NORTRID: Process OSPFv3-1-IPv6 could not pick a router-id, please configure manually

RP/0/0/CPU0:XR1(config)#    router ospfv3 1
RP/0/0/CPU0:XR1(config-ospfv3)#    area 0
RP/0/0/CPU0:XR1(config-ospfv3-ar)#    interface Loopback0
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      !
```

```
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      interface GigabitEthernet0/0/0/0.519
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      !
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      interface GigabitEthernet0/0/0/0.619
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      !
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#      interface GigabitEthernet0/0/0/0.1920
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#commit
Sun Apr 19 22:46:09.003 UTC
RP/0/0/CPU0:Apr 19 22:46:09.123 : ospfv3[1024]: %ROUTING-OSPFv3-5-HA_NOTICE_START : Starting OSPFv3
RP/0/0/CPU0:Apr 19 22:46:09.393 : ospfv3[1024]: %ROUTING-OSPFv3-5-HA_NOTICE : Process 1: OSPFv3 process initializati
RP/0/0/CPU0:Apr 19 22:46:09.423 : ospfv3[1024]: %ROUTING-OSPFv3-5-HA_NOTICE : Process 1: Signaled PROC_AVAILABLE
RP/0/0/CPU0:Apr 19 22:46:13.242 : config[65709]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#end
RP/0/0/CPU0:Apr 19 22:46:22.402 : config[65709]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin
 RP/0/0/CPU0:XR1#RP/0/0/CPU0:Apr 19 22:46:23.112 :
 ospfv3[1024]: %ROUTING-OSPFv3-4-NORTRID : OSPFv3 process 1 could not pick a router-id, please configure manually


RP/0/0/CPU0:XR1#conf t
Sun Apr 19 22:48:24.533 UTC
RP/0/0/CPU0:XR1(config)#    router ospfv3 1 RP/0/0/CPU0:XR1(config-ospfv3)# router-id 19.19.19.19
RP/0/0/CPU0:XR1(config-ospfv3)#commit
Sun Apr 19 22:48:28.003 UTC
RP/0/0/CPU0:Apr 19 22:48:28.183 : config[65709]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR1(config-ospfv3)#eRP/0/0/CPU0:Apr 19 22:48:28.713 :
 ospfv3[1024]: %ROUTING-OSPFv3-5-ADJCHG : Process 1, Nbr 5.5.5.5 on GigabitEthernet0/0/0/0.519 from LOADING to FULL,
  RP/0/0/CPU0:XR1(config-ospfv3)#eRP/0/0/CPU0:Apr 19 22:48:28.713 :
 ospfv3[1024]: %ROUTING-OSPFv3-5-ADJCHG : Process 1, Nbr 6.6.6.6 on GigabitEthernet0/0/0/0.619 from LOADING to FULL,
      RP/0/0/CPU0:XR1(config-ospfv3)#eRP/0/0/CPU0:Apr 19 22:48:28.713 :
 ospfv3[1024]: %ROUTING-OSPFv3-5-ADJCHG : Process 1, Nbr 20.20.20.20 on GigabitEthernet0/0/0/0.1920 from LOADING to F
```

All routers should have OSPFv3 adjacencies with their directly connected neighbors.

```
R6#show ipv6 ospf neighbor

            OSPFv3 Router with ID (6.6.6.6) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
19.19.19.19       1   FULL/BDR        00:00:31    8               GigabitEthernet1.619
5.5.5.5           1   FULL/BDR        00:00:33    12              GigabitEthernet1.56
4.4.4.4           1   FULL/BDR        00:00:38    14              GigabitEthernet1.46
3.3.3.3           1   FULL/BDR        00:00:32    13              GigabitEthernet1.36
```

```
RP/0/0/CPU0:XR1#show ospfv3 neighbor

Sun Apr 19 23:05:06.015 UTC

Neighbors for OSPFv3 1

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
20.20.20.20     1     FULL/BDR        00:00:35    7               GigabitEthernet0/0/0/0.1920
    Neighbor is up for 00:02:55
5.5.5.5         1     FULL/BDR        00:00:33    13              GigabitEthernet0/0/0/0.519
    Neighbor is up for 00:07:38
6.6.6.6         1     FULL/DR         00:00:33    14              GigabitEthernet0/0/0/0.619
    Neighbor is up for 00:03:46

Total neighbor count: 3
```

Since there is only one OSPFv3 area, the database should be identical at all places throughout the topology.

```
R6#show ipv6 ospf database

           OSPFv3 Router with ID (6.6.6.6) (Process ID 1)

               Router Link States (Area 0)

ADV Router       Age         Seq#        Fragment ID  Link count  Bits
1.1.1.1         479         0x80000002  0            1           None
2.2.2.2         468         0x80000004  0            3           None
3.3.3.3         458         0x80000004  0            3           None
4.4.4.4         458         0x80000004  0            4           None
5.5.5.5         446         0x80000004  0            3           None
6.6.6.6         253         0x80000003  0            4           None
19.19.19.19     198         0x80000004  0            3           None
20.20.20.20     199         0x80000002  0            1           None

               Net Link States (Area 0)

ADV Router       Age         Seq#        Link ID    Rtr count
2.2.2.2         478         0x80000001  13         2
3.3.3.3         472         0x80000001  11         2
4.4.4.4         468         0x80000001  11         2
4.4.4.4         468         0x80000001  12         2
5.5.5.5         464         0x80000001  11         2
6.6.6.6         457         0x80000001  11         2
```

```
6.6.6.6         457         0x80000001  12         2
6.6.6.6         457         0x80000001  13         2
6.6.6.6         253         0x80000001  14         2
19.19.19.19     447         0x80000001  7          2
19.19.19.19     198         0x80000001  9          2

               Link (Type-8) Link States (Area 0)

ADV Router       Age         Seq#        Link ID    Interface
6.6.6.6         497         0x80000001  14         Gi1.619
19.19.19.19     256         0x80000001  8          Gi1.619
5.5.5.5         503         0x80000001  12         Gi1.56
6.6.6.6         497         0x80000001  13         Gi1.56
4.4.4.4         507         0x80000001  14         Gi1.46
6.6.6.6         497         0x80000001  12         Gi1.46
3.3.3.3         512         0x80000001  13         Gi1.36
6.6.6.6         497         0x80000001  11         Gi1.36

               Intra Area Prefix Link States (Area 0)

ADV Router       Age         Seq#        Link ID    Ref-lstype  Ref-LSID
1.1.1.1         479         0x80000003  0          0x2001      0
2.2.2.2         468         0x80000005  0          0x2001      0
2.2.2.2         478         0x80000001  13312      0x2002      13
3.3.3.3         458         0x80000005  0          0x2001      0
3.3.3.3         472         0x80000001  11264      0x2002      11
4.4.4.4         458         0x80000005  0          0x2001      0
4.4.4.4         468         0x80000001  11264      0x2002      11
4.4.4.4         468         0x80000001  12288      0x2002      12
5.5.5.5         446         0x80000005  0          0x2001      0
5.5.5.5         464         0x80000001  11264      0x2002      11
6.6.6.6         253         0x80000004  0          0x2001      0
6.6.6.6         457         0x80000001  11264      0x2002      11
6.6.6.6         457         0x80000001  12288      0x2002      12
6.6.6.6         457         0x80000001  13312      0x2002      13
6.6.6.6         253         0x80000001  14336      0x2002      14
19.19.19.19     198         0x80000006  0          0x2001      0
19.19.19.19     447         0x80000001  7168       0x2002      7
19.19.19.19     198         0x80000001  9216       0x2002      9
20.20.20.20     198         0x80000003  0          0x2001      0

RP/0/0/CPU0:XR1#show ospfv3 database

Sun Apr 19 23:06:25.649 UTC

            OSPFv3 Router with ID (19.19.19.19) (Process ID 1)
```

```
                Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
1.1.1.1         533         0x80000002 0            1           None
2.2.2.2         523         0x80000004 0            3           None
3.3.3.3         512         0x80000004 0            3           None
4.4.4.4         511         0x80000004 0            4           None
5.5.5.5         498         0x80000004 0            3           None
6.6.6.6         306         0x80000003 0            4           None
19.19.19.19     249         0x80000004 0            3           None
20.20.20.20     250         0x80000002 0            1           None

                Net Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Rtr count
2.2.2.2         532         0x80000001 13         2
3.3.3.3         528         0x80000001 11         2
4.4.4.4         521         0x80000001 11         2
4.4.4.4         521         0x80000001 12         2
5.5.5.5         515         0x80000001 11         2
6.6.6.6         511         0x80000001 11         2
6.6.6.6         511         0x80000001 12         2
6.6.6.6         511         0x80000001 13         2
6.6.6.6         306         0x80000001 14         2
19.19.19.19     498         0x80000001 7          2
19.19.19.19     249         0x80000001 9          2

                Link (Type-8) Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Interface
19.19.19.19     301         0x80000001 9          Gi0/0/0/0.1920
20.20.20.20     255         0x80000001 7          Gi0/0/0/0.1920
5.5.5.5         555         0x80000001 13         Gi0/0/0/0.519
19.19.19.19     538         0x80000001 7          Gi0/0/0/0.519
6.6.6.6         550         0x80000001 14         Gi0/0/0/0.619
19.19.19.19     308         0x80000001 8          Gi0/0/0/0.619

                Intra Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
1.1.1.1         533         0x80000003 0          0x2001      0
2.2.2.2         523         0x80000005 0          0x2001      0
2.2.2.2         532         0x80000001 13312      0x2002      13
3.3.3.3         512         0x80000005 0          0x2001      0
3.3.3.3         528         0x80000001 11264      0x2002      11
```

```
4.4.4.4         511         0x80000005 0          0x2001      0
4.4.4.4         521         0x80000001 11264      0x2002      11
4.4.4.4         521         0x80000001 12288      0x2002      12
5.5.5.5         498         0x80000005 0          0x2001      0
5.5.5.5         515         0x80000001 11264      0x2002      11
6.6.6.6         306         0x80000004 0          0x2001      0
6.6.6.6         511         0x80000001 11264      0x2002      11
6.6.6.6         511         0x80000001 12288      0x2002      12
6.6.6.6         511         0x80000001 13312      0x2002      13
6.6.6.6         306         0x80000001 14336      0x2002      14
19.19.19.19     249         0x80000006 0          0x2001      0
19.19.19.19     498         0x80000001 7168       0x2002      7
19.19.19.19     249         0x80000001 9216       0x2002      9
20.20.20.20     250         0x80000003 0          0x2001      0
```

All devices should have all IPv6 routes installed.

```
R6#show ipv6 route ospf

IPv6 Routing Table - default - 25 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       a - Application
O   2001::1:1:1:1/128 [110/3]
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001::2:2:2:2/128 [110/2]
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001::3:3:3:3/128 [110/1]
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
O   2001::4:4:4:4/128 [110/1]
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001::5:5:5:5/128 [110/1]
     via FE80::250:56FF:FE9E:962, GigabitEthernet1.56
O   2001::19:19:19:19/128 [110/1]
     via FE80::250:56FF:FE9E:59FE, GigabitEthernet1.619
O   2001::20:20:20:20/128 [110/2]
     via FE80::250:56FF:FE9E:59FE, GigabitEthernet1.619
O   2001:10:1:2::/64 [110/3]
```

```
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
O   2001:10:19:20::/64 [110/2]
     via FE80::250:56FF:FE9E:59FE, GigabitEthernet1.619
O   2001:20:2:3::/64 [110/2]
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
O   2001:20:2:4::/64 [110/2]
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001:20:3:4::/64 [110/2]
     via FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.36
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001:20:4:2::/64 [110/2]
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
O   2001:20:4:5::/64 [110/2]
     via FE80::250:56FF:FE9E:1302, GigabitEthernet1.46
     via FE80::250:56FF:FE9E:962, GigabitEthernet1.56
O   2001:20:5:19::/64 [110/2]
     via FE80::250:56FF:FE9E:962, GigabitEthernet1.56
     via FE80::250:56FF:FE9E:59FE, GigabitEthernet1.619
RP/0/0/CPU0:XR1#show route ipv6 ospf

Sun Apr 19 23:07:27.005 UTC

O    2001::1:1:1:1/128
      [110/4] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/4] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001::2:2:2:2/128
      [110/3] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/3] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001::3:3:3:3/128
      [110/2] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
O    2001::4:4:4:4/128
      [110/2] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/2] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001::5:5:5:5/128
      [110/1] via fe80::250:56ff:fe9e:962, 00:09:18, GigabitEthernet0/0/0/0.519
O    2001::6:6:6:6/128
      [110/1] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
O    2001::20:20:20:20/128
      [110/1] via fe80::250:56ff:fe9e:27ac, 00:05:10, GigabitEthernet0/0/0/0.1920
O    2001:10:1:2::/64
      [110/4] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/4] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001:20:2:3::/64
      [110/3] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
O    2001:20:2:4::/64
```

```
      [110/3] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/3] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001:20:3:4::/64
      [110/3] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/3] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001:20:3:6::/64
      [110/2] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
O    2001:20:4:2::/64
      [110/3] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/3] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
O    2001:20:4:5::/64
      [110/2] via fe80::250:56ff:fe9e:962, 00:09:18, GigabitEthernet0/0/0/0.519
O    2001:20:4:6::/64
      [110/2] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
O    2001:20:5:6::/64
      [110/2] via fe80::250:56ff:fe9e:5cec, 00:06:06, GigabitEthernet0/0/0/0.619
      [110/2] via fe80::250:56ff:fe9e:962, 00:06:06, GigabitEthernet0/0/0/0.519
```

All devices should have full IP reachability to each other.

```
R1#ping 2001::20:20:20:20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20:20:20:20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/20/23 ms

R1#traceroute 2001::20:20:20:20
Type escape sequence to abort.
Tracing the route to 2001::20:20:20:20

  1 2001:10:1:2::2 16 msec 2 msec 1 msec
  2 2001:20:2:4::4 2 msec 2 msec 1 msec
  3 2001:20:4:5::5 14 msec 15 msec 14 msec
  4 2001:20:5:19::19 23 msec 6 msec 14 msec
  5 2001::20:20:20:20 107 msec 18 msec 20 msec

RP/0/0/CPU0:XR2#ping 2001::1:1:1:1
Sun Apr 19 23:09:35.697 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/15/19 ms

RP/0/0/CPU0:XR2#traceroute 2001::1:1:1:1
```

```
Sun Apr 19 23:09:13.728 UTC

Type escape sequence to abort.
Tracing the route to 2001::1:1:1:1

 1  2001:10:19:20::19 19 msec 9 msec 9 msec
 2  2001:20:5:19::5 9 msec 9 msec 9 msec
 3  2001:20:4:5::4 9 msec 9 msec 9 msec
 4  2001:20:4:2::2 9 msec 9 msec 9 msec
 5  2001:10:1:2::12 9 msec 19 msec 9 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv3 Network Types

- Change the OSPF Network Type of the link between R5 and XR1 to Point-to-Point.

Configuration

```
R5:
interface GigabitEthernet1.519
 ipv6 ospf network point-to-point

XR1:
router ospfv3 1
 area 0
 interface GigabitEthernet0/0/0/0.519
  network point-to-point
  !
 !
!
```

Verification

XR1 now runs OSPF Network Type Point-to-Point on the Ethernet link to R5, while still running the default Network Type Broadcast on the Ethernet link to R6.

```
RP/0/0/CPU0:XR1#show ospfv3 interface | include "line protocol|Network Type"
Tue Apr 21 21:52:55.944 UTC
GigabitEthernet0/0/0/0.519 is up, line protocol is up Network Type POINT_TO_POINT, Cost: 1
GigabitEthernet0/0/0/0.619 is up, line protocol is up Network Type BROADCAST, Cost: 1

GigabitEthernet0/0/0/0.1920 is up, line protocol is up
  Network Type BROADCAST, Cost: 1
Loopback0 is up, line protocol is up
  Network Type LOOPBACK, Cost: 0
```

Like in OSPFv2, changing Ethernet links that connect only two routers together to Network Type Point-to-Point removes the need for the Network LSA (LSA Type 2) that is generated by the Designated Router. This both simplifies the SPF lookup in the database and makes the size of the database smaller. As seen below, a Network LSA is generated for all Ethernet links with the exception of the link between R5 and XR1.

```
RP/0/0/CPU0:XR1#show ospfv3 database

Tue Apr 21 21:53:53.700 UTC

            OSPFv3 Router with ID (19.19.19.19) (Process ID 1)

            Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
1.1.1.1         151         0x80000002 0            1           None
2.2.2.2         137         0x80000004 0            3           None
3.3.3.3         118         0x80000004 0            3           None
4.4.4.4         78          0x80000004 0            4           None
5.5.5.5         60          0x80000006 0            3           None
6.6.6.6         76          0x80000003 0            4           None
19.19.19.19     68          0x8000005f 0            3           None
20.20.20.20     1938        0x80000055 0            1           None

            Net Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Rtr count
2.2.2.2         150         0x80000001 13         2
3.3.3.3         147         0x80000001 11         2
3.3.3.3         118         0x80000001 13         2
4.4.4.4         136         0x80000001 11         2
4.4.4.4         136         0x80000001 12         2
4.4.4.4         123         0x80000001 13         2
6.6.6.6         76          0x80000001 12         2
6.6.6.6         76          0x80000001 13         2
19.19.19.19     115         0x80000001 8          2
19.19.19.19     1775        0x80000054 9          2

            Link (Type-8) Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Interface
19.19.19.19     1775        0x80000054 9          Gi0/0/0/0.1920
20.20.20.20     1938        0x80000054 7          Gi0/0/0/0.1920
5.5.5.5         121         0x80000001 13         Gi0/0/0/0.519
19.19.19.19     68          0x80000055 7          Gi0/0/0/0.519
```

```
6.6.6.6         116         0x80000001 14         Gi0/0/0/0.619
19.19.19.19     1775        0x80000054 8          Gi0/0/0/0.619

            Intra Area Prefix Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
1.1.1.1         151         0x80000003 0          0x2001      0
2.2.2.2         137         0x80000005 0          0x2001      0
2.2.2.2         150         0x80000001 13312      0x2002      13
3.3.3.3         118         0x80000005 0          0x2001      0
3.3.3.3         147         0x80000001 11264      0x2002      11
3.3.3.3         118         0x80000001 13312      0x2002      13
4.4.4.4         78          0x80000005 0          0x2001      0
4.4.4.4         136         0x80000001 11264      0x2002      11
4.4.4.4         136         0x80000001 12288      0x2002      12
4.4.4.4         123         0x80000001 13312      0x2002      13
5.5.5.5         77          0x80000002 0          0x2001      0
6.6.6.6         76          0x80000002 0          0x2001      0
6.6.6.6         76          0x80000001 12288      0x2002      12
6.6.6.6         76          0x80000001 13312      0x2002      13
19.19.19.19     69          0x80000060 0          0x2001      0
19.19.19.19     115         0x80000001 8192       0x2002      8
19.19.19.19     1775        0x80000054 9216       0x2002      9
20.20.20.20     1938        0x80000056 0          0x2001      0
```

XR1 continues generating a Network LSA for the Broadcast or Non- Broadcast Network Type links on which it is the DR.

```
RP/0/0/CPU0:XR1#show ospfv3 database network adv-router 19.19.19.19
Tue Apr 21 21:54:34.157 UTC

            OSPFv3 Router with ID (19.19.19.19) (Process ID 1)

            Net Link States (Area 0)

  LS age: 155
  Options: (V6-Bit E-Bit R-Bit DC-Bit)
  LS Type: Network Links Link State ID: 8 (Interface ID of Designated Router)
Advertising Router: 19.19.19.19
  LS Seq Number: 80000001
  Checksum: 0x1a36
  Length: 32
      Attached Router: 19.19.19.19
      Attached Router: 6.6.6.6
```

```
  LS age: 1816
  Options: (V6-Bit E-Bit R-Bit DC-Bit)
  LS Type: Network Links Link State ID: 9 (Interface ID of Designated Router)
 Advertising Router: 19.19.19.19

  LS Seq Number: 80000054
  Checksum: 0x289b
  Length: 32
      Attached Router: 19.19.19.19
      Attached Router: 20.20.20.20
```

R6 is the DR for its links to R5 and R4, therefore it generates a Network LSA for each of these.

```
RP/0/0/CPU0:XR1#show ospfv3 database network adv-router 6.6.6.6

Tue Apr 21 21:55:29.083 UTC

            OSPFv3 Router with ID (19.19.19.19) (Process ID 1)

            Net Link States (Area 0)

  LS age: 171
  Options: (V6-Bit E-Bit R-Bit DC-Bit)
  LS Type: Network Links Link State ID: 12 (Interface ID of Designated Router)
 Advertising Router: 6.6.6.6
  LS Seq Number: 80000001
  Checksum: 0x5963
  Length: 32
      Attached Router: 6.6.6.6
      Attached Router: 4.4.4.4

  LS age: 171
  Options: (V6-Bit E-Bit R-Bit DC-Bit)
  LS Type: Network Links Link State ID: 13 (Interface ID of Designated Router)
 Advertising Router: 6.6.6.6

  LS Seq Number: 80000001
  Checksum: 0x8136
  Length: 32
      Attached Router: 6.6.6.6
      Attached Router: 5.5.5.5
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv3 Path Selection

- Change the OSPF cost on the link between R6 and XR1 so that bidirectional traffic between R1 and XR2 prefers to use the link between R5 and XR1.

Configuration

```
R6:
interface GigabitEthernet1.619
 ipv6 ospf cost 100

XR1:
router ospfv3 1
 area 0
  interface GigabitEthernet0/0/0/0.619
   cost 100
  !
 !
!
```

Verification

With the higher cost value of 100, the link between R6 and XR1 will be the less preferred path through the network.

```
R6#show ipv6 ospf interface | include line protocol|Cost
Loopback0 is up, line protocol is up
  Network Type LOOPBACK, Cost: 1 GigabitEthernet1.619
 is up, line protocol is up    Network Type BROADCAST, Cost: 100
GigabitEthernet1.56 is up, line protocol is up
  Network Type BROADCAST, Cost: 1
GigabitEthernet1.46 is up, line protocol is up
  Network Type BROADCAST, Cost: 1
GigabitEthernet1.36 is up, line protocol is up
  Network Type BROADCAST, Cost: 1
```

```
RP/0/0/CPU0:XR1#show ospfv3 interface | include "line protocol|Cost"

Tue Apr 21 22:04:52.605 UTC
GigabitEthernet0/0/0/0.519 is up, line protocol is up
  Network Type POINT_TO_POINT, Cost: 1 GigabitEthernet0/0/0/0.619
 is up, line protocol is up  Network Type BROADCAST, Cost: 100

GigabitEthernet0/0/0/0.1920 is up, line protocol is up
  Network Type BROADCAST, Cost: 1
Loopback0 is up, line protocol is up
  Network Type LOOPBACK, Cost: 0
```

The result of this cost change is that traffic avoids the link between R6 and XR1 due to its higher cost value and instead uses the link between R5 and XR1.

```
R1#traceroute 2001::20:20:20:20

Type escape sequence to abort.
Tracing the route to 2001::20:20:20:20

  1 2001:10:1:2::2 11 msec 2 msec 1 msec
  2 2001:20:2:4::4 2 msec 1 msec 3 msec
  3 2001:20:4:5::5 14 msec 15 msec 14 msec 4 2001:20:5:19::19 17 msec 12 msec 14 msec
  5 2001::20:20:20:20 26 msec 16 msec 16 msec
RP/0/0/CPU0:XR2#traceroute 2001::1:1:1:1
Tue Apr 21 22:12:18.445 UTC

Type escape sequence to abort.
Tracing the route to 2001::1:1:1:1

 1  2001:10:19:20::19 19 msec 9 msec 9 msec
 2  2001:20:5:19::5 9 msec 9 msec 9 msec 3  2001:20:4:5::4 9 msec 9 msec 9 msec

 4  2001:20:4:2::2 19 msec 19 msec 39 msec
 5  2001:10:1:2::12 49 msec 19 msec 19 msec
```

Note that depending on the ECMP hashing done by the routers making forwarding decisions, the path prior to making the metric change could have also been traversing the R5-XR1 link.

```
RP/0/0/CPU0:XR1(config)# router ospfv3 1
RP/0/0/CPU0:XR1(config-ospfv3)#  area 0
RP/0/0/CPU0:XR1(config-ospfv3-ar)#  interface GigabitEthernet0/0/0/0.619
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)# no cost 100
RP/0/0/CPU0:XR1(config-ospfv3-ar-if)#commit
```

```
R6(config)# interface GigabitEthernet1.619
R6(config-subif)#  no ipv6 ospf cost 100
```

With the costs reset to their default values, XR1 uses two equal cost paths to reach R1. Depending on the input to the ECMP hash function (L3-L4 headers), XR1 could forward packets towards R5. Both of the available paths are marked as "path-idx 0" and "path-idx 1". This index corresponds to the output of the hash, as can be gleaned from the bottom section of the show command.

```
RP/0/0/CPU0:XR1#show cef ipv6 2001::1:1:1:1/128 detail

Tue Apr 21 22:17:21.263 UTC 2001::1:1:1:1/128
, version 348, internal 0x4000001 0x0 (ptr 0xa0ef6a74) [1], 0x0 (0xa0ec17e8), 0x0 (0x0)
 Updated Apr 21 22:08:42.779
 local adjacency fe80::250:56ff:fe9e:962
 Prefix Len 128, traffic index 0, precedence n/a, priority 1
  gateway array (0xa0d4a220) reference count 8, flags 0x0, source rib (6), 0 backups
                [9 type 3 flags 0x8081 (0xa0e0b8fc) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0xa0ec17e8, sh-ldi=0xa0e0b8fc]
 via fe80::250:56ff:fe9e:962, GigabitEthernet0/0/0/0.519
, 7 dependencies, weight 0, class 0 [flags 0x0] path-idx 0
 NHID 0x0 [0xa15842c4 0x0]
    next hop fe80::250:56ff:fe9e:962
    tx adjacency via fe80::250:56ff:fe9e:5cec, GigabitEthernet0/0/0/0.619
, 7 dependencies, weight 0, class 0 [flags 0x0] path-idx 1
 NHID 0x0 [0xa1584248 0x0]
    next hop fe80::250:56ff:fe9e:5cec
    tx adjacency



    Load distribution: 0 1 (refcount 9)
 Hash
  OK  Interface                 Address 0      Y   GigabitEthernet0/0/0/0.519 fe80::250:56ff:fe9e:962
 1      Y   GigabitEthernet0/0/0/0.619 fe80::250:56ff:fe9e:5cec
```

The hash function can be tested by providing inputs as shown below:

```
RP/0/0/CPU0:XR1#show cef ipv6 exact-route 2001::20:20:20:20 2001::1:1:1:1 protocol icmp ingress-interface GigabitEth

Tue Apr 21 22:19:54.073 UTC 2001::1:1:1:1/128
, version 348, internal 0x4000001 0x0 (ptr 0xa0ef6a74) [1], 0x0 (0xa0ec17e8), 0x0 (0x0)
 Updated Apr 21 22:08:42.779
```

```
 local adjacency fe80::250:56ff:fe9e:962
 Prefix Len 128, traffic index 0, precedence n/a, priority 1 via GigabitEthernet0/0/0/0.519
 via fe80::250:56ff:fe9e:962, GigabitEthernet0/0/0/0.519
, 7 dependencies, weight 0, class 0 [flags 0x0] path-idx 0
 NHID 0x0 [0xa15842c4 0x0]
    next hop fe80::250:56ff:fe9e:962
    tx adjacency
```

Note that the output of the hash function changes as the inputs change:

```
RP/0/0/CPU0:XR1#show cef ipv6 exact-route 2FF1::100:1:1 2001::1:1:1:1
Tue Apr 21 22:22:48.671 UTC 2001::1:1:1:1/128
, version 348, internal 0x4000001 0x0 (ptr 0xa0ef6a74) [1], 0x0 (0xa0ec17e8), 0x0 (0x0)
 Updated Apr 21 22:08:42.779
 local adjacency fe80::250:56ff:fe9e:5cec
 Prefix Len 128, traffic index 0, precedence n/a, priority 1 via GigabitEthernet0/0/0/0.619
 via fe80::250:56ff:fe9e:5cec, GigabitEthernet0/0/0/0.619
, 7 dependencies, weight 0, class 0 [flags 0x0] path-idx 1
 NHID 0x0 [0xa1584248 0x0]
    next hop fe80::250:56ff:fe9e:5cec
    tx adjacency
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv3 BFD

- Configure BFD for OSPF between R2 and R3 so that if these is a failure of the link between them they begin reconvergence in less than one second.

Configuration

> Note: BFD for IPv6 is not supported in IOS XR until software release 4.1. Additionally, BFD is not supported on the current releases of XRv.

```
R2:
interface GigabitEthernet1.23
ipv6 ospf bfd
bfd interval 250 min_rx 250 multiplier 3

R3:
interface GigabitEthernet1.23
ipv6 ospf bfd
bfd interval 250 min_rx 250 multiplier 3
```

Verification

R2 and R3 are BFD adjacent for OSPFv3.

```
R2#show bfd neighbors detail

IPv6 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
FE80::250:56FF:FE9E:6E6A                1/1          Up        Up        Gi1.23
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: FE80::250:56FF:FE9E:35D1
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 250000, MinRxInt: 250000, Multiplier: 3
```

```
Received MinRxInt: 250000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 250(0)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0
Tx Count: 0, Tx Interval (ms) min/max/avg: 0/0/0
Elapsed time watermarks: 0 0 (last: 0) Registered protocols: OSPFv3 CEF

Uptime: 00:00:09
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 1                - Your Discr.: 1
             Min tx interval: 250000     - Min rx interval: 250000
             Min Echo interval: 0
```

R2 disables its link connecting to R3 at timestamp 18:33:16.657.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#service timestamps log datetime msec
R2(config)#int Gig1.23 R2(config-subif)#shutdown
R2(config-subif)#*Apr 23 18:33:16.657 : %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on GigabitEthernet1.23
 from FULL to DOWN, Neighbor Down
: Interface down or detached
R2(config-subif)#
```

R3 detects this via BFD at timestamp 18:33:17.330 and declares the OSPFv3 neighbor down, meeting the requirement to begin reconvergence within 1 second.

```
R3# *Apr 23 18:33:17.330 : %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet1.23
 from FULL to DOWN, Neighbor Down: BFD node down
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

OSPFv3 Encryption and Authentication

- Configure OSPFv3 IPsec ESP Encryption and Authentication between XR1 and XR2 using the following parameters:
  - Use Security Parameter Index (SPI) 1920
  - Use ESP with AES 256-bit Encryption and SHA1 Authentication
  - For the AES encryption key use 0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
  - For the SHA authentication key 0x0123456789012345678901234567890123456789

Configuration

> OSPFv3 IPsec ESP Encryption and Authentication is not supported in regular IOS until software release 12.4(9)T

```
XR1:
router ospfv3 1
 area 0
  interface GigabitEthernet0/0/0/0.1920
   encryption ipsec spi 1920 esp aes 256
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef authentication
sha1 0123456789012345678901234567890123456789
  !
 !
!

XR2:
router ospfv3 1
 area 0
  interface GigabitEthernet0/0/0/0.1920
   encryption ipsec spi 1920 esp aes 256
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef authentication
sha1 0123456789012345678901234567890123456789
  !
```

```
 !
!
```

Verification

XR1 and XR2 are running ESP encryption and authentication for OSPFv3 on the link connecting them, and they are OSPFv3 adjacent.

```
RP/0/0/CPU0:XR1#show ospfv3 interface GigabitEthernet0/0/0/0.1920
Thu Apr 23 18:47:36.318 UTC

GigabitEthernet0/0/0/0.1920 is up, line protocol is up, ipsec is up
  Link Local address fe80::250:56ff:fe9e:59fe, Interface ID 9
  Area 0, Process ID 1, Instance ID 0, Router ID 19.19.19.19
  Network Type BROADCAST, Cost: 1 ESP Encryption AES-256, Authentication SHA1, SPI 1920
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 20.20.20.20, local address fe80::250:56ff:fe9e:27ac
  Backup Designated router (ID) 19.19.19.19, local address fe80::250:56ff:fe9e:59fe
  Flush timer for old DR LSA due in 00:00:33
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 0/4/1, flood queue length 0
  Next 0(0)/0(0)/0(0)
  Last flood scan length is 1, maximum is 20
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 20.20.20.20  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Reference count is 5

RP/0/0/CPU0:XR2#show ospfv3 interface GigabitEthernet0/0/0/0.1920
Thu Apr 23 18:47:57.987 UTC

GigabitEthernet0/0/0/0.1920 is up, line protocol is up, ipsec is up
  Link Local address fe80::250:56ff:fe9e:27ac, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 20.20.20.20
  Network Type BROADCAST, Cost: 1 ESP Encryption AES-256, Authentication SHA1, SPI 1920
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 20.20.20.20, local address fe80::250:56ff:fe9e:27ac
  Backup Designated router (ID) 19.19.19.19, local address fe80::250:56ff:fe9e:59fe
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 0/2/1, flood queue length 0
  Next 0(0)/0(0)/0(0)
```

```
  Last flood scan length is 1, maximum is 14
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 19.19.19.19  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Reference count is 37

RP/0/0/CPU0:XR1#show ospfv3 neighbor


Thu Apr 23 18:56:49.190 UTC


Neighbors for OSPFv3 1


Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
20.20.20.20     1     FULL/DR         00:00:39    7               GigabitEthernet0/0/0/0.1920
    Neighbor is up for 00:11:38
5.5.5.5         1     FULL/  -        00:00:33    13              GigabitEthernet0/0/0/0.519
    Neighbor is up for 00:11:39
6.6.6.6         1     FULL/DR         00:00:36    14              GigabitEthernet0/0/0/0.619
    Neighbor is up for 00:11:39


Total neighbor count: 3
RP/0/0/CPU0:XR2#show ospfv3 neighbor
Thu Apr 23 18:56:26.292 UTC


Neighbors for OSPFv3 1


Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
19.19.19.19     1     FULL/BDR        00:00:38    9               GigabitEthernet0/0/0/0.1920


    Neighbor is up for 00:11:15


Total neighbor count: 1
```

Notice that one hop IPSec tunnels have been created between XR1 and XR2. The IPSec tunnel is encrypting the OSPFv3 traffic. The transform set is using AES 256 bit with SHA1 for hashing. The SA type is shown as manual, as all the keys were entered manually (no ISAKAMP stage).

```
RP/0/0/CPU0:XR1#show crypto ipsec sa


Thu Apr 23 18:58:30.933 UTC


SA id:          2
Node id:        0/0/CPU0 SA Type:        MANUAL
```

```
SA State:       UP
Ref Count:      1
outbound esp sas:  spi: 0x780(1920)
 transform: esp-256-aes esp-sha-hmac
        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
inbound esp sas:  spi: 0x780(1920)
 transform: esp-256-aes esp-sha-hmac

        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

Single-Level IS-IS

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IPv4**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Using the Base IPv4 Diagram, configure IS-IS Level 2 on all interfaces of all devices.
- Use NET addresses in the format 49.0001.0000.0000.000Y.00, where Y is the router number.
- Advertise the Loopback interfaces of the routers using the **passive-interface** or **passive** command.

Configuration

```
R1:
interface GigabitEthernet1.12
 ip router isis
!
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
 passive-interface Loopback0

R2:
interface GigabitEthernet1.23
 ip router isis
!
interface GigabitEthernet1.24
ip router isis
!
interface GigabitEthernet1.12
 ip router isis
!
router isis
 net 49.0001.0000.0000.0002.00
```

```
 is-type level-2-only
 passive-interface Loopback0

R3:
interface GigabitEthernet1.23
 ip router isis
!
interface GigabitEthernet1.34
 ip router isis
!
interface GigabitEthernet1.36
 ip router isis
!
router isis
 net 49.0001.0000.0000.0003.00
 is-type level-2-only
 passive-interface Loopback0

R4:
interface GigabitEthernet1.24
 ip router isis
!
interface GigabitEthernet1.34
 ip router isis
!
interface GigabitEthernet1.45
 ip router isis
!
interface GigabitEthernet1.46
 ip router isis
!
router isis
 net 49.0001.0000.0000.0004.00
 is-type level-2-only
 passive-interface Loopback0

R5:
interface GigabitEthernet1.45
 ip router isis
!
interface GigabitEthernet1.56
 ip router isis
!
interface GigabitEthernet1.519
 ip router isis
!
```

```
router isis
 net 49.0001.0000.0000.0005.00
 is-type level-2-only
 passive-interface Loopback0

R6:
interface GigabitEthernet1.36
 ip router isis
!
interface GigabitEthernet1.46
 ip router isis
!
interface GigabitEthernet1.56
 ip router isis
!
interface GigabitEthernet1.619
 ip router isis
!
router isis
 net 49.0001.0000.0000.0006.00
 is-type level-2-only
 passive-interface Loopback0

XR1:
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
!
interface GigabitEthernet0/0/0/0.519
  address-family ipv4 unicast
  !
!
interface GigabitEthernet0/0/0/0.619
  address-family ipv4 unicast
  !
!
interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 unicast
  !
 !
!
```

```
XR2:
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 unicast
  !
 !
!
```

Verification

All devices should have Level 2 IS-IS adjacencies with their directly connected neighbors.

```
R6#show isis neighbors

System Id      Type Interface    IP Address      State Holdtime Circuit Id
R3             L2   Gi1.36       20.3.6.3        UP    8        R3.03
R4             L2   Gi1.46       20.4.6.4        UP    26       R6.02
R5             L2   Gi1.56       20.5.6.5        UP    20       R6.03
XR1            L2   Gi1.619      20.6.19.19      UP    24       R6.04

RP/0/0/CPU0:XR1#show isis adjacency

Thu Apr 23 19:21:47.737 UTC

IS-IS 1 Level-2 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
R6             Gi0/0/0/0.619    0050.569e.5cec Up    7    00:02:12 Yes None None
R5             Gi0/0/0/0.519    0050.569e.0962 Up    22   00:02:12 Yes None None
XR2            Gi0/0/0/0.1920   0050.569e.27ac Up    28   00:01:21 Yes None None

Total adjacency count: 3
```

All devices should have identical Link State Databases, with a single LSP generated by all routers in addition to a Pseudo Node LSP generated for each Ethernet segment. This behavior is similar to how the OSPF Designated Router originates a Network LSA (LSA Type 2) for segments running OSPF Network Type Broadcast.

```
R6#show isis database



IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000003   0x29C1        782               0/0/0
R1.01-00              0x00000001   0x21B9        783               0/0/0
R2.00-00              0x00000005   0x1535        796               0/0/0
R2.02-00              0x00000001   0x5283        797               0/0/0
R3.00-00              0x00000007   0xE443        860               0/0/0
R3.01-00              0x00000001   0x2DA9        789               0/0/0
R3.02-00              0x00000001   0x587B        795               0/0/0
R3.03-00              0x00000002   0x814E        860               0/0/0
R4.00-00              0x00000007   0x2C1D        859               0/0/0
R4.03-00              0x00000001   0x705F        803               0/0/0
R5.00-00              0x00000007   0xC914        1024              0/0/0
R6.00-00            * 0x00000007   0xDE36        1025              0/0/0
R6.02-00            * 0x00000002   0x6864        861               0/0/0
R6.03-00            * 0x00000002   0x7A50        862               0/0/0
R6.04-00            * 0x00000001   0x6B4B        1026              0/0/0
XR1.00-00             0x00000004   0x67E4        1073              0/0/0
XR1.01-00             0x00000001   0xA2E9        1073              0/0/0
XR1.05-00             0x00000001   0xE0C2        1027              0/0/0
XR2.00-00             0x00000003   0xEF2B        1079              0/0/0

RP/0/0/CPU0:XR1#show isis database

Thu Apr 23 19:22:44.274 UTC

IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00              0x00000003   0x29c1        770             0/0/0
R1.01-00              0x00000001   0x21b9        771             0/0/0
R2.00-00              0x00000005   0x1535        784             0/0/0
R2.02-00              0x00000001   0x5283        785             0/0/0
R3.00-00              0x00000007   0xe443        844             0/0/0
R3.01-00              0x00000001   0x2da9        777             0/0/0
R3.02-00              0x00000001   0x587b        783             0/0/0
R3.03-00              0x00000002   0x814e        844             0/0/0
R4.00-00              0x00000007   0x2c1d        845             0/0/0
R4.03-00              0x00000001   0x705f        791             0/0/0
R5.00-00              0x00000007   0xc914        1016            0/0/0
R6.00-00              0x00000007   0xde36        1016            0/0/0
```

```
R6.02-00              0x00000002   0x6864        843            0/0/0
R6.03-00              0x00000002   0x7a50        846            0/0/0
R6.04-00              0x00000001   0x6b4b        1016           0/0/0
XR1.00-00           * 0x00000004   0x67e4        1061           0/0/0
XR1.01-00             0x00000001   0xa2e9        1061           0/0/0
XR1.05-00             0x00000001   0xe0c2        1017           0/0/0
XR2.00-00             0x00000003   0xef2b        1068           0/0/0

 Total Level-2 LSP count: 19     Local Level-2 LSP count: 1
```

All devices should have L2 routes to every segment in the topology.

```
R1#show ip route isis

Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
i L2     2.2.2.2 [115/10] via 10.1.2.2, 00:07:20, GigabitEthernet1.12
      3.0.0.0/32 is subnetted, 1 subnets
i L2     3.3.3.3 [115/20] via 10.1.2.2, 00:07:20, GigabitEthernet1.12
      4.0.0.0/32 is subnetted, 1 subnets
i L2     4.4.4.4 [115/20] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
      5.0.0.0/32 is subnetted, 1 subnets
i L2     5.5.5.5 [115/30] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
      6.0.0.0/32 is subnetted, 1 subnets
i L2     6.6.6.6 [115/30] via 10.1.2.2, 00:06:11, GigabitEthernet1.12
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
i L2     10.19.20.0/24 [115/50] via 10.1.2.2, 00:03:28, GigabitEthernet1.12
      19.0.0.0/32 is subnetted, 1 subnets
i L2     19.19.19.19 [115/40] via 10.1.2.2, 00:03:28, GigabitEthernet1.12
      20.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
i L2     20.2.3.0/24 [115/20] via 10.1.2.2, 00:07:20, GigabitEthernet1.12
i L2     20.2.4.0/24 [115/20] via 10.1.2.2, 00:07:20, GigabitEthernet1.12
i L2     20.3.4.0/24 [115/30] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
i L2     20.3.6.0/24 [115/30] via 10.1.2.2, 00:07:20, GigabitEthernet1.12
```

```
i L2     20.4.5.0/24 [115/30] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
i L2     20.4.6.0/24 [115/30] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
i L2     20.5.6.0/24 [115/40] via 10.1.2.2, 00:06:11, GigabitEthernet1.12
i L2     20.5.19.0/24 [115/40] via 10.1.2.2, 00:07:10, GigabitEthernet1.12
i L2     20.6.19.0/24 [115/40] via 10.1.2.2, 00:06:11, GigabitEthernet1.12
i L2     20.20.20.20/32 [115/50] via 10.1.2.2, 00:02:39, GigabitEthernet1.12
RP/0/0/CPU0:XR2#show route ipv4 isis

Thu Apr 23 19:23:33.001 UTC

i L2 1.1.1.1/32 [115/50] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 2.2.2.2/32 [115/40] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 3.3.3.3/32 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 4.4.4.4/32 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 5.5.5.5/32 [115/20] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 6.6.6.6/32 [115/20] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 10.1.2.0/24 [115/50] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 19.19.19.19/32 [115/10] via 10.19.20.19, 00:03:01, GigabitEthernet0/0/0/0.1920
i L2 20.2.3.0/24 [115/40] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.2.4.0/24 [115/40] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.3.4.0/24 [115/40] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.3.6.0/24 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.4.5.0/24 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.4.6.0/24 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.5.6.0/24 [115/30] via 10.19.20.19, 00:02:55, GigabitEthernet0/0/0/0.1920
i L2 20.5.19.0/24 [115/20] via 10.19.20.19, 00:03:01, GigabitEthernet0/0/0/0.1920
i L2 20.6.19.0/24 [115/20] via 10.19.20.19, 00:03:01, GigabitEthernet0/0/0/0.1920
```

All devices should have full reachability to all other devices in the topology.

```
R1#ping 20.20.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/10 ms

    R1#traceroute 20.20.20.20
    Type escape sequence to abort.
    Tracing the route to 20.20.20.20
    VRF info: (vrf in name/id, vrf out name/id)
      1 10.1.2.2 4 msec 1 msec 1 msec
      2 20.2.3.3 6 msec 2 msec 1 msec
      3 20.3.6.6 1 msec 1 msec 1 msec
      4 20.6.19.19 10 msec 12 msec 13 msec
      5 10.19.20.20 13 msec *  3 msec
```

```
RP/0/0/CPU0:XR2#ping 1.1.1.1

Thu Apr 23 19:24:27.227 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

RP/0/0/CPU0:XR2#traceroute 1.1.1.1

Thu Apr 23 19:24:31.847 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.4.5.4 0 msec  0 msec  0 msec
 4  20.2.4.2 0 msec  0 msec  0 msec
 5  10.1.2.1 39 msec  *  0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

IS-IS Network Types

- Change the IS-IS Network Type of the link between R5 and XR1 to Point-to-Point.

Configuration

```
R5:
interface GigabitEthernet1.519
 isis network point-to-point

XR1:
router isis 1
 interface GigabitEthernet0/0/0/0.519
  point-to-point
  !
 !
!
```

Verification

Prior to changing the IS-IS Network Type, R5 and XR1 generate L2 LAN Hellos on the Ethernet link connecting them.

```
R5#debug isis adj-packets GigabitEthernet1.519

IS-IS Adjacency related packets debugging is on for router process null
R5# ISIS-Adj:
Rec L2 IIH from 0050.569e.59fe (GigabitEthernet1.519), cir type L2, cir id 0000.0000.0019.05
, length 1497, ht(10)
ISIS-Adj: he_knows_us 1, old state 0, new state 0, level 2
R5#
ISIS-Adj: Rec L2 IIH from 0050.569e.59fe (GigabitEthernet1.519), cir type L2, cir id 0000.0000.0019.05, length 1497,
ISIS-Adj: he_knows_us 1, old state 0, new state 0, level 2
R5#
ISIS-Adj: Rec L2 IIH from 0050.569e.59fe (GigabitEthernet1.519), cir type L2, cir id 0000.0000.0019.05, length 1497,
ISIS-Adj: he_knows_us 1, old state 0, new state 0, level 2
```

```
ISIS-Adj: Sending L2 LAN IIH on GigabitEthernet1.519
, length 1497
R5#
ISIS-Adj: Rec L2 IIH from 0050.569e.59fe (GigabitEthernet1.519), cir type L2, cir id 0000.0000.0019.05, length 1497,
ISIS-Adj: he_knows_us 1, old state 0, new state 0, level 2
```

While running the default Network Type of Broadcast, a Pseudo Node LSP is generated by the Designated Intermediate System (DIS) on the link between R5 and XR1. In this case R5 was elected the DIS.

```
RP/0/0/CPU0:XR1#show isis database XR1.05-00 detail


Thu Apr 23 21:48:01.046 UTC


IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
XR1.05-00             0x0000000c   0xcacd        848             0/0/0
  Metric: 0          IS XR1.00
  Metric: 0          IS R5.00
```

Once the Network Type is changed to Point-to-Point, R5 and XR1 generate P2P Hellos, and there is no DIS election nor Pseudo Node LSP for the segment between them. Like in OSPF this helps reduce the size of the database and simplifies the SPF calculation for links that are broadcast (e.g. Ethernet) but only have two routers on them.

```
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#    interface GigabitEthernet1.519R5(config-subif)#     isis network point-to-point
R5(config-subif)#
RP/0/0/CPU0:XR1#conf t
Thu Apr 23 21:48:57.943 UTC
RP/0/0/CPU0:XR1(config)#    router isis 1
RP/0/0/CPU0:XR1(config-isis)#     interface GigabitEthernet0/0/0/0.519
RP/0/0/CPU0:XR1(config-isis-if)#      point-to-point


RP/0/0/CPU0:XR1(config-isis-if)#      !
RP/0/0/CPU0:XR1(config-isis-if)#commit
Thu Apr 23 21:49:00.562 UTC
```

The Circuit ID of 00 means that there is no DIS on the segment, and hence the Network Type is Point-to-Point.

```
R5#show isis neighbors



System Id      Type Interface    IP Address      State Holdtime Circuit Id
R4             L2   Gi1.45       20.4.5.4        UP    9        R4.03
R6             L2   Gi1.56       20.5.6.6        UP    9        R6.03
XR1            L2   Gi1.519      20.5.19.19      UP    25       00
RP/0/0/CPU0:XR1#show isis adjacency
Thu Apr 23 21:51:01.564 UTC

IS-IS 1 Level-2 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
R6             Gi0/0/0/0.619    0050.569e.5cec Up    6    02:31:25 Yes None None
R5             Gi0/0/0/0.519    *PtoP*         Up    26   00:01:51 Yes None None


XR2            Gi0/0/0/0.1920   0050.569e.27ac Up    24   02:30:35 Yes None None


Total adjacency count: 3
```

R5 now sends and receives Serial (Point-to-Point) Hellos on the segment to XR1.

```
R5#debug isis adj-packets GigabitEthernet1.519

IS-IS Adjacency related packets debugging is on for router process null
R5#
ISIS-Adj: Sending serial IIH on GigabitEthernet1.519, 3way state:UP, length 1496
R5#
ISIS-Adj: Rec serial IIH from 0050.569e.59fe (GigabitEthernet1.519), cir type L2, cir id 00, length 1497
ISIS-Adj: rcvd state UP, old state UP, new state UP, nbr usable TRUE
ISIS-Adj: newstate:0, state_changed:0, going_up:0, going_down:0
ISIS-Adj: Action = ACCEPT
ISIS-Adj: ACTION_ACCEPT:
```

A Pseudo Node LSP is no longer generated for this segment in the database. The LSP Holdtime of 0 indicates that the old LSP is currently aging out and will eventually be deleted.

```
R5#show isis database

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x0000000E   0x13CC        505               0/0/0
R1.01-00              0x0000000D   0x09C5        1060              0/0/0
R2.00-00              0x00000010   0xFE40        504               0/0/0
```

```
R2.02-00              0x0000000C   0x3C8E        643                 0/0/0
R3.00-00              0x00000012   0xCE4E        603                 0/0/0
R3.01-00              0x0000000C   0x17B4        1008                0/0/0
R3.02-00              0x0000000D   0x4087        1072                0/0/0
R3.03-00              0x0000000D   0x6B59        546                 0/0/0
R4.00-00              0x00000012   0x1628        682                 0/0/0
R4.03-00              0x0000000C   0x5A6A        524                 0/0/0
R5.00-00            * 0x00000014   0xB421        997                 0/0/0
R6.00-00              0x00000012   0xC841        720                 0/0/0
R6.02-00              0x0000000D   0x526F        670                 0/0/0
R6.03-00              0x0000000E   0x625C        794                 0/0/0
R6.04-00              0x0000000C   0x5556        501                 0/0/0
XR1.00-00             0x00000011   0xD384        993                 0/0/0
XR1.01-00             0x0000000C   0x8CF4        810                 0/0/0
XR1.05-00             0x0000000C   0x0000        0 (987)             0/0/0
XR2.00-00             0x0000000E   0xD936        665                 0/0/0
```

R5#show isis database XR1.00-00 detail

```
IS-IS Level-2 LSP XR1.00-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
XR1.00-00             0x00000011   0xD384        868               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: XR1
  IP Address:   19.19.19.19
  Metric: 10         IS XR1.01
  Metric: 10         IS R6.04 Metric: 10         IS R5.00
  Metric: 10         IP 10.19.20.0 255.255.255.0
  Metric: 0          IP 19.19.19.19 255.255.255.255
  Metric: 10         IP 20.5.19.0 255.255.255.0
  Metric: 10         IP 20.6.19.0 255.255.255.0
```

R5#show isis database R5.00-00 detail

```
IS-IS Level-2 LSP R5.00-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R5.00-00            * 0x00000014   0xB421        804               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: R5
  Metric: 10         IS R4.03
  Metric: 10         IS R6.03
```

```
 Metric: 10          IS XR1.00


  IP Address:   5.5.5.5
  Metric: 10         IP 20.4.5.0 255.255.255.0
  Metric: 10         IP 20.5.6.0 255.255.255.0
  Metric: 10         IP 20.5.19.0 255.255.255.0
  Metric: 0          IP 5.5.5.5 255.255.255.255
```

R5 is only advertising one LSP, however XR1 is advertising two. This is because XR1 is the DIS for the segment between XR1 and XR2.

```
R5#show isis database



IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000011   0x0DCF        781               0/0/0
R1.01-00              0x0000000F   0x05C7        566               0/0/0
R2.00-00              0x00000013   0xF843        864               0/0/0
R2.02-00              0x0000000F   0x3691        1035              0/0/0
R3.00-00              0x00000015   0xC851        782               0/0/0
R3.01-00              0x0000000E   0x13B6        542               0/0/0
R3.02-00              0x0000000F   0x3C89        624               0/0/0
R3.03-00              0x00000010   0x655C        679               0/0/0
R4.00-00              0x00000015   0x102B        1154              0/0/0
R4.03-00              0x0000000F   0x546D        608               0/0/0
R5.00-00            * 0x00000016   0xB023        390               0/0/0

R6.00-00              0x00000015   0xC244        966               0/0/0
R6.02-00              0x00000010   0x4C72        811               0/0/0
R6.03-00              0x00000011   0x5C5F        1018              0/0/0
R6.04-00              0x0000000F   0x4F59        632               0/0/0
XR1.00-00             0x00000013   0xCF86        629               0/0/0
XR1.01-00             0x0000000F   0x86F7        1073              0/0/0

XR2.00-00             0x00000011   0xD339        1043              0/0/0
R5#show isis database XR1.01-00 detail




IS-IS Level-2 LSP XR1.01-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL XR1.01-00
            0x0000000F   0x86F7        981               0/0/0 Metric: 0          IS XR1.00
Metric: 0          IS XR2.00
```

Another benefit gained by changing the network type to point-to-point on directly connected LAN segments is the reduced flooding of CSNP packets. On a point-to-point link, ISIS will send an initial CSNP (Complete Sequence Number Packet) when the adjacency is being established. This is similar to the DBD exchange in OSPF. As soon as the adjacency is established and the CSNP is exchanged, each device on the point-to-point link will acknowledge the CSNP with a PSNP. This makes flooding over point-to-point links reliable, as CSNP packets are acknowledged. In contrast, broadcast segments flood CSNP packets at set intervals instead of only during adjacency establishment - causing additional overhead. The flooded CSNP packets are not acknowledged over LAN segments. Instead of relying on acknowledgments for reliability, the DIS floods the CSNP periodically to ensure all devices in the LAN segment have the latest CSNP.

Notice that the CSNP is being flooded by the DIS every 10 seconds on the broadcast segment adjacencies, yet no SNP packets are being received from the adjacency with XR1

```
R5#show isis neighbors

System Id      Type Interface    IP Address      State Holdtime Circuit Id
R4             L2   Gi1.45       20.4.5.4        UP    8        R4.03
R6             L2   Gi1.56       20.5.6.6        UP    8        R6.03
XR1            L2   Gi1.519      20.5.19.19      UP    25       00
R5#debug isis snp-packets

*Apr 25 19:37:24.777: %SYS-5-CONFIG_I: Configured from console by console *Apr 25
19:37:24.964: ISIS-Snp: Rec L2 CSNP from 0000.0000.0004 (GigabitEthernet1.45)
*Apr 25 19:37:24.964: ISIS-SNP: CSNP range 0000.0000.0000.00-00 to FFFF.FFFF.FFFF.FF-FF
*Apr 25 19:37:24.964: ISIS-SNP: Same entry 0000.0000.0001.00-00, seq B
*Apr 25 19:37:24.964: ISIS-SNP: Same entry 0000.0000.0001.01-00, seq 9
*Apr 25 19:37:24.964: ISIS-SNP: Same entry 0000.0000.0002.00-00, seq D
*Apr 25 19:37:24.964: ISIS-SNP: Same entry 0000.0000.0002.02-00, seq 9
R5#
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0003.00-00, seq D
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0003.01-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0003.02-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0003.03-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0004.00-00, seq E0
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0004.03-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0005.00-00, seq D
R5#
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0006.00-00, seq E1
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0006.02-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0006.03-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0006.04-00, seq 9
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0019.00-00, seq E4
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0019.01-00, seq DC
*Apr 25 19:37:24.965: ISIS-SNP: Same entry 0000.0000.0020.00-00, seq DE
R5#
R5# *Apr 25 19:37:30.964: ISIS-Snp: Rec L2 CSNP from 0000.0000.0006 (GigabitEthernet1.56)
*Apr 25 19:37:30.964: ISIS-SNP: CSNP range 0000.0000.0000.00-00 to FFFF.FFFF.FFFF.FF-FF
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0001.00-00, seq B
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0001.01-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0002.00-00, seq D
```

```
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0002.02-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0003.00-00, seq D
R5#
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0003.01-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0003.02-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0003.03-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0004.00-00, seq E0
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0004.03-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0005.00-00, seq D
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0006.00-00, seq E1
R5#
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0006.02-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0006.03-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0006.04-00, seq 9
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0019.00-00, seq E4
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0019.01-00, seq DC
*Apr 25 19:37:30.964: ISIS-SNP: Same entry 0000.0000.0020.00-00, seq DE *Apr 25
19:37:33.327: ISIS-Snp: Rec L2 CSNP from 0000.0000.0004 (GigabitEthernet1.45)
R5#
*Apr 25 19:37:33.327: ISIS-SNP: CSNP range 0000.0000.0000.00-00 to FFFF.FFFF.FFFF.FF-FF
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0001.00-00, seq B
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0001.01-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0002.00-00, seq D
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0002.02-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0003.00-00, seq D
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0003.01-00, seq 9
R5#
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0003.02-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0003.03-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0004.00-00, seq E0
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0004.03-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0005.00-00, seq D
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0006.00-00, seq E1
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0006.02-00, seq 9
R5#
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0006.03-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0006.04-00, seq 9
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0019.00-00, seq E4
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0019.01-00, seq DC
*Apr 25 19:37:33.327: ISIS-SNP: Same entry 0000.0000.0020.00-00, seq DE *Apr 25
19:37:39.033: ISIS-Snp: Rec L2 CSNP from 0000.0000.0006 (GigabitEthernet1.56)

*Apr 25 19:37:39.033: ISIS-SNP: CSNP range 0000.0000.0000.00-00 to FFFF.FFFF.FFFF.FF-FF
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0001.00-00, seq B
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0001.01-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0002.00-00, seq D
```

```
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0002.02-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0003.00-00, seq D
R5#
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0003.01-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0003.02-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0003.03-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0004.00-00, seq E0
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0004.03-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0005.00-00, seq D
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0006.00-00, seq E1
R5#
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0006.02-00, seq 9
*Apr 25 19:37:39.033: ISIS-SNP: Same entry 0000.0000.0006.03-00, seq 9
*Apr 25 19:37:39.034: ISIS-SNP: Same entry 0000.0000.0006.04-00, seq 9
*Apr 25 19:37:39.034: ISIS-SNP: Same entry 0000.0000.0019.00-00, seq E4
*Apr 25 19:37:39.034: ISIS-SNP: Same entry 0000.0000.0019.01-00, seq DC
*Apr 25 19:37:39.034: ISIS-SNP: Same entry 0000.0000.0020.00-00, seq DE
R5#
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

IS-IS Path Selection

- Change the IS-IS metric on the link between R6 and XR1 so that bidirectional traffic between R1 and XR2 prefers to use the link between R5 and XR1.

Configuration

```
R6:
interface GigabitEthernet1.619
 isis metric 20 level-2

XR1:
router isis 1
 interface GigabitEthernet0/0/0/0.619
  address-family ipv4 unicast
   metric 20
  !
 !
!
```

Verification

Unlike OSPF, IS-IS metric values are not based on bandwidth. Instead, each interface gets a default metric of 10, as seen below. All link types, including Ethernet, FastEthernet, GigabitEthernet, and OC-48 POS links have a metric of 10:

```
R5#show clns interface | include line protocol|Metric
GigabitEthernet1 is up, line protocol is up
GigabitEthernet1.5 is deleted, line protocol is down
GigabitEthernet1.45 is up, line protocol is up Level-2 Metric: 10, Priority: 64, Circuit ID: R4.03
    Level-2 IPv6 Metric: 10
GigabitEthernet1.56 is up, line protocol is up Level-2 Metric: 10, Priority: 64, Circuit ID: R6.03
    Level-2 IPv6 Metric: 10
GigabitEthernet1.58 is deleted, line protocol is down
GigabitEthernet1.100 is deleted, line protocol is down
```

```
GigabitEthernet1.519 is up, line protocol is up Level-2 Metric: 10, Priority: 64, Circuit ID: XR1.00
    Level-2 IPv6 Metric: 10
GigabitEthernet2 is up, line protocol is up
GigabitEthernet3 is up, line protocol is up
Loopback0 is up, line protocol is up
RP/0/0/CPU0:XR1#show isis interface | include "Loopback|Gig|Metric"

Sat Apr 25 19:51:54.886 UTC
Loopback0                  Enabled
    Metric (L1/L2):        0/0
GigabitEthernet0/0/0/0.519  Enabled Metric (L1/L2):         10/10
GigabitEthernet0/0/0/0.619  Enabled Metric (L1/L2):         10/10
GigabitEthernet0/0/0/0.1920 Enabled Metric (L1/L2):         10/10
```

The result of this is that traffic follows the shortest hop count from the source to the destination in the network. Paths that have equal number of hops are then sent to CEF for the specific source, destination, flow, etc. load balancing method that is configured.

```
R2#show ip route 20.20.20.20

Routing entry for 20.20.20.20/32
  Known via "isis", distance 115, metric 40, type level-2
  Redistributing via isis
  Last update from 20.2.3.3 on GigabitEthernet1.23, 00:00:20 ago
  Routing Descriptor Blocks:  * 20.2.4.4, from 20.20.20.20, 00:00:20 ago, via GigabitEthernet1.24
      Route metric is 40, traffic share count is 1
20.2.3.3, from 20.20.20.20, 00:00:20 ago, via GigabitEthernet1.23
      Route metric is 40, traffic share count is 1

R2#show isis topology XR2
Translating "XR2"



Tag null:

IS-IS 0 level-2 path to XR2
System Id            Metric     Next-Hop             Interface    SNPA XR2 40
R3                   Gi1.23      0050.569e.6e6a
 R4                   Gi1.24      0050.569e.1302



R1#traceroute 20.20.20.20
```

```
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.2.2 4 msec 1 msec 1 msec
 2 20.2.3.3 1 msec 6 msec 2 msec 3 20.3.6.6 1 msec 1 msec 2 msec
 4 20.6.19.19 9 msec 12 msec 13 msec
 5 10.19.20.20 13 msec *  4 msec

RP/0/0/CPU0:XR1#show route ipv4 1.1.1.1/32
Sat Apr 25 19:53:41.229 UTC

Routing entry for 1.1.1.1/32
  Known via "isis 1", distance 115, metric 40, type level-2
  Installed Apr 25 19:51:28.058 for 00:02:13
  Routing Descriptor Blocks 20.5.19.5, from 1.1.1.1, via GigabitEthernet0/0/0/0.519
      Route metric is 40 20.6.19.6, from 1.1.1.1, via GigabitEthernet0/0/0/0.619
      Route metric is 40
  No advertising protos.
RP/0/0/CPU0:XR2#traceroute 1.1.1.1

Sat Apr 25 19:54:01.938 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 9 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.4.5.4 0 msec  0 msec  0 msec
 4  20.2.4.2 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  0 msec
```

By increasing the cost of less desirable paths, these links are eliminated from the resulting Shortest Path Tree of the SPF calculation.

```
R2#show ip route 20.20.20.20
Routing entry for 20.20.20.20/32
  Known via "isis", distance 115, metric 40, type level-2
  Redistributing via isis
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:00:07 ago
  Routing Descriptor Blocks:  * 20.2.4.4, from 20.20.20.20, 00:00:07 ago, via GigabitEthernet1.24
      Route metric is 40, traffic share count is 1

R2#show isis topology XR2
Translating "XR2"
```

```
Tag null:

IS-IS 0 level-2 path to XR2
System Id            Metric     Next-Hop             Interface    SNPA XR2 40
R4                   Gi1.24      0050.569e.1302

RP/0/0/CPU0:XR1#show route ipv4 1.1.1.1/32
Sat Apr 25 19:55:29.241 UTC

Routing entry for 1.1.1.1/32
  Known via "isis 1", distance 115, metric 40, type level-2
  Installed Apr 25 19:54:45.414 for 00:00:43
  Routing Descriptor Blocks 20.5.19.5, from 1.1.1.1, via GigabitEthernet0/0/0/0.519

      Route metric is 40
  No advertising protos.
```

The result of this change is that the R6 to XR1 link is avoided unless it is the only possible option.

```
R1#traceroute 20.20.20.20
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec
  2 20.2.4.4 1 msec 1 msec 1 msec
  3 20.4.5.5 1 msec 2 msec 5 msec 4 20.5.19.19 10 msec 12 msec 13 msec
  5 10.19.20.20 13 msec *  3 msec

RP/0/0/CPU0:XR2#traceroute 1.1.1.1

Sat Apr 25 19:56:27.038 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.4.5.4 0 msec  0 msec  0 msec
 4  20.2.4.2 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

IS-IS BFD

- Configure BFD for IS-IS between R4 and R5 so that if there is a failure of the link between them they begin reconvergence in less than one second.

Configuration

```
> Note: BFD is not supported on the current versions of XRv


R4:
interface GigabitEthernet1.45
 bfd interval 250 min_rx 250 multiplier 3
 isis bfd

R5:
interface GigabitEthernet1.45
 bfd interval 250 min_rx 250 multiplier 3
 isis bfd
```

Verification

R4 and R5 are BFD adjacent via IS-IS, and are configured to detect a failure in 750ms.

```
R4#show bfd neighbors detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
20.4.5.5                             4097/4097       Up        Up        Gi1.45
Session state is UP and using echo function with 250 ms interval.
Session Host: Software
OurAddr: 20.4.5.4
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(160)
Rx Count: 154, Rx Interval (ms) min/max/avg: 1/993/867 last: 626 ms ago
Tx Count: 161, Tx Interval (ms) min/max/avg: 2/1001/876 last: 224 ms ago
Elapsed time watermarks: 0 0 (last: 0) Registered protocols: ISIS CEF

Uptime: 00:02:13
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 0                               Multiplier: 3
               - Length: 24
             My Discr.: 4097             - Your Discr.: 4097
             Min tx interval: 1000000    - Min rx interval: 1000000 Min Echo interval: 250000
```

```
R5#show bfd neighbors detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
20.4.5.4                             4097/4097       Up        Up        Gi1.45
Session state is UP and using echo function with 250 ms interval.
Session Host: Software
OurAddr: 20.4.5.5
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(247)
Rx Count: 246, Rx Interval (ms) min/max/avg: 2/1045/876 last: 322 ms ago
Tx Count: 249, Tx Interval (ms) min/max/avg: 1/1000/865 last: 457 ms ago
Elapsed time watermarks: 0 0 (last: 0) Registered protocols: ISIS CEF
Uptime: 00:03:35
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 0                               Multiplier: 3
               - Length: 24
             My Discr.: 4097             - Your Discr.: 4097
             Min tx interval: 1000000    - Min rx interval: 1000000 Min Echo interval: 250000
```

R4’s interface is disabled at time index 20:27:57.415. R5 detects the failure at

20:27:58.063, within 1 second at time index 20:27:57.415.

```
RP/0/0/CPU0:XR2#ping 1.1.1.1 count 100000
Sat Apr 25 20:27:55.818 UTC
Type escape sequence to abort.
Sending 100000, 100-byte ICMP Echos to 1.1.1.
!!!!!!!!!!!!!!!!!!!!!!
R5#debug bfd event
BFD event debugging is on
R5(config)#R5(config)#router isis
R5(config-router)#log-adjacency-changes all
R5(config-router)#service timestamp log datetime msec
R5(config)#end

R4#debug bfd event
R4#conf tR4(config)#int g1.45
R4(config-subif)#shut
R4(config-subif)#*Apr 25 20:27:57.415
: BFD-DEBUG EVENT: bfd_session_destroyed, proc:ISIS, handle:1 act
*Apr 25 20:27:57.422: BFD-DEBUG EVENT: bfd_session_destroyed, proc:CEF, handle:1 act
*Apr 25 20:27:57.425: BFD-DEBUG Event: V1 FSM ld:4097 handle:1 event:Session delete state:UP (0)
R4(config-subif)#
*Apr 25 20:28:00.422: BFD-DEBUG Event: V1 FSM ld:4097 handle:1 event:DETECT TIMER EXPIRED state:ADMIN DOWN (0)
*Apr 25 20:28:00.422: BFD-DEBUG Event: decreasing credits by 12 [to 0] (0)


R5# *Apr 25 20:27:58.063
: BFD-DEBUG Event: V1 FSM ld:4097 handle:1 event:ECHO FAILURE state:UP (0)
*Apr 25 20:27:58.063: BFD-DEBUG Event: notify client(CEF) IP:20.4.5.4, ld:4097, handle:1, event:DOWN, cp independent
*Apr 25 20:27:58.063: BFD-DEBUG Event: notify client(ISIS) IP:20.4.5.4, ld:4097, handle:1, event:DOWN, cp independen
*Apr 25 20:27:58.063: BFD-DEBUG Event: notify client(CEF) IP:20.4.5.4, ld:4097, handle:1, event:DOWN, cp independent
R5# *Apr 25 20:27:58.063:
%CLNS-5-ADJCHANGE: ISIS: Adjacency to R4 (GigabitEthernet1.45) Down, bfd neighbor down

R5#
*Apr 25 20:28:04.775: %CLNS-5-ADJCHANGE: ISIS: Adjacency to R4 (GigabitEthernet1.45) Down, hold time expired
R5#
*Apr 25 20:28:04.775: BFD-DEBUG EVENT: bfd_session_destroyed, proc:ISIS, handle:1 act
```

Notice that there are 6 seconds worth of dropped packets. Although the the failure was detected within 1 second, it still takes ISIS around 5 seconds to converge with default timers. Like OSPF, these timers can be tuned to achieve subsecond convergence however.

```
RP/0/0/CPU0:XR2#ping 1.1.1.1 count 100000

Sat Apr 25 20:27:55.818 UTC
Type escape sequence to abort.
Sending 100000, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
Success rate is 98 percent (292/295), round-trip min/avg/max = 1/21/139 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

IS-IS Authentication

- Configure clear text IS-IS Authentication between R6 and XR1 using the password “INECLEAR”.
- Configure MD5 IS-IS Authentication between R5 and XR1 using the password “INEMD5”.

Configuration

```
R5:
key chain ISIS
 key 1
  key-string INEMD5
!
interface GigabitEthernet1.519
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

R6:
key chain ISIS
 key 1
  key-string INECLEAR
!
interface GigabitEthernet1.619
 isis authentication mode text level-2
 isis authentication key-chain ISIS

XR1:
router isis 1
 !
 interface GigabitEthernet0/0/0/0.519
  hello-password hmac-md5 INEMD5
  !
 !
 interface GigabitEthernet0/0/0/0.619
  hello-password text INECLEAR
```

```
  address-family ipv4 unicast
  !
 !
!
```

Verification

ISIS has several authentication methods, each one designed for a specific purpose. Authentication information is carried inside of the Authentication Information TLV, type 10, in all PDUs. Interface level authentication is used to authenticate the hello (IIH) packets. It can be configured using either clear text with the legacy 'isis password' command, or MD5 using key-chains at the interface level. The level can also be specified, by default both L1 and L2 hello packets are authenticated.

Area and Domain authentication are used to authenticate LSPs, CSNPs, and PSNPs in L1 and L2 respectively. Neither of these authentication mechanisms authenticate hellos. Domain and Area authentication mechanisms have been superseded by a newer protocol level authentication. The newer mechanisms is configured at the routing process with key-chains and supports authentication LSPs, CSNPs, and PSNPs in L1 and L2 using MD5 or clear text.

```
RP/0/0/CPU0:XR1#show isis adjacency

Sat Apr 25 23:52:39.087 UTC

IS-IS 1 Level-2 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
R6             Gi0/0/0/0.619    0050.569e.5cec Up    7    00:10:06 Yes None None
R5             Gi0/0/0/0.519    *PtoP*         Up    28   01:09:33 Yes None None

XR2            Gi0/0/0/0.1920   0050.569e.27ac Up    29   01:09:39 Yes None None

Total adjacency count: 3
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

Multi-Level IS-IS

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IPv4**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Using the Base IPv4 Diagram, configure IS-IS on all interfaces of the devices as follows:
  - R1, R2, R3, and R4 should use NET addresses 49.1234.0000.0000.000Y.00 where Y is their router number.
  - R5 and R6 should use NET addresses 49.0056.0000.0000.0000Y.00 where Y is their router number.
  - XR1 and XR2 should use NET addresses 49.1920.0000.0000.000Y.00 where Y is their router number.
- Configure IS-IS Level assignments as follows:
  - R1 and R2 should be L1 only routers.
  - R3 and R4 should be L1/L2 routers, with their links to R2 running Level-1 and all other links running Level-2.
  - R5 and R6 should be L2 only routers.
  - XR1 should be an L1/L2 router, with its link to XR2 running Level-1 and all other links running Level-2.
  - XR2 should be an L1 only router.
- Advertise the Loopback interfaces of the routers using the **passive-interface** or **passive** command.

Configuration

```
R1:
interface GigabitEthernet1.12
 ip router isis
!
router isis
 net 49.1234.0000.0000.0001.00
```

```
 is-type level-1
 passive-interface Loopback0

R2:
interface GigabitEthernet1.23
 ip router isis
!
interface GigabitEthernet1.24
 ip router isis
!
interface GigabitEthernet1.12
 ip router isis
!
router isis
 net 49.1234.0000.0000.0002.00
 is-type level-1
 passive-interface Loopback0

R3:
interface GigabitEthernet1.23
 ip router isis
 isis circuit-type level-1
!
interface GigabitEthernet1.34
 ip router isis
 isis circuit-type level-2
!
interface GigabitEthernet1.36
 ip router isis
 isis circuit-type level-2
!
interface Loopback0
 isis circuit-type level-2
!
router isis
 net 49.1234.0000.0000.0003.00
 is-type level-1-2
 passive-interface Loopback0

R4:
interface GigabitEthernet1.24
 ip router isis
 isis circuit-type level-1
!
interface GigabitEthernet1.34
 ip router isis
```

```
 isis circuit-type level-2
!
interface GigabitEthernet1.45
 ip router isis
 isis circuit-type level-2
!
interface GigabitEthernet1.46
 ip router isis
 isis circuit-type level-2
!
interface Loopback0
 isis circuit-type level-2
!
router isis
 net 49.1234.0000.0000.0004.00
 is-type level-1-2
 passive-interface Loopback0

R5:
interface GigabitEthernet1.45
 ip router isis
!
interface GigabitEthernet1.56
 ip router isis
!
interface GigabitEthernet1.519
 ip router isis
!
router isis
 net 49.0056.0000.0000.0005.00
 is-type level-2-only
 passive-interface Loopback0

R6:
interface GigabitEthernet1.36
 ip router isis
!
interface GigabitEthernet1.46
 ip router isis
!
interface GigabitEthernet1.56
 ip router isis
!
interface GigabitEthernet1.619
 ip router isis
!
```

```
router isis
 net 49.0056.0000.0000.0006.00
 is-type level-2-only
 passive-interface Loopback0

XR1:
router isis 1
 is-type level-1-2
 net 49.1920.0000.0000.0019.00
 interface Loopback0
  passive
  circuit-type level-2
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.519
  circuit-type level-2
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.619
  circuit-type level-2
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.1920
  circuit-type level-1
  address-family ipv4 unicast
  !
 !
!

XR2:
router isis 1
 is-type level-1
 net 49.1920.0000.0000.0020.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 unicast
  !
 !
```

```
!
```

Verification

All routers should be adjacent with all their directly connected neighbors. R1, R2, & XR2 should be forming only L1 adjacencies, R3, R4, & XR1 should be forming both L1 and L2 adjacencies, and R5 & R6 should be forming only L2 adjacencies.

```
R1#show isis neighbors

Tag null:System Id Type
 Interface   IP Address      State Holdtime Circuit Id R2 L1
   Gi1.12      10.1.2.2        UP     29       R1.01
R2#show isis neighbors

Tag null:System Id Type
 Interface   IP Address      State Holdtime Circuit Id R1 L1
   Gi1.12      10.1.2.1        UP     7        R1.01        R3 L1
   Gi1.23      20.2.3.3        UP     6        R3.01        R4 L1
   Gi1.24      20.2.4.4        UP     28       R2.02
R3#show isis neighbors

Tag null:System Id Type
 Interface   IP Address      State Holdtime Circuit Id R2 L1
  Gi1.23      20.2.3.2        UP     28       R3.01        R4 L2
  Gi1.34      20.3.4.4        UP     22       R3.02        R6 L2
  Gi1.36      20.3.6.6        UP     26       R3.03

R4#show isis neighbors
System Id Type
 Interface   IP Address      State Holdtime Circuit Id R2 L1
   Gi1.24      20.2.4.2        UP     9        R2.02        R3 L2
   Gi1.34      20.3.4.3        UP     9        R3.02        R5 L2
   Gi1.45      20.4.5.5        UP     23       R4.03        R6 L2
   Gi1.46      20.4.6.6        UP     7        R6.02
R5#show isis neighbors
System Id Type
 Interface   IP Address      State Holdtime Circuit Id R4 L2
      Gi1.45      20.4.5.4        UP     8        R4.03        R6 L2
      Gi1.56      20.5.6.6        UP     7        R6.03        XR1 L2
      Gi1.519     20.5.19.19      UP     9        XR1.05
R6#show isis neighbors
System Id Type
 Interface   IP Address      State Holdtime Circuit Id
```

```
R3 L2
      Gi1.36      20.3.6.3        UP     9        R3.03       R4 L2
      Gi1.46      20.4.6.4        UP     29       R6.02       R5 L2
      Gi1.56      20.5.6.5        UP     27       R6.03       XR1 L2
      Gi1.619     20.6.19.19      UP     24       R6.04


RP/0/0/CPU0:XR1#show isis adjacency
Mon Apr 27 22:52:44.605 UTC
IS-IS 1 Level-1 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
XR2            Gi0/0/0/0.1920   0050.569e.27ac Up    21   00:07:15 Yes None None

Total adjacency count: 1
IS-IS 1 Level-2 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
R6             Gi0/0/0/0.619    0050.569e.5cec Up    7    00:07:39 Yes None None
R5             Gi0/0/0/0.519    0050.569e.0962 Up    28   00:07:39 Yes None None

Total adjacency count: 2
RP/0/3/CPU0:XR2#show isis adjacency
Mon Apr 27 22:53:25.703 UTC
IS-IS 1 Level-1 adjacencies:

System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
                                                                       BFD  BFD
XR1            Gi0/0/0/0.1920   0050.569e.59fe Up    8    00:07:57 Yes None None

Total adjacency count: 1
```

R1 and R2, as Level-1 only routers, should see Level-1 routes within their own Area, and a default route out to the L1/L2 routers.

```
R1#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 10.1.2.2 to network 0.0.0.0
i*L1  0.0.0.0/0
 [115/20] via 10.1.2.2, 00:09:17, GigabitEthernet1.12
      2.0.0.0/32 is subnetted, 1 subnets i L1      2.2.2.2
 [115/10] via 10.1.2.2, 00:10:39, GigabitEthernet1.12
      20.0.0.0/24 is subnetted, 2 subnets i L1      20.2.3.0
 [115/20] via 10.1.2.2, 00:10:39, GigabitEthernet1.12 i L1      20.2.4.0
 [115/20] via 10.1.2.2, 00:10:39, GigabitEthernet1.12

R2#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 20.2.4.4 to network 0.0.0.0
i*L1  0.0.0.0/0
 [115/10] via 20.2.4.4, 00:09:57, GigabitEthernet1.24
                [115/10] via 20.2.3.3, 00:09:57, GigabitEthernet1.23
      1.0.0.0/32 is subnetted, 1 subnets i L1      1.1.1.1
 [115/10] via 10.1.2.1, 00:11:20, GigabitEthernet1.12
```

R3 and R4, as L1/L2 routers, should see L1 routes from R1 and R2, and L2 routes about all other destinations in the topology.

```
R3#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
  1.0.0.0/32 is subnetted, 1 subnets i L1
1.1.1.1 [115/20] via 20.2.3.2, 00:11:23, GigabitEthernet1.23
  2.0.0.0/32 is subnetted, 1 subnets i L1
2.2.2.2 [115/10] via 20.2.3.2, 00:11:33, GigabitEthernet1.23
  4.0.0.0/32 is subnetted, 1 subnets i L2
4.4.4.4 [115/10] via 20.3.4.4, 00:10:57, GigabitEthernet1.34
  5.0.0.0/32 is subnetted, 1 subnets i L2
5.5.5.5 [115/20] via 20.3.6.6, 00:05:02, GigabitEthernet1.36
            [115/20] via 20.3.4.4, 00:05:02, GigabitEthernet1.34
  6.0.0.0/32 is subnetted, 1 subnets i L2
6.6.6.6 [115/10] via 20.3.6.6, 00:10:43, GigabitEthernet1.36
  10.0.0.0/24 is subnetted, 2 subnets i L1
10.1.2.0 [115/20] via 20.2.3.2, 00:11:33, GigabitEthernet1.23 i L2
10.19.20.0 [115/30] via 20.3.6.6, 00:10:06, GigabitEthernet1.36
  19.0.0.0/32 is subnetted, 1 subnets i L2
19.19.19.19 [115/20] via 20.3.6.6, 00:10:14, GigabitEthernet1.36
  20.0.0.0/8 is variably subnetted, 13 subnets, 2 masks i L1
20.2.4.0/24 [115/20] via 20.2.3.2, 00:11:33, GigabitEthernet1.23 i L2
20.4.5.0/24 [115/20] via 20.3.4.4, 00:05:02, GigabitEthernet1.34 i L2
20.4.6.0/24 [115/20] via 20.3.6.6, 00:10:43, GigabitEthernet1.36
                [115/20] via 20.3.4.4, 00:10:43, GigabitEthernet1.34 i L2
20.5.6.0/24 [115/20] via 20.3.6.6, 00:10:43, GigabitEthernet1.36 i L2
20.5.19.0/24 [115/30] via 20.3.6.6, 00:05:02, GigabitEthernet1.36
                 [115/30] via 20.3.4.4, 00:05:02, GigabitEthernet1.34 i L2
20.6.19.0/24 [115/20] via 20.3.6.6, 00:10:43, GigabitEthernet1.36 i L2
20.20.20.20/32 [115/30] via 20.3.6.6, 00:09:53, GigabitEthernet1.36
```

R4#show ip route isis Codes: L - local, 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, H - NHRP, l - LISP a - application route + - replicated route, % - next hop override

```
Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets i L1
     1.1.1.1 [115/20] via 20.2.4.2, 00:11:46, GigabitEthernet1.24
      2.0.0.0/32 is subnetted, 1 subnets i L1
     2.2.2.2 [115/10] via 20.2.4.2, 00:11:57, GigabitEthernet1.24
      3.0.0.0/32 is subnetted, 1 subnets i L2
     3.3.3.3 [115/10] via 20.3.4.3, 00:11:57, GigabitEthernet1.34
      5.0.0.0/32 is subnetted, 1 subnets i L2
     5.5.5.5 [115/10] via 20.4.5.5, 00:06:01, GigabitEthernet1.45
```

```
      6.0.0.0/32 is subnetted, 1 subnets i L2
     6.6.6.6 [115/10] via 20.4.6.6, 00:11:42, GigabitEthernet1.46
      10.0.0.0/24 is subnetted, 2 subnets i L1
     10.1.2.0 [115/20] via 20.2.4.2, 00:11:57, GigabitEthernet1.24 i L2
     10.19.20.0 [115/30] via 20.4.6.6, 00:06:01, GigabitEthernet1.46
                    [115/30] via 20.4.5.5, 00:06:01, GigabitEthernet1.45
      19.0.0.0/32 is subnetted, 1 subnets i L2
     19.19.19.19 [115/20] via 20.4.6.6, 00:06:01, GigabitEthernet1.46
                     [115/20] via 20.4.5.5, 00:06:01, GigabitEthernet1.45
      20.0.0.0/8 is variably subnetted, 14 subnets, 2 masks i L1
     20.2.3.0/24 [115/20] via 20.2.4.2, 00:11:57, GigabitEthernet1.24 i L2
     20.3.6.0/24 [115/20] via 20.4.6.6, 00:11:42, GigabitEthernet1.46
                     [115/20] via 20.3.4.3, 00:11:42, GigabitEthernet1.34 i L2
     20.5.6.0/24 [115/20] via 20.4.6.6, 00:06:01, GigabitEthernet1.46
                     [115/20] via 20.4.5.5, 00:06:01, GigabitEthernet1.45 i L2
     20.5.19.0/24 [115/20] via 20.4.5.5, 00:06:01, GigabitEthernet1.45 i L2
     20.6.19.0/24 [115/20] via 20.4.6.6, 00:11:42, GigabitEthernet1.46 i L2
     20.20.20.20/32 [115/30] via 20.4.6.6, 00:06:01, GigabitEthernet1.46
                        [115/30] via 20.4.5.5, 00:06:01, GigabitEthernet1.45
```

R5 and R6, as L2 only routers, should see L2 routes about all prefixes in the topology.

```
R5#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets i L2
     1.1.1.1 [115/30] via 20.4.5.4, 00:06:56, GigabitEthernet1.45
      2.0.0.0/32 is subnetted, 1 subnets i L2
     2.2.2.2 [115/20] via 20.4.5.4, 00:06:56, GigabitEthernet1.45
      3.0.0.0/32 is subnetted, 1 subnets i L2
     3.3.3.3 [115/20] via 20.5.6.6, 00:06:56, GigabitEthernet1.56
                 [115/20] via 20.4.5.4, 00:06:56, GigabitEthernet1.45
      4.0.0.0/32 is subnetted, 1 subnets
```

```
i L2
     4.4.4.4 [115/10] via 20.4.5.4, 00:06:56, GigabitEthernet1.45
      6.0.0.0/32 is subnetted, 1 subnets i L2
     6.6.6.6 [115/10] via 20.5.6.6, 00:12:35, GigabitEthernet1.56
      10.0.0.0/24 is subnetted, 2 subnets i L2
     10.1.2.0 [115/30] via 20.4.5.4, 00:06:56, GigabitEthernet1.45 i L2
     10.19.20.0 [115/20] via 20.5.19.19, 00:11:58, GigabitEthernet1.519
      19.0.0.0/32 is subnetted, 1 subnets i L2
     19.19.19.19 [115/10] via 20.5.19.19, 00:12:08, GigabitEthernet1.519
      20.0.0.0/8 is variably subnetted, 13 subnets, 2 masks i L2
     20.2.3.0/24 [115/30] via 20.5.6.6, 00:06:56, GigabitEthernet1.56
                 [115/30] via 20.4.5.4, 00:06:56, GigabitEthernet1.45 i L2
     20.2.4.0/24 [115/20] via 20.4.5.4, 00:06:56, GigabitEthernet1.45 i L2
     20.3.4.0/24 [115/20] via 20.4.5.4, 00:06:56, GigabitEthernet1.45 i L2
     20.3.6.0/24 [115/20] via 20.5.6.6, 00:12:35, GigabitEthernet1.56 i L2
     20.4.6.0/24 [115/20] via 20.5.6.6, 00:06:56, GigabitEthernet1.56
                 [115/20] via 20.4.5.4, 00:06:56, GigabitEthernet1.45 i L2
     20.6.19.0/24 [115/20] via 20.5.19.19, 00:12:08, GigabitEthernet1.519
                  [115/20] via 20.5.6.6, 00:12:08, GigabitEthernet1.56 i L2
     20.20.20.20/32
           [115/20] via 20.5.19.19, 00:11:46, GigabitEthernet1.519
```

R6#show ip route isis

```
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets i L2
     1.1.1.1 [115/30] via 20.4.6.4, 00:13:23, GigabitEthernet1.46
             [115/30] via 20.3.6.3, 00:13:23, GigabitEthernet1.36
      2.0.0.0/32 is subnetted, 1 subnets i L2
     2.2.2.2 [115/20] via 20.4.6.4, 00:13:33, GigabitEthernet1.46
             [115/20] via 20.3.6.3, 00:13:33, GigabitEthernet1.36
      3.0.0.0/32 is subnetted, 1 subnets i L2
     3.3.3.3 [115/10] via 20.3.6.3, 00:13:33, GigabitEthernet1.36
      4.0.0.0/32 is subnetted, 1 subnets
```

```
i L2
    4.4.4.4 [115/10] via 20.4.6.4, 00:13:33, GigabitEthernet1.46
     5.0.0.0/32 is subnetted, 1 subnets i L2
    5.5.5.5 [115/10] via 20.5.6.5, 00:13:33, GigabitEthernet1.56
     10.0.0.0/24 is subnetted, 2 subnets i L2
    10.1.2.0 [115/30] via 20.4.6.4, 00:13:33, GigabitEthernet1.46
                 [115/30] via 20.3.6.3, 00:13:33, GigabitEthernet1.36 i L2
    10.19.20.0 [115/20] via 20.6.19.19, 00:12:53, GigabitEthernet1.619
     19.0.0.0/32 is subnetted, 1 subnets i L2
    19.19.19.19 [115/10] via 20.6.19.19, 00:13:03, GigabitEthernet1.619
     20.0.0.0/8 is variably subnetted, 14 subnets, 2 masks i L2
    20.2.3.0/24 [115/20] via 20.3.6.3, 00:13:33, GigabitEthernet1.36 i L2
    20.2.4.0/24 [115/20] via 20.4.6.4, 00:13:33, GigabitEthernet1.46 i L2
    20.3.4.0/24 [115/20] via 20.4.6.4, 00:13:33, GigabitEthernet1.46
                    [115/20] via 20.3.6.3, 00:13:33, GigabitEthernet1.36 i L2
    20.4.5.0/24 [115/20] via 20.5.6.5, 00:07:51, GigabitEthernet1.56
                    [115/20] via 20.4.6.4, 00:07:51, GigabitEthernet1.46 i L2
    20.5.19.0/24 [115/20] via 20.6.19.19, 00:13:03, GigabitEthernet1.619
                     [115/20] via 20.5.6.5, 00:13:03, GigabitEthernet1.56 i L2
    20.20.20.20/32
          [115/20] via 20.6.19.19, 00:12:41, GigabitEthernet1.619
```

XR1, as an L1/L2 router, should see L1 routes from XR2, and L2 routes about all other prefixes in the topology from R5 and R6.

```
RP/0/0/CPU0:XR1#show route ipv4 isis


Mon Apr 27 22:58:56.690 UTC
 i L2
 1.1.1.1/32 [115/40] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
               [115/40] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519 i L2
 2.2.2.2/32 [115/30] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
               [115/30] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519 i L2
 3.3.3.3/32 [115/20] via 20.6.19.6, 00:13:42, GigabitEthernet0/0/0/0.619 i L2
 4.4.4.4/32 [115/20] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
               [115/20] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519 i L2
 5.5.5.5/32 [115/10] via 20.5.19.5, 00:13:45, GigabitEthernet0/0/0/0.519 i L2
 6.6.6.6/32 [115/10] via 20.6.19.6, 00:13:45, GigabitEthernet0/0/0/0.619 i L2
 10.1.2.0/24 [115/40] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
                [115/40] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519 i L2
 20.2.3.0/24 [115/30] via 20.6.19.6, 00:13:42, GigabitEthernet0/0/0/0.619 i L2
 20.2.4.0/24 [115/30] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
                [115/30] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519 i L2
 20.3.4.0/24 [115/30] via 20.6.19.6, 00:08:37, GigabitEthernet0/0/0/0.619
                [115/30] via 20.5.19.5, 00:08:37, GigabitEthernet0/0/0/0.519
```

```
i L2
 20.3.6.0/24 [115/20] via 20.6.19.6, 00:13:45, GigabitEthernet0/0/0/0.619 i L2
 20.4.5.0/24 [115/20] via 20.5.19.5, 00:13:45, GigabitEthernet0/0/0/0.519 i L2
 20.4.6.0/24 [115/20] via 20.6.19.6, 00:13:45, GigabitEthernet0/0/0/0.619 i L2
 20.5.6.0/24 [115/20] via 20.6.19.6, 00:13:45, GigabitEthernet0/0/0/0.619
                 [115/20] via 20.5.19.5, 00:13:45, GigabitEthernet0/0/0/0.519
i L1 20.20.20.20/32 [115/10] via 10.19.20.20, 00:13:25, GigabitEthernet0/0/0/0.1920
```

XR2, as an L1 only router, should see only an L1 default from XR1, its L1/L2 router, as there are no other prefixes advertised into the L1 domain other than its connected routes.

```
RP/0/0/CPU0:XR2#show ip route isis
Mon Apr 27 22:59:43.727 UTC
i*L1 0.0.0.0/0
 [115/10] via 10.19.20.19, 00:14:09, GigabitEthernet0/0/0/0.1920
```

The L1/L2 routers R4, R5, and XR1 should all be setting the Attached (ATT) bit in the Link State Database to indicate to the L1 routers that they are a default exit point out to the L2 domain.

```
R2#show isis database



Tag null:
IS-IS Level-1 Link State Database: LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime ATT
/P/OL
R1.00-00              0x00000004   0xF7AE        1010               0/0/0
R1.01-00              0x00000002   0x8DC5        916                0/0/0
R2.00-00            * 0x00000006   0xE322        899                0/0/0
R2.02-00            * 0x00000002   0xBE8F        882                0/0/0
R3.00-00              0x00000004   0xD132        991 1/0/0

R3.01-00              0x00000002   0x9BB1        933                0/0/0
R4.00-00              0x00000004   0x47B7        1051 1/0/0

RP/0/0/CPU0:XR2#show isis database


Mon Apr 27 23:02:02.167 UTC


IS-IS 1 (Level-1) Link State Database LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime ATT
/P/OL XR1.00-00             0x00000004   0xcbf7        1020 1/0/0


XR1.01-00             0x00000002   0xa0ea        894              0/0/0
XR2.00-00           * 0x00000004   0x5c87        973              0/0/0


 Total Level-1 LSP count: 3     Local Level-1 LSP count: 1
```

Note that the Attached bit is stripped as advertisements are sent out to the L2 domain, as only the L1 routers should be using this to default to their L1/L2 exit points.

```
R5#show isis database
IS-IS Level-2 Link State Database:


LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R3.00-00              0x00000007   0x58F3        951               0/0/0
R3.02-00              0x00000002   0x567C        979               0/0/0
R3.03-00              0x00000002   0x814E        865               0/0/0
R4.00-00              0x00000008   0x3934        1146              0/0/0
R4.03-00              0x00000001   0x705F        451               0/0/0
R5.00-00            * 0x00000005   0x0F7B        452               0/0/0
R6.00-00              0x00000005   0x0CB5        1023              0/0/0
R6.02-00              0x00000002   0x6864        799               0/0/0
R6.03-00              0x00000002   0x7A50        913               0/0/0
```

```
R6.04-00              0x00000002   0x694C        961             0/0/0
XR1.00-00             0x00000006   0x1BBF        848             0/0/0
XR1.05-00             0x00000002   0xDEC3        1004            0/0/0
```

All routes should have full reachability to all prefixes in the topology.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 5 msec 1 msec 1 msec
  2 20.2.3.3 1 msec 2 msec 1 msec
  3 20.3.6.6 6 msec 1 msec 1 msec
  4 20.6.19.19 8 msec 12 msec 13 msec
  5 10.19.20.20 13 msec *  3 msec
RP/0/0/CPU0:XR2#traceroute 1.1.1.1

Mon Apr 27 23:05:00.425 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.4.5.4 0 msec  0 msec  0 msec
 4  20.2.4.2 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  0 msec
```

Any router that has both an L1 and an L2 route to the same destination should prefer the L1 route over L2. For example, R3 prefers to route to R2 to reach the link between R2 and R4, as opposed to routing directly to R4. This route preference is similar to OSPF always preferring Intra Area routers over Inter Area routes.

```
R3#show ip route 20.2.4.4
Routing entry for 20.2.4.0/24  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 20.2.3.2 on GigabitEthernet1.23, 00:22:12 ago
  Routing Descriptor Blocks:
  * 20.2.3.2, from 2.2.2.2, 00:22:12 ago, via GigabitEthernet1.23
      Route metric is 20, traffic share count is 1
R3#traceroute 20.2.4.4
Type escape sequence to abort.
Tracing the route to 20.2.4.4
VRF info: (vrf in name/id, vrf out name/id)
```

```
 1 20.2.3.2 4 msec 2 msec 1 msec

   2 20.2.4.4 2 msec *  2 msec
```

In order for the L1L2 ISIS router to set the ATT bit on its LSP, it not only has to be L1L2 router, but also be connected to two distinct areas. If the areas of all the routers were changed to be the same, yet maintained the same level configuration, XR1, R3, and R4 would not generate the ATT bit.

Note that the L1L2 router itself does not have to be directly attached to the two distinct areas - as long as there is another distinct area connected into L2, the L1L2 router would generate the ATT bit into L1. Take the following example,: R5, R6, XR1, and XR2 are in area 49.9999 but maintain the current level configurations, and R1, R2, R3, and R4 are in area 49.1111 and maintain the current level configurations. XR1, the L1L2 router for XR2, is not directly connected to two distinct areas, but the L2 domain to which XR1 connects to does connect to another area (R5 and R6 in area 49.9999 connect to R3 and R4 in area 49.1111).

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

IS-IS Route Leaking

- Configure IS-IS Route Leaking from Level 2 to Level 1 on the L1/L2 routers as follows:
  - R3 should advertise the L2 prefix 5.5.5.5/32 to its L1 routers.
  - R4 should advertise the L2 prefix 6.6.6.6/32 to its L1 routers.
  - XR1 should advertise the 3.3.3.3/32 and 4.4.4.4/32 prefixes to its L1 routers.
- Configure IS-IS Route Leaking from Level 1 to Level 2 on the L1/L2 routers as follows:
  - R3 should not advertise the L1 prefix 2.2.2.2/32 to its L2 routers.
  - R4 should not advertise the L1 prefix 1.1.1.1/32 to its L2 routers

Configuration

```
R3:
router isis
 redistribute isis ip level-1 into level-2 route-map L1_TO_L2_LEAK
 redistribute isis ip level-2 into level-1 route-map L2_TO_L1_LEAK
!
ip prefix-list L2_TO_L1_PL permit 5.5.5.5/32
!
ip prefix-list L1_TO_L2_PL permit 2.2.2.2/32
!
route-map L2_TO_L1_LEAK permit 10
 match ip address prefix L2_TO_L1_PL
!
route-map L1_TO_L2_LEAK deny 10
 match ip address prefix L1_TO_L2_PL
!
route-map L1_TO_L2_LEAK permit 20


R4:
router isis
 redistribute isis ip level-1 into level-2 route-map L1_TO_L2_LEAK
```

```
 redistribute isis ip level-2 into level-1 route-map L2_TO_L1_LEAK
!
ip prefix-list L2_TO_L1_PL permit 6.6.6.6/32
!
ip prefix-list L1_TO_L2_PL permit 1.1.1.1/32
!
route-map L2_TO_L1_LEAK permit 10
 match ip address prefix L2_TO_L1_PL
!
route-map L1_TO_L2_LEAK deny 10
 match ip address prefix L1_TO_L2_PL
!
route-map L1_TO_L2_LEAK permit 20



XR1:
route-policy ISIS_ROUTE_LEAKING
  if destination in (3.3.3.3/32, 4.4.4.4/32) then
    pass
  endif
end-policy
!
router isis 1
 address-family ipv4 unicast
  propagate level 2 into level 1 route-policy ISIS_ROUTE_LEAKING
 !
!
end
```

Verification

Previously R1 and R2 only knew their own L1 routes as well as a default route to the L1/L2 routes. Now the specific routes 5.5.5.5/32 and 6.6.6.6/32 are advertised via R3 and R4 respectively.

```
R2#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
```

```
       + - replicated route, % - next hop override

Gateway of last resort is 20.2.4.4 to network 0.0.0.0

i*L1  0.0.0.0/0 [115/10] via 20.2.4.4, 00:21:12, GigabitEthernet1.24
                [115/10] via 20.2.3.3, 00:21:12, GigabitEthernet1.23
      1.0.0.0/32 is subnetted, 1 subnets
i L1     1.1.1.1 [115/10] via 10.1.2.1, 00:21:43, GigabitEthernet1.12
      5.0.0.0/32 is subnetted, 1 subnets i ia      5.5.5.5
 [115/158] via 20.2.3.3, 00:13:20, GigabitEthernet1.23
      6.0.0.0/32 is subnetted, 1 subnets i ia      6.6.6.6
 [115/148] via 20.2.4.4, 00:13:12, GigabitEthernet1.24
```

Due to the longest match routing principle, traffic going to 5.5.5.5/32 will always prefer R3 as the exit point, while traffic going to 6.6.6.6/32 will always prefer R4.

```
R1#traceroute 5.5.5.5

Type escape sequence to abort.
Tracing the route to 5.5.5.5
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 2 msec 1 msec 1 msec 2 20.2.3.3 6 msec 2 msec 1 msec
  3 20.3.6.6 1 msec 1 msec 1 msec
  4 20.5.6.5 10 msec *  3 msec
R1#traceroute 6.6.6.6

Type escape sequence to abort.
Tracing the route to 6.6.6.6
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 1 msec 2 msec 1 msec 2 20.2.4.4 1 msec 6 msec 2 msec

  3 20.4.6.6 2 msec *  2 msec
```

In the case that one of these exit points are down, traffic will fall back to the least specific match of 0.0.0.0/0 that is installed due to the Attached (ATT) bit being set in the IS-IS LSDB.

```
R1#show ip cef 6.6.6.6 detail
 6.6.6.6/32, epoch 2
 nexthop 10.1.2.2 GigabitEthernet1.12

R1#traceroute 6.6.6.6

Type escape sequence to abort.
Tracing the route to 6.6.6.6
```

```
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 1 msec 2 msec 1 msec 2 20.2.4.4 1 msec 6 msec 2 msec
  3 20.4.6.6 2 msec *  2 msec

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface Gig1.24R2(config-subif)#shutdown
R2(config-subif)#end
R2#show ip cef 6.6.6.6 detail
 0.0.0.0/0
, epoch 2, flags [default route] nexthop 10.1.2.2 GigabitEthernet1.12
R1#traceroute 6.6.6.6
Type escape sequence to abort.
Tracing the route to 6.6.6.6
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 6 msec 2 20.2.3.3 2 msec 1 msec 1 msec

  3 20.3.6.6 2 msec *  2 msec
```

Route leaking can also be used to filter routes as they are converted from L1 to L2. Previously R6 had equal longest matches to 1.1.1.1/32 and 2.2.2.2/32 via R3 and R4. After route leaking filtering is applied, R6 has only one possible path to each of these destinations.

```
R6#show ip route 1.1.1.1
Routing entry for 1.1.1.1/32
  Known via "isis", distance 115, metric 30, type level-2
  Redistributing via isis
  Last update from 20.3.6.3 on GigabitEthernet1.36, 00:20:33 ago
  Routing Descriptor Blocks:  * 20.3.6.3, from 3.3.3.3, 00:20:33 ago, via GigabitEthernet1.36
      Route metric is 30, traffic share count is 1
R6#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis
  Last update from 20.4.6.4 on GigabitEthernet1.46, 00:00:02 ago
  Routing Descriptor Blocks:  * 20.4.6.4, from 4.4.4.4, 00:00:02 ago, via GigabitEthernet1.46

      Route metric is 20, traffic share count is 1
```

Unlike L2 to L1 route leaking, which allows traffic engineering based on longest match, but still allows for fallback to a default route, filtering of L1 to L2 origination via route leaking does not allow for redundancy. For example in this case that R3 loses its link to the L1 domain, the 1.1.1.1/32 prefix becomes unreachable because R4 is configured to deny origination of this prefix from L1 into L2.

```
R6#show ip route 1.1.1.1
 Routing entry for 1.1.1.1/32
  Known via "isis", distance 115, metric 30, type level-2
  Redistributing via isis
  Last update from 20.3.6.3 on FastEthernet0/0.36, 00:20:02 ago
  Routing Descriptor Blocks: * 20.3.6.3, from 3.3.3.3
, 00:20:02 ago, via FastEthernet0/0.36
      Route metric is 30, traffic share count is 1
 R6#ping 1.1.1.1

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:!!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
 R6#

 R3#conf t
 Enter configuration commands, one per line.  End with CNTL/Z.
 R3(config)#int Gig1.23R3(config-subif)#shut
 R3(config-subif)#end
 R6#show ip route 1.1.1.1
 % Network not in table
 R6#show ip cef 1.1.1.1
 0.0.0.0/0 no route
 R6#ping 1.1.1.1
 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:.....

 Success rate is 0 percent (0/5)
```

Route leaking in IOS XR uses the same logic as regular IOS, however the matching of prefixes occurs through the usage of the Routing Policy Language (RPL).

```
RP/0/0/CPU0:XR1#show rpl
 Tue Apr 28 00:39:42.306 UTC
 route-policy ISIS_ROUTE_LEAKING
   if destination in (3.3.3.3/32, 4.4.4.4/32) then
     pass
   endif
 end-policy
 !
 RP/0/0/CPU0:XR1#show run router isis
```

```
Tue Apr 28 00:40:07.194 UTC
router isis 1
 net 49.1920.0000.0000.0019.00
 address-family ipv4 unicast propagate level 2 into level 1 route-policy ISIS_ROUTE_LEAKING

 !
<snip>
```

The result of this configuration is that XR2 learns the specific routes of 3.3.3.3/32 and 4.4.4.4/32 via XR1.

```
RP/0/0/CPU0:XR2#show route isis
Tue Apr 28 00:42:15.775 UTC

i*L1 0.0.0.0/0 [115/10] via 10.19.20.19, 00:27:24, GigabitEthernet0/0/0/0.1920
i ia 3.3.3.3/32 [115/30] via 10.19.20.19, 00:27:24, GigabitEthernet0/0/0/0.1920
i ia 4.4.4.4/32 [115/30] via 10.19.20.19, 00:27:24, GigabitEthernet0/0/0/0.1920
```

To make this configuration more modular, the RPL policy could have called an external prefixset, similar to a prefix-list in regular IOS, that could be used to match the prefixes in question to be leaked. A configuration such as this could be written as follows:

```
RP/0/0/CPU0:XR1#show rpl
Tue Apr 28 00:44:13.650 UTC
prefix-set ISIS_ROUTES
  3.3.3.3/32,
  4.4.4.4/32
end-set
!
route-policy ISIS_ROUTE_LEAKING
  if destination in ISIS_ROUTES then
    pass
  endif
 end-policy
!
RP/0/0/CPU0:XR1#show run router isis

Tue Apr 28 00:44:18.881 UTC
router isis 1
 net 49.1920.0000.0000.0019.00
 address-family ipv4 unicast
  propagate level 2 into level 1 route-policy ISIS_ROUTE_LEAKING
 !
```

```
<snip>
```

Route-maps can be used to control redistribution in IOS, as shown in this example, in addition to distribute-lists.

When an L1L2 router leaks L2 routes into L1, the routes are advertised in IP Internal Reachability Information TLVs. An important factor about route leaking in ISIS is the setting of the U/D bit within the TLV of the leaked route. This is similar to the "Down" bit in OSPF, and it is paramount in preventing loops. An L1L2 router that receives a route with the U/D bit attached via L1 will not re-advertise this same route into L2. This behavior is described in RFC-2966.

The leaked routes can be observed by looking at the L1L2 router's LSP doing the leaking:

```
RP/0/0/CPU0:XR2#show isis database XR1.00-00 detail

Tue Apr 28 00:48:24.390 UTC

IS-IS 1 (Level-1) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
XR1.00-00             0x00000006   0x1a47        478             1/0/0
  Area Address: 49.1920
  NLPID:        0xcc
  Hostname:     XR1
  IP Address:   19.19.19.19
  Metric: 10         IS XR1.01 Metric: 20         IP-Interarea 3.3.3.3/32
 Metric: 20         IP-Interarea 4.4.4.4/32

  Metric: 10         IP 10.19.20.0/24
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

Single-Topology IS-IS

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IPv4 and IPv6**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 and IPv6 Diagram** in order to complete this task.

- Using the Base IPv4/IPv6 diagram, configure IS-IS Level 2 on all interfaces of all devices.
- Use NET addresses in the format 49.0001.0000.0000.000Y.00, where *Y* is the router number.
- Advertise both the IPv4 and IPv6 addresses of all links using single topology IS-IS.
- Advertise the Loopback interfaces of the routers using the **passive-interface** or **passive** command.

Configuration

```
R1:
interface GigabitEthernet1.12
 ip router isis
 ipv6 router isis
!
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
 passive-interface Loopback0

R2:
interface GigabitEthernet1.23
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.24
 ip router isis
 ipv6 router isis
```

```
!
interface GigabitEthernet1.12
 ip router isis
 ipv6 router isis
!
router isis
 net 49.0001.0000.0000.0002.00
 is-type level-2-only
 passive-interface Loopback0

R3:
interface GigabitEthernet1.23
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.34
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.36
 ip router isis
 ipv6 router isis
!
router isis
 net 49.0001.0000.0000.0003.00
 is-type level-2-only
 passive-interface Loopback0

R4:
interface GigabitEthernet1.24
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.34
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.45
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.46
 ip router isis
 ipv6 router isis
!
router isis
```

```
 net 49.0001.0000.0000.0004.00
 is-type level-2-only
 passive-interface Loopback0

R5:
interface GigabitEthernet1.45
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.56
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.519
 ip router isis
 ipv6 router isis
!
router isis
 net 49.0001.0000.0000.0005.00
 is-type level-2-only
 passive-interface Loopback0

R6:
interface GigabitEthernet1.36
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.46
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.56
 ip router isis
 ipv6 router isis
!
interface GigabitEthernet1.619
 ip router isis
 ipv6 router isis
!
router isis
 net 49.0001.0000.0000.0006.00
 is-type level-2-only
 passive-interface Loopback0

XR1:
router isis 1
```

```
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 address-family ipv6 unicast
  single-topology
 !
 interface Loopback0
  passive
  address-family ipv6 unicast
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.519
  address-family ipv4 unicast
  address-family ipv6 unicast
  !
!
interface GigabitEthernet0/0/0/0.619
  address-family ipv4 unicast
  address-family ipv6 unicast
 !
!
interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 unicast
  address-family ipv6 unicast
  !
 !
!

XR2:
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 address-family ipv6 unicast
  single-topology
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
  address-family ipv6 unicast
 !
!
interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 unicast
  address-family ipv6 unicast
  !
 !
```

```
!
```

Verification

Single Topology IS-IS is used when multiple protocol stacks, such as IPv4 and IPv6, are configured in an identical 1:1 basis on all interfaces in the topology. Since the multi-protocol topology is essentially identical, it allows a single SPF calculation to apply to both protocol stacks at the same time, simplifying the database calculation and protocol overhead of IS-IS. In other words, for single topology IS-IS to work, each interface that runs IPv4 must also run IPv6, and each interface that runs IPv6 must also run IPv4. This is one of the design advantages of IS-IS over OSPFv2, as OSPFv2 and OSPFv3 are unrelated protocols used to route IPv4 and IPv6 respectively, while IS-IS can route both with a single calculation, arguably resulting in a more efficient design. Note however that there is a newer version of OSPFv3 which is Multi-Address Family aware, and can route IPv4 and IPv6 under the same instance.

By default, IS-IS instances in regular IOS run in Single Topology mode, while IOS XR IS-IS instances run in Multi Topology mode. These modes are not compatible with each other and must be configured to match, or to run in transition mode. In this example Single Topology is run on all devices since the IPv4 and IPv6 topology is on a 1:1 basis.

From an operational point of view as seen below, IS-IS still maintains a single adjacency between devices even though it is routing both IPv4 and IPv6, as opposed to OSPF which would require a separate OSPFv2 and OSPFv3 adjacency to accomplish the same design. Even the Multi-AF version of OSPFv3 requires separate adjacencies per address family.

```
R6#show isis neighbors

System Id      Type Interface    IP Address      State Holdtime Circuit Id
R3             L2   Gi1.36       20.3.6.3        UP    9        R3.03
R4             L2   Gi1.46       20.4.6.4        UP    21       R6.02
R5             L2   Gi1.56       20.5.6.5        UP    24       R6.03
XR1            L2   Gi1.619      20.6.19.19      UP    24       R6.04


RP/0/0/CPU0:XR1#show isis adjacency

Wed Apr 29 22:34:57.021 UTC

IS-IS 1 Level-2 adjacencies:
System Id      Interface        SNPA           State Hold Changed  NSF IPv4 IPv6
```

```
                                                                      BFD  BFD
R6             Gi0/0/0/0.619    0050.569e.5cec Up    7    00:06:38 Yes None None
R5             Gi0/0/0/0.519    0050.569e.0962 Up    23   00:03:14 Yes None None
XR2            Gi0/0/0/0.1920   0050.569e.27ac Up    25   00:06:30 Yes None None

Total adjacency count: 3
```

From the surface the database structure looks identical to normal IPv4 only IS-IS, i.e. Integrated IS-IS.

```
R6#show isis database


IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000003   0x21E6        561               0/0/0
R1.01-00              0x00000001   0x21B9        562               0/0/0
R2.00-00              0x00000005   0x8997        577               0/0/0
R2.02-00              0x00000001   0x5283        578               0/0/0
R3.00-00              0x00000005   0x3FA2        745               0/0/0
R3.01-00              0x00000001   0x2DA9        573               0/0/0
R3.02-00              0x00000001   0x587B        580               0/0/0
R3.03-00              0x00000001   0x834D        746               0/0/0
R4.00-00              0x00000EAF   0x2776        963               0/0/0
R4.03-00              0x00000001   0x705F        964               0/0/0
R5.00-00              0x00000005   0xB7B2        987               0/0/0
R6.00-00            * 0x00000006   0x995A        989               0/0/0
R6.02-00            * 0x00000001   0x6A63        748               0/0/0
R6.03-00            * 0x00000002   0x7A50        986               0/0/0
R6.04-00            * 0x00000001   0x6B4B        763               0/0/0
XR1.00-00             0x00000005   0x9052        813               0/0/0
XR1.01-00             0x00000001   0xA2E9        768               0/0/0
XR1.05-00             0x00000003   0xDCC4        982               0/0/0
XR2.00-00             0x00000004   0x50B7        820               0/0/0
RP/0/0/CPU0:XR1#show isis database


Wed Apr 29 22:36:01.976 UTC


IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00              0x00000003   0x21e6        575             0/0/0
R1.01-00              0x00000001   0x21b9        576             0/0/0
R2.00-00              0x00000005   0x8997        591             0/0/0
R2.02-00              0x00000001   0x5283        592             0/0/0
R3.00-00              0x00000005   0x3fa2        758             0/0/0
R3.01-00              0x00000001   0x2da9        587             0/0/0
```

```
R3.02-00              0x00000001   0x587b        594             0/0/0
R3.03-00              0x00000001   0x834d        759             0/0/0
R4.00-00              0x00000eaf   0x2776        937             0/0/0
R4.03-00              0x00000001   0x705f        938             0/0/0
R5.00-00              0x00000005   0xb7b2        964             0/0/0
R6.00-00              0x00000006   0x995a        962             0/0/0
R6.02-00              0x00000001   0x6a63        761             0/0/0
R6.03-00              0x00000002   0x7a50        960             0/0/0
R6.04-00              0x00000001   0x6b4b        787             0/0/0
XR1.00-00           * 0x00000005   0x9052        790             0/0/0
XR1.01-00             0x00000001   0xa2e9        788             0/0/0
XR1.05-00             0x00000003   0xdcc4        959             0/0/0
XR2.00-00             0x00000004   0x50b7        796             0/0/0

 Total Level-2 LSP count: 19     Local Level-2 LSP count: 1
```

When we look into the details of the database, the difference becomes evident that both IPv4 and IPv6 attributes are now associated with the link states. Additionally, a new NLPID (Network Layer Protocol ID) is advertised in the Supported Protocols TLV: 0x8E. This protocol ID represents IPv6, 0xCC is for IPv4.

```
R6#show isis database R1.00-00 detail



IS-IS Level-2 LSP R1.00-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000004   0x1FE7        1184              0/0/0
  Area Address: 49.0001 NLPID:        0xCC 0x8E

  Hostname: R1
  Metric: 10         IS R1.01
  IP Address:   1.1.1.1
  Metric: 10         IP 10.1.2.0 255.255.255.0
  Metric: 0          IP 1.1.1.1 255.255.255.255 IPv6 Address: 2001::1:1:1:1
 Metric: 10          IPv6 2001:10:1:2::/64
 Metric: 0           IPv6 2001::1:1:1:1/128

RP/0/0/CPU0:XR1#show isis database R1.00-00 detail

Wed Apr 29 22:36:32.884 UTC

IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00              0x00000003   0x21e6        544             0/0/0
```

```
  Area Address: 49.0001 NLPID:        0xcc
NLPID:        0x8e
  Hostname:     R1
  Metric: 10         IS R1.01
  IP Address:   1.1.1.1
  Metric: 10         IP 10.1.2.0/24
  Metric: 0          IP 1.1.1.1/32 IPv6 Address: 2001::1:1:1:1
Metric: 10         IPv6 2001:10:1:2::/64
Metric: 0          IPv6 2001::1:1:1:1/128
```

From the routing table and forwarding plane's point of view, the result is the same as if the IPv4 and IPv6 FIBs had been populated by two separate protocols.

```
R1#show ip route isis
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
i L2     2.2.2.2 [115/10] via 10.1.2.2, 00:17:53, GigabitEthernet1.12
      3.0.0.0/32 is subnetted, 1 subnets
i L2     3.3.3.3 [115/20] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
      4.0.0.0/32 is subnetted, 1 subnets
i L2     4.4.4.4 [115/20] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
      5.0.0.0/32 is subnetted, 1 subnets
i L2     5.5.5.5 [115/30] via 10.1.2.2, 00:11:17, GigabitEthernet1.12
      6.0.0.0/32 is subnetted, 1 subnets
i L2     6.6.6.6 [115/30] via 10.1.2.2, 00:14:55, GigabitEthernet1.12
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
i L2     10.19.20.0/24 [115/50] via 10.1.2.2, 00:14:38, GigabitEthernet1.12
      20.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
i L2     20.2.3.0/24 [115/20] via 10.1.2.2, 00:17:53, GigabitEthernet1.12
i L2     20.2.4.0/24 [115/20] via 10.1.2.2, 00:17:53, GigabitEthernet1.12
i L2     20.3.4.0/24 [115/30] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
i L2     20.3.6.0/24 [115/30] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
i L2     20.4.5.0/24 [115/30] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
```

```
i L2     20.4.6.0/24 [115/30] via 10.1.2.2, 00:17:43, GigabitEthernet1.12
i L2     20.5.6.0/24 [115/40] via 10.1.2.2, 00:11:17, GigabitEthernet1.12
i L2     20.5.19.0/24 [115/40] via 10.1.2.2, 00:11:17, GigabitEthernet1.12
i L2     20.6.19.0/24 [115/40] via 10.1.2.2, 00:14:55, GigabitEthernet1.12
i L2     20.20.20.20/32 [115/50] via 10.1.2.2, 00:13:48, GigabitEthernet1.12

R1#show ipv6 route isis
IPv6 Routing Table - default - 22 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       a - Application
I2  2001::2:2:2:2/128 [115/10]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::3:3:3:3/128 [115/20]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::4:4:4:4/128 [115/20]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::5:5:5:5/128 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::6:6:6:6/128 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::19:19:19:19/128 [115/40]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001::20:20:20:20/128 [115/50]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:10:19:20::/64 [115/50]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:2:3::/64 [115/20]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:2:4::/64 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:3:4::/64 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:3:6::/64 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:4:2::/64 [115/20]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:4:5::/64 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:4:6::/64 [115/30]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
```

```
I2  2001:20:5:6::/64 [115/40]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:5:19::/64 [115/40]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
I2  2001:20:6:19::/64 [115/40]
     via FE80::250:56FF:FE9E:35D1, GigabitEthernet1.12
```

RP/0/3/CPU0:XR2#show route ipv4 isis

```
Wed Apr 29 22:44:05.553 UTC

i L2 1.1.1.1/32 [115/40] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                [115/40] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 2.2.2.2/32 [115/30] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                [115/30] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 3.3.3.3/32 [115/20] via 20.6.19.6, 00:14:55, GigabitEthernet0/0/0/0.619
i L2 4.4.4.4/32 [115/20] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                [115/20] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 5.5.5.5/32 [115/10] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 6.6.6.6/32 [115/10] via 20.6.19.6, 00:14:55, GigabitEthernet0/0/0/0.619
i L2 10.1.2.0/24 [115/40] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                 [115/40] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 20.2.3.0/24 [115/30] via 20.6.19.6, 00:14:55, GigabitEthernet0/0/0/0.619
i L2 20.2.4.0/24 [115/30] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                 [115/30] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 20.3.4.0/24 [115/30] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                 [115/30] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 20.3.6.0/24 [115/20] via 20.6.19.6, 00:14:55, GigabitEthernet0/0/0/0.619
i L2 20.4.5.0/24 [115/20] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 20.4.6.0/24 [115/20] via 20.6.19.6, 00:14:55, GigabitEthernet0/0/0/0.619
i L2 20.5.6.0/24 [115/20] via 20.6.19.6, 00:12:17, GigabitEthernet0/0/0/0.619
                 [115/20] via 20.5.19.5, 00:12:17, GigabitEthernet0/0/0/0.519
i L2 20.20.20.20/32 [115/10] via 10.19.20.20, 00:14:55, GigabitEthernet0/0/0/0.1920
```

RP/0/3/CPU0:XR2#show route ipv6 isis

```
Wed Apr 29 22:44:10.183 UTC

i L2 2001::1:1:1:1/128
     [115/40] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/40] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001::2:2:2:2/128
     [115/30] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/30] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001::3:3:3:3/128
     [115/20] via fe80::250:56ff:fe9e:5cec, 00:14:59, GigabitEthernet0/0/0/0.619
i L2 2001::4:4:4:4/128
     [115/20] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
```

```
     [115/20] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001::5:5:5:5/128
     [115/10] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001::6:6:6:6/128
     [115/10] via fe80::250:56ff:fe9e:5cec, 00:14:59, GigabitEthernet0/0/0/0.619
i L2 2001::20:20:20:20/128
     [115/10] via fe80::250:56ff:fe9e:27ac, 00:14:59, GigabitEthernet0/0/0/0.1920
i L2 2001:10:1:2::/64
     [115/40] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/40] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001:20:2:3::/64
     [115/30] via fe80::250:56ff:fe9e:5cec, 00:14:59, GigabitEthernet0/0/0/0.619
i L2 2001:20:2:4::/64
     [115/30] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/30] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001:20:3:4::/64
     [115/30] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/30] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001:20:3:6::/64
     [115/20] via fe80::250:56ff:fe9e:5cec, 00:14:59, GigabitEthernet0/0/0/0.619
i L2 2001:20:4:2::/64
     [115/40] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
     [115/40] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001:20:4:5::/64
     [115/20] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
i L2 2001:20:4:6::/64
  [115/20] via fe80::250:56ff:fe9e:5cec, 00:14:59, GigabitEthernet0/0/0/0.619
i L2 2001:20:5:6::/64
  [115/20] via fe80::250:56ff:fe9e:5cec, 00:12:21, GigabitEthernet0/0/0/0.619
  [115/20] via fe80::250:56ff:fe9e:962, 00:12:21, GigabitEthernet0/0/0/0.519
```

The final result is that all devices should have full IPv4 and IPv6 reachability to each other.

```
R1#ping 20.20.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/11 ms
R1#ping 2001::20:20:20:20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20:20:20:20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/19/32 ms
RP/0/0/CPU0:XR2#ping 1.1.1.1
```

```
Wed Apr 29 22:45:50.866 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
RP/0/0/CPU0:XR2#ping 2001::1:1:1:1

Wed Apr 29 22:45:59.166 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/19/19 ms
```

Note that IPv4 and IPv6 traffic must follow the same path throughout the network now, as the Shortest Path Tree for each of them are the same.

```
R1#traceroute 20.20.20.20
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 1 msec 2 msec 1 msec
  2 20.2.3.3 1 msec 1 msec 6 msec
  3 20.3.6.6 2 msec 1 msec 1 msec
  4 20.6.19.19 9 msec 12 msec 13 msec
  5 10.19.20.20 13 msec *  3 msec
R1#traceroute 2001::20:20:20:20

Type escape sequence to abort.
Tracing the route to 2001::20:20:20:20

  1 2001:10:1:2::2 3 msec 2 msec 1 msec
  2 2001:20:2:3::3 2 msec 1 msec 6 msec
  3 2001:20:3:6::6 4 msec 15 msec 14 msec
  4 2001:20:6:19::19 17 msec 12 msec 22 msec
  5 2001::20:20:20:20 28 msec 20 msec 20 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 2: IGP v4

Multi-Topology IS-IS

- Configure IS-IS to run in Multi Topology mode on all devices.
- Change the IS-IS metric on the path from R2 to R3 to R6 to XR1 and back so that IPv4 traffic between R1 and XR2 prefers to use R4 and R5 in the transit path.
- Change the IS-IS metric on the path from R2 to R4 to R5 to XR1 and back so that IPv6 traffic between R1 and XR2 prefers to use R3 and R6 in the transit path.

Configuration

```
R1:
router isis
 metric-style wide
 !
 address-family ipv6
  multi-topology

R2:
interface GigabitEthernet1.23
 isis metric 20
!
interface GigabitEthernet1.24
 isis ipv6 metric 20
!
 router isis
   metric-style wide
 !
address-family ipv6
multi-topology

R3:
interface GigabitEthernet1.36
 isis metric 20
!
router isis
 metric-style wide
```

```
 !
 address-family ipv6
  multi-topology

R4:
interface GigabitEthernet1.24
 isis ipv6 metric 20
!
interface GigabitEthernet1.45
 isis ipv6 metric 20
!
router isis
 metric-style wide
 !
 address-family ipv6
  multi-topology

R5:
interface GigabitEthernet1.45
 isis ipv6 metric 20
!
interface GigabitEthernet1.519
 isis ipv6 metric 20
!
router isis
 metric-style wide
 !
 address-family ipv6
  multi-topology

R6:
interface GigabitEthernet1.36
 isis metric 20
!
interface GigabitEthernet1.619
 isis metric 20
!
router isis
 metric-style wide
 !
 address-family ipv6
  multi-topology

XR1:
router isis 1
 address-family ipv4 unicast
```

```
  metric-style wide
 !
 address-family ipv6 unicast
  metric-style wide
  no single-topology
 !
 interface GigabitEthernet0/0/0/0.519
  address-family ipv6 unicast
   metric 20
  !
 !
 interface GigabitEthernet0/0/0/0.619
  address-family ipv4 unicast
   metric 20
  !
 !
!

XR2:
router isis 1
 address-family ipv4 unicast
  metric-style wide
 !
 address-family ipv6 unicast
  metric-style wide
  no single-topology
 !
!
```

Verification

In Multi Topology IS-IS, separate protocol stacks maintain separate database structures and use separate SPF runs, which means that one topology is independent of another. Multi Topology IS-IS is most useful in practical IPv4 to IPv6 migration scenarios, where IPv6 is slowly introduced to the already existing IPv4 core. During migration the IPv4 and IPv6 topologies are kept separate from a database calculation point of view inside of IS-IS. Once the migration is complete and IPv4 and IPv6 run on a 1:1 basis with each other, Single Topology IS-IS can be enabled, which means that both IPv4 and IPv6 topology share the same database and SPF run. Note that this design is only possible if IPv4 runs on all interfaces that IPv6 runs on and vice-versa, otherwise database inconsistencies can occur which can result in loss of reachability in the network.

Prior to making any changes to the previous example, R1's IPv4 and IPv6 traffic follow the same path to reach XR2.

```
R1#traceroute 20.20.20.20

 Type escape sequence to abort.
 Tracing the route to 20.20.20.20

  1  10.1.2.2    0   msec    0   msec    0  msec
  2  20.2.3.3    0   msec    4   msec    0  msec
  3  20.3.6.6    0   msec    4   msec    0  msec
  4  20.6.19.19  0   msec    0   msec    4  msec
  5  10.19.20.20 4   msec *  4   msec
 R1#traceroute 2001::20:20:20:20


 Type escape sequence to abort.
 Tracing the route to 2001::20:20:20:20

  1 2000:10:1:2::2    8 msec  0  msec  0  msec
  2 2000:20:2:3::3    8 msec  4  msec  0  msec
  3 2000:20:3:6::6    8 msec  12 msec  0  msec
  4 2000:20:6:19::19  4 msec  4  msec  0  msec
  5 2000::20:20:20:20 8 msec  4  msec  4  msec
```

After the Multi Topology and metric changes, IPv4 traffic follows the path along the bottom of the topology through R4 and R5, while IPv6 traffic follows the path along the top of the topology through R3 and R6.

```
R1#traceroute 20.20.20.20
 Type escape sequence to abort.
 Tracing the route to 20.20.20.20
 VRF info: (vrf in name/id, vrf out name/id)
   1 10.1.2.2 4 msec 1 msec 6 msec
   2 20.2.4.4 2 msec 1 msec 1 msec
   3 20.4.5.5 1 msec 1 msec 1 msec
   4 20.5.19.19 8 msec 12 msec 13 msec
   5 10.19.20.20 13 msec *  3 msec

 R1#traceroute 2001::20:20:20:20
 Type escape sequence to abort.
 Tracing the route to 2001::20:20:20:20

   1 2001:10:1:2::2 4 msec 2 msec 1 msec
   2 2001:20:2:3::3 2 msec 1 msec 6 msec
```

```
  3 2001:20:3:6::6 5 msec 15 msec 14 msec
  4 2001:20:6:19::19 16 msec 13 msec 15 msec
  5 2001::20:20:20:20 24 msec 20 msec 20 msec

R2#show ip route 20.20.20.20
Routing entry for 20.20.20.20/32
  Known via "isis", distance 115, metric 40, type level-2
  Redistributing via isis
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:04:25 ago
  Routing Descriptor Blocks:  * 20.2.4.4, from 20.20.20.20, 00:04:25 ago, via GigabitEthernet1.24
      Route metric is 40, traffic share count is 1
R2#show ipv6 route 2001::20:20:20:20

Routing entry for 2001::20:20:20:20/128
  Known via "isis", distance 115, metric 40, type level-2
  Route count is 1/1, share count 0
  Routing paths: FE80::250:56FF:FE9E:6E6A, GigabitEthernet1.23
      Last updated 00:04:10 ago

RP/0/0/CPU0:XR2#traceroute 1.1.1.1
Wed Apr 29 23:24:16.468 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 0 msec  0 msec  0 msec
 3  20.4.5.4 0 msec  0 msec  0 msec
 4  20.2.4.2 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  0 msec
RP/0/0/CPU0:XR2#traceroute 2001::1:1:1:1
Wed Apr 29 23:24:45.326 UTC

Type escape sequence to abort.
Tracing the route to 2001::1:1:1:1

 1  2001:10:19:20::19 19 msec 19 msec 9 msec
 2  2001:20:6:19::6 9 msec 9 msec 9 msec
 3  2001:20:3:6::3 9 msec 9 msec 9 msec
 4  2001:20:2:3::2 69 msec 19 msec 9 msec
 5  2001:10:1:2::1 9 msec 9 msec 9 msec

RP/0/0/CPU0:XR1#show route ipv4 1.1.1.1
Wed Apr 29 23:27:27.715 UTC

Routing entry for 1.1.1.1/32
```

```
  Known via "isis 1", distance 115, metric 40, type level-2
  Installed Apr 29 23:21:42.999 for 00:05:44
  Routing Descriptor Blocks 20.5.19.5, from 1.1.1.1, via GigabitEthernet0/0/0/0.519
      Route metric is 40
  No advertising protos.
RP/0/0/CPU0:XR1#show route ipv6 2001::1:1:1:1
Wed Apr 29 23:27:40.274 UTC

Routing entry for 2001::1:1:1:1/128
  Known via "isis 1", distance 115, metric 50, type level-2
  Installed Apr 29 23:21:41.289 for 00:05:59
  Routing Descriptor Blocks fe80::250:56ff:fe9e:5cec, from 2001::1:1:1:1, via GigabitEthernet0/0/0/0.619

      Route metric is 50
  No advertising protos.
```

When we look at the detailed view of the IS-IS database we can see that the IPv6 information is encoded as MT for Multi Topology, and that separate IPv4 and IPv6 metrics can exist. Note that Wide Metric Style is required in order to encode the Multi Topology information in the database.

```
RP/0/0/CPU0:XR2#show isis database R1.00-00 detail

Wed Apr 29 23:28:59.849 UTC

IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00              0x00000005   0xc206        720             0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  NLPID:        0x8e MT:           Standard (IPv4 Unicast)
 MT:           IPv6 Unicast
                                     0/0/0
  Hostname:     R1
  Metric: 10         IS-Extended R1.01
  Metric: 10         MT (IPv6 Unicast) IS-Extended R1.01
  IP Address:   1.1.1.1
  Metric: 0          IP-Extended 1.1.1.1/32
  Metric: 10         IP-Extended 10.1.2.0/24
  IPv6 Address: 2001::1:1:1:1
  Metric: 10         MT (IPv6 Unicast) IPv6 2001::1:1:1:1/128
  Metric: 10         MT (IPv6 Unicast) IPv6 2001:10:1:2::/64
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

Basic LDP

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Statically set their MPLS LDP Router-IDs to be their Loopback0 interfaces.

Configuration

```
R2:
mpls label protocol ldp
!
interface GigabitEthernet1.23
 mpls ip
!
interface GigabitEthernet1.24
 mpls ip
!
mpls ldp router-id Loopback0

R3:
mpls label protocol ldp
!
interface GigabitEthernet1.23
 mpls ip
!
interface GigabitEthernet1.34
 mpls ip
!
interface GigabitEthernet1.36
 mpls ip
!
```

```
mpls ldp router-id Loopback0

R4:
mpls label protocol ldp
!
interface GigabitEthernet1.24
 mpls ip
!
interface GigabitEthernet1.34
 mpls ip
!
interface GigabitEthernet1.45
 mpls ip
!
interface GigabitEthernet1.46
 mpls ip
!
mpls ldp router-id Loopback0

R5:
mpls label protocol ldp
!
interface GigabitEthernet1.45
 mpls ip
!
interface GigabitEthernet1.56
 mpls ip
!
interface GigabitEthernet1.519
 mpls ip
!
mpls ldp router-id Loopback0

R6:
mpls label protocol ldp
!
interface GigabitEthernet1.36
 mpls ip
!
interface GigabitEthernet1.46
 mpls ip
!
interface GigabitEthernet1.56
 mpls ip
!
interface GigabitEthernet1.619
```

```
 mpls ip
!
mpls ldp router-id Loopback0

XR1:
mpls ldp
 router-id 19.19.19.19
 interface GigabitEthernet0/0/0/0.519
 !
 interface GigabitEthernet0/0/0/0.619
 !
!
```

Verification

show mpls interfaces is a good way to quickly verify that LDP, TDP, RSVP, BGP, etc. labeling is enabled on the correct links.

```
R6#show mpls interfaces
   Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet1.36    Yes (ldp)     No        No  No     Yes
GigabitEthernet1.46    Yes (ldp)     No        No  No     Yes
GigabitEthernet1.56    Yes (ldp)     No        No  No     Yes
GigabitEthernet1.619   Yes (ldp)     No        No  No     Yes
RP/0/0/CPU0:XR1#show mpls interfaces
Thu Apr 30 00:28:10.775 UTC
Interface                 LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------GigabitEthernet0/0/0/0.519 Yes
      No       No Yes
GigabitEthernet0/0/0/0.619 Yes      No       No Yes
```

All routers should have formed an LDP adjacency with their directly connected neighbors. Note that this adjacency requires an IGP route to the Transport Address of the LDP session (similar to the BGP update source), which will be the highest Loopback address by default, the same as the LDP Router-ID.

```
R6#show mpls ldp neighbor
 Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 6.6.6.6:0
 TCP connection: 3.3.3.3.646 - 6.6.6.6.31475
 State: Oper
; Msgs sent/rcvd: 24/24; Downstream
    Up time: 00:01:55
    LDP discovery sources:
```

```
      GigabitEthernet1.36, Src IP addr: 20.3.6.3
    Addresses bound to peer LDP Ident:
      20.2.3.3        20.3.4.3        20.3.6.3        3.3.3.3
Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 6.6.6.6:0
 TCP connection: 4.4.4.4.646 - 6.6.6.6.29814
 State: Oper
; Msgs sent/rcvd: 24/24; Downstream
    Up time: 00:01:55
    LDP discovery sources:
      GigabitEthernet1.46, Src IP addr: 20.4.6.4
    Addresses bound to peer LDP Ident:
      20.2.4.4        20.3.4.4        20.4.5.4        20.4.6.4
      4.4.4.4          Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 6.6.6.6:0
 TCP connection: 5.5.5.5.646 - 6.6.6.6.44270
 State: Oper
; Msgs sent/rcvd: 24/24; Downstream
    Up time: 00:01:55
    LDP discovery sources:
      GigabitEthernet1.56, Src IP addr: 20.5.6.5
    Addresses bound to peer LDP Ident:
      20.4.5.5        20.5.6.5        20.5.19.5       5.5.5.5
Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 6.6.6.6:0
 TCP connection: 19.19.19.19.64567 - 6.6.6.6.646
 State: Oper
; Msgs sent/rcvd: 23/24; Downstream
    Up time: 00:01:39
    LDP discovery sources:
      GigabitEthernet1.619, Src IP addr: 20.6.19.19
    Addresses bound to peer LDP Ident:
      20.5.19.19      20.6.19.19      10.19.20.19     19.19.19.19
RP/0/0/CPU0:XR1#show mpls ldp neighbor


Thu Apr 30 00:32:41.907 UTC


Peer LDP Identifier: 5.5.5.5:0
  TCP connection: 5.5.5.5:646 - 19.19.19.19:12149
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 27/27; Downstream-Unsolicited
  Up time: 00:05:02
  LDP Discovery Sources:
      GigabitEthernet0/0/0/0.519
  Addresses bound to this peer:
      5.5.5.5        20.4.5.5       20.5.6.5       20.5.19.5


Peer LDP Identifier: 6.6.6.6:0
```

```
  TCP connection: 6.6.6.6:646 - 19.19.19.19:64567
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 28/27; Downstream-Unsolicited
  Up time: 00:05:02
  LDP Discovery Sources:
      GigabitEthernet0/0/0/0.619
  Addresses bound to this peer:
      6.6.6.6         20.3.6.6        20.4.6.6        20.5.6.6
      20.6.19.6
```

Once the LDP adjacencies are formed, labels should be advertised for all IGP learned prefixes, along with all connected interfaces running IGP and LDP. *Pop Label* in the below output indicates that the local device is the Penultimate Hop (next-to-last hop), and that the top-most label in the MPLS stack should be removed when forwarding traffic towards the destination. *No Label* or *Unlabeled*, as seen in XR1's output on the link towards XR2, indicates that the outgoing interface is not running MPLS, and that the entire MPLS stack should be removed when forwarding traffic towards that link. Normally in the MPLS core you should not see the *No Label* or *Unlabeled* output; this should only be seen on the edge of the network.

```
R6#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         16         1.1.1.1/32       0             Gi1.36     20.3.6.3
           16         1.1.1.1/32       0             Gi1.46     20.4.6.4
17         17         2.2.2.2/32       0             Gi1.36     20.3.6.3
           17         2.2.2.2/32       0             Gi1.46     20.4.6.4
18         Pop Label  3.3.3.3/32       0             Gi1.36     20.3.6.3

19         Pop Label  4.4.4.4/32       0             Gi1.46     20.4.6.4
20         Pop Label  5.5.5.5/32       0             Gi1.56     20.5.6.5
21         21         10.1.2.0/24      0             Gi1.36     20.3.6.3
           21         10.1.2.0/24      0             Gi1.46     20.4.6.4
22         Pop Label  10.19.20.0/24    0             Gi1.619    20.6.19.19
23         Pop Label  19.19.19.19/32   0             Gi1.619    20.6.19.19
24         Pop Label  20.2.3.0/24      0             Gi1.36     20.3.6.3
25         Pop Label  20.2.4.0/24      0             Gi1.46     20.4.6.4
26         Pop Label  20.3.4.0/24      0             Gi1.36     20.3.6.3
           Pop Label  20.3.4.0/24      0             Gi1.46     20.4.6.4
27         Pop Label  20.4.5.0/24      0             Gi1.46     20.4.6.4
           Pop Label  20.4.5.0/24      0             Gi1.56     20.5.6.5
28         Pop Label  20.5.19.0/24     0             Gi1.56     20.5.6.5
           Pop Label  20.5.19.0/24     0             Gi1.619    20.6.19.19
29         16014      20.20.20.20/32   0             Gi1.619    20.6.19.19
```

```
RP/0/0/CPU0:XR1#show mpls forwarding

Thu Apr 30 00:34:10.141 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  18          3.3.3.3/32         Gi0/0/0/0.619 20.6.19.6       0
16001  Pop         6.6.6.6/32         Gi0/0/0/0.619 20.6.19.6       726
16002  Pop         20.4.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16003  Pop         20.3.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16004  24          20.2.3.0/24        Gi0/0/0/0.619 20.6.19.6       0
16005  16          1.1.1.1/32         Gi0/0/0/0.519 20.5.19.5       0
       16          1.1.1.1/32         Gi0/0/0/0.619 20.6.19.6       0
16006  17          2.2.2.2/32         Gi0/0/0/0.519 20.5.19.5       0
       17          2.2.2.2/32         Gi0/0/0/0.619 20.6.19.6       0
16007  19          4.4.4.4/32         Gi0/0/0/0.519 20.5.19.5       0
       19          4.4.4.4/32         Gi0/0/0/0.619 20.6.19.6       0
16008  Pop         5.5.5.5/32         Gi0/0/0/0.519 20.5.19.5       726
16009  Pop         20.5.6.0/24        Gi0/0/0/0.519 20.5.19.5       0
       Pop         20.5.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16010  Pop         20.4.5.0/24        Gi0/0/0/0.519 20.5.19.5       0
16011  26          20.3.4.0/24        Gi0/0/0/0.519 20.5.19.5       0
       26          20.3.4.0/24        Gi0/0/0/0.619 20.6.19.6       0
16012  25          20.2.4.0/24        Gi0/0/0/0.519 20.5.19.5       0
       25          20.2.4.0/24        Gi0/0/0/0.619 20.6.19.6       0
16013  21          10.1.2.0/24        Gi0/0/0/0.519 20.5.19.5       0
       21          10.1.2.0/24        Gi0/0/0/0.619 20.6.19.6       0
16014  Unlabelled  20.20.20.20/32     Gi0/0/0/0.1920 10.19.20.20     0
```

Each device keeps a data structure for each prefix to label binding. XR1 created local label 16000 for 3.3.3.3/32. This label binding is being advertised to R5 and R6, outlining the downstream unsolicited label allocation mode of LDP. R5 and R6 each advertise their local label binding for 3.3.3.3/32, which is label 18 for both.

```
RP/0/0/CPU0:XR1#show mpls ldp bindings 3.3.3.3/32 detail

Thu Apr 30 00:35:14.336 UTC 3.3.3.3/32
, rev 24 Local binding: label: 16000
 Advertised to: (2 peers)
            5.5.5.5:0          6.6.6.6:0
          Acked by: (2 peers)
            5.5.5.5:0          6.6.6.6:0          Remote bindings: (2 peers)

            Peer                Label       Stale
```

```
    ----------------   ---------   -----
    5.5.5.5:0          18           N
    6.6.6.6:0          18           N
```

Traceroutes from R1 and XR2 indicate the traffic between them is normal unlabeled IPv4 traffic on their links to R2 and XR1 respectively, but is MPLS label switched when it goes into the core of the network. The label values seen in the traceroute output will vary depending on the particular destination you are trying to reach.

```
R1#traceroute 20.20.20.20
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec
  2 20.2.4.4 [MPLS: Label 29 Exp 0] 12 msec 12 msec 12 msec
  3 20.4.5.5 [MPLS: Label 30 Exp 0] 12 msec 12 msec 12 msec
  4 20.5.19.19 [MPLS: Label 16014 Exp 0] 12 msec 16 msec 16 msec
  5 10.19.20.20 20 msec *  12 msec

RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Thu Apr 30 00:43:10.494 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 9 msec  0 msec  0 msec
 2  20.5.19.5 [MPLS: Label 16 Exp 0] 9 msec  0 msec  0 msec
 3  20.4.5.4 [MPLS: Label 16 Exp 0] 9 msec  0 msec  0 msec
 4  20.2.4.2 [MPLS: Label 16 Exp 0] 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  0 msec
```

Input and output labels along the transit path can be tracked by looking at the mpls forwarding table, or by viewing the output of **debug mpls packet**. Rx indicates packets received, while tx indicates packets transmitted. Rx packets should have their label values correlated with the *Local Label* field in the **show mpls forwarding-table** output, while tx with the *Outgoing Label* value. Note that the CSR1000v does not support debugging of mpls packets.

According to the traceroute from R1 to XR2, R2 is pushing label 29 as the packets are being forwarded towards 20.20.20.20. At this point, R2 does a routing lookup, encapsulates the packets with a single label, and forwards them towards R4.

```
R2#show mpls forwarding-table 20.20.20.20

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
30         30         20.20.20.20/32   0             Gi1.23     20.2.3.3
29         20.20.20.20/32   0             Gi1.24     20.2.4.4

R2#show ip cef 20.20.20.20 detail

20.20.20.20/32, epoch 2, per-destination sharing
  local label info: global/30
  nexthop 20.2.3.3 GigabitEthernet1.23 label 30 nexthop 20.2.4.4 GigabitEthernet1.24 label 29
```

R4 receives the labeled packet and does a lookup in the LFIB, resulting in a label SWAP operation. The packet is forwarded towards R5 as label 29 is swapped with label 30. Notice that the 'Bytes Switched' counter is increasing for this entry.

```
R4#show mpls forwarding-table labels 29

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface              29
30         20.20.20.20/32   5998          Gi1.45     20.4.5.5

           29         20.20.20.20/32   0             Gi1.46     20.4.6.6
```

R5 receives the labeled packet and performs a similar operation - SWAP.

```
R5#show mpls forwarding-table labels 30

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
30         16014      20.20.20.20/32   6372          Gi1.519    20.5.19.19
```

XR1 receives the labeled packet, removes the label, and forwards the unlabeled packet towards XR2.

```
RP/0/0/CPU0:XR1#show mpls forwarding |  utility egrep "16014"

Thu Apr 30 01:04:55.554 UTC
16014  Unlabelled  20.20.20.20/32     Gi0/0/0.1920 10.19.20.20     8414
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP OSPF Autoconfig

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Using MPLS LDP Autoconfig in OSPF, configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Statically set their MPLS LDP Router-IDs to be their Loopback0 interfaces.

Configuration

```
R2:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R3:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R4:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R5:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
```

```
R6:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

XR1:
router ospf 1
 mpls ldp auto-config
!
mpls ldp
 router-id 19.19.19.19
!
```

Verification

Similar to the previous example, LDP is enabled on the interfaces running IGP of the routers. The only difference from this config and the previous one, other than the obvious shortcut in the syntax of enabling LDP once globally, is that LDP is running on the edge interfaces of R2 connecting to R1 and of XR1 connecting to XR2.

```
R2#show mpls interfaces

Interface              IP            Tunnel   BGP Static OperationalGigabitEthernet1.23     Yes (ldp)
     No        No  No      Yes         GigabitEthernet1.24     Yes (ldp)
     No        No  No      Yes         GigabitEthernet1.12     Yes (ldp)
     No        No  No      Yes
RP/0/0/CPU0:XR1#show mpls interfaces
Thu Apr 30 03:19:15.532 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------GigabitEthernet0/0/0/0.519 Yes
      No       No       YesGigabitEthernet0/0/0/0.619 Yes
      No       No       YesGigabitEthernet0/0/0/0.1920 Yes
     No       No       Yes
```

If desired these interfaces could have LDP selectively *disabled* as follows, not with the **no mpls ip** command, but with the **no mpls ldp igp autoconfig** in regular IOS.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int Gig1.12R2(config-if)#no mpls ip
% LDP remains enabled on interface Gi1.12 by autoconfig.
```

```
 Autoconfig can be removed from Gi1.12 with 'no mpls ldp igp autoconfig.'
R2(config-if)#no mpls ldp igp autoconfig

R2(config-if)#end R2#
%SYS-5-CONFIG_I: Configured from console by consoleR2#show mpls interfaces
Interface              IP            Tunnel   BGP Static OperationalGigabitEthernet1.23      Yes (ldp)
     No       No  No      Yes         GigabitEthernet1.24     Yes (ldp)
    No       No  No      Yes
```

In IOS XR autoconfig can be selectively disabled under the **mpls ldp** subconfiguration mode, as seen below.

```
RP/0/0/CPU0:XR1#conf t
Thu Apr 30 03:22:30.809 UTCRP/0/0/CPU0:XR1(config)#mpls ldp
RP/0/0/CPU0:XR1(config-ldp)#interface g0/0/0/0.1920
RP/0/0/CPU0:XR1(config-ldp-if)#igp auto-config disable

RP/0/0/CPU0:XR1(config-ldp-if)#show config
Thu Apr 30 03:22:57.167 UTC
Building configuration...
!! IOS XR Configuration 5.2.0
mpls ldp
 interface GigabitEthernet0/0/0/0.1920
  address-family ipv4 igp auto-config disable
  !
 !
!
end

RP/0/0/CPU0:XR1(config-ldp-if)#commit
Thu Apr 30 03:23:16.776 UTC
RP/0/0/CPU0:XR1(config-ldp-if)#end
RP/0/0/CPU0:XR1#show mpls interfaces

Thu Apr 30 03:23:22.645 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------GigabitEthernet0/0/0/0.519 Yes
      No       No       YesGigabitEthernet0/0/0/0.619 Yes
      No       No       Yes

R6#show mpls interfaces detail

Interface GigabitEthernet1.36:
        Type Unknown
        IP labeling enabled (ldp) :
```

```
IGP config

        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
Interface GigabitEthernet1.46:
        Type Unknown
        IP labeling enabled (ldp) : IGP config
        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
Interface GigabitEthernet1.56:
        Type Unknown
        IP labeling enabled (ldp) : IGP config
        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
Interface GigabitEthernet1.619:
        Type Unknown
        IP labeling enabled (ldp) : IGP config

        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP IS-IS Autoconfig

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **IS-IS**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Using MPLS LDP Autoconfig in IS-IS, configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Statically set their MPLS LDP Router-IDs to be their Loopback0 interfaces.

Configuration

```
R2:
router isis
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R3:
router isis
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R4:
router isis
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

R5:
router isis
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
```

```
R6:
router isis
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0

XR1:
router isis 1
 address-family ipv4 unicast
  mpls ldp auto-config
 !
!
mpls ldp
 router-id Loopback0
!
```

Verification

This example is similar to the previous one of running OSPF and MPLS LDP Autoconfig, in which all interfaces running OSPF had LDP automatically enabled. In this case all interfaces running IS-IS have LDP automatically enabled. The end result is the same as if you had manually configured LDP on all interfaces, however it simplifies the steps needed to enable MPLS, and ensures that some interfaces running IGP are not left without LDP running, which can cause blackholes in the data plane.

Again since the links on R2 and XR1 facing R1 and XR2 respectively are running IS-IS, they also have LDP enabled, as seen below.

```
R2#show mpls interfaces

Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet1.23    Yes (ldp)     No       No  No     Yes
        GigabitEthernet1.24    Yes (ldp)     No       No  No     Yes
        GigabitEthernet1.12    Yes (ldp)     No       No  No     Yes

RP/0/0/CPU0:XR1#show mpls interfaces

Fri May  1 00:24:11.983 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------GigabitEthernet0/0/0/0.519
 Yes      No       No       YesGigabitEthernet0/0/0/0.619
 Yes      No       No       YesGigabitEthernet0/0/0/0.1920
 Yes     No       No       Yes
```

Autoconfig could then be selectively *disabled* if desired as follows.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int Gig1.12R2(config-if)#no mpls ldp igp autoconfig

R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by consoleR2#show mpls interfaces
Interface              IP
       Tunnel        BGP Static  Operational GigabitEthernet1.23   Yes (ldp)
 No          No  No      Yes GigabitEthernet1.24   Yes (ldp)
 No          No  No      Yes

RP/0/0/CPU0:XR1#conf t
Fri May  1 00:26:11.395 UTC
RP/0/0/CPU0:XR1(config)#mpls ldp RP/0/0/CPU0:XR1(config-ldp)#interface GigabitEthernet 0/0/0/0.1920
RP/0/0/CPU0:XR1(config-ldp-if)#igp auto-config disable

RP/0/0/CPU0:XR1(config-ldp-if)#commit
Fri May  1 00:26:48.412 UTC
RP/0/0/CPU0:XR1(config-ldp-if)#end
RP/0/0/CPU0:XR1#show mpls interfaces

Fri May  1 00:27:04.751 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------GigabitEthernet0/0/0/0.519
 Yes      No       No       YesGigabitEthernet0/0/0/0.619
 Yes      No       No       Yes
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP Authentication

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Statically set their MPLS LDP Router-IDs to be their Loopback0 interfaces.
- Configure authentication for the LDP peerings as follows:
  - R2 and R3 should authenticate their LDP session with the password "R2R3PASS".
  - R2 and R4 should authenticate their LDP session with the password "R2R4PASS".
  - R3, R4, R5, and R6 should all require that every LDP session use authentication.
  - R5 should use the default password "R5PASS" for all sessions.
  - R4, R6, and XR1 should all use the password "R5PASS" for their peering to R5.
  - R3, R4, and R6 should use password option 1 with the password "R3R4R6PASS" to authenticate their peerings as a group.
  - R6 and XR1 should fallback to the default password "DEFAULTPASS" for any other unmatched sessions.

Configuration

```
R2:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
!
mpls ldp neighbor 3.3.3.3 password R2R3PASS
```

```
mpls ldp neighbor 4.4.4.4 password R2R4PASS

R3:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
!
mpls ldp password required
mpls ldp password option 1 for R3_R4_R6 R3R4R6PASS
mpls ldp neighbor 2.2.2.2 password R2R3PASS
!
ip access-list standard R3_R4_R6
 permit 3.3.3.3
 permit 4.4.4.4
 permit 6.6.6.6

R4:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
!
mpls ldp password required
mpls ldp password option 1 for R3_R4_R6 R3R4R6PASS
mpls ldp neighbor 2.2.2.2 password R2R4PASS
mpls ldp neighbor 5.5.5.5 password R5PASS
!
ip access-list standard R3_R4_R6
 permit 3.3.3.3
 permit 4.4.4.4
 permit 6.6.6.6

R5:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0
!
mpls ldp password required
mpls ldp password fallback R5PASS

R6:
router ospf 1
 mpls ldp autoconfig
!
```

```
mpls ldp router-id Loopback0
!
mpls ldp password required
mpls ldp password option 1 for R3_R4_R6 R3R4R6PASS
mpls ldp password fallback DEFAULTPASS
mpls ldp neighbor 5.5.5.5 password R5PASS
!
ip access-list standard R3_R4_R6
 permit 3.3.3.3
 permit 4.4.4.4
 permit 6.6.6.6

XR1:
router ospf 1
 mpls ldp auto-config
!
mpls ldp
 router-id 19.19.19.19
 neighbor password clear DEFAULTPASS
 neighbor 5.5.5.5 password clear R5PASS
```

Verification

LDP Authentication, similar to BGP Authentication, uses the MD5 hash field of the TCP header for peer authentication. The neighbor address that should be matched for authentication is the LDP Router-ID, not the interface IP address nor the LDP transport address.

As seen in this example, authentication can be configured on a per-neighbor basis, for a group of neighbors with the **password option** syntax, or as a default password with the **fallback** option. The **mpls ldp password required** command in regular IOS stops the formation of new LDP peerings that do not have the correct password configured. For example in R2's case we have not configured the **password required** option, so if a new peer were discovered R2 would form the peering even though there is no password configured.

Final verification of this configuration is based on whether the LDP peerings properly establish, and from the detailed output below we can see whether the password is configured per neighbor, per option, or for fallback, and whether or not authentication is required.

R2#show mpls ldp neighbor detail | include Peer LDP Ident|MD5|Password
Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 2.2.2.2:0 TCP connection: 3.3.3.3.28273 - 2.2.2.2.646; MD5 on **Password: not required, neighbor, in use**

Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 2.2.2.2:0 TCP connection: 4.4.4.4.16814 - 2.2.2.2.646; **MD5 on Password: not required, neighbor, in use**

R3#show mpls ldp neighbor detail | include Peer LDP Ident|MD5|Password
Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 3.3.3.3:0 TCP connection: 2.2.2.2.646 - 3.3.3.3.42712; **MD5 on Password: required, neighbor, in use** Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 3.3.3.3:0 TCP connection: 4.4.4.4.51384 - 3.3.3.3.646; **MD5 on Password: required, option 1, in use** Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 3.3.3.3:0 TCP connection: 6.6.6.6.40642 - 3.3.3.3.646; **MD5 on Password: required, option 1, in use**

```
R4#show mpls ldp neighbor detail | include Peer LDP Ident|MD5|Password
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 2.2.2.2.646 - 4.4.4.4.28273; MD5 on
 Password: required, neighbor, in use
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 3.3.3.3.646 - 4.4.4.4.51384; MD5 on
 Password: required, option 1, in use
    Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 6.6.6.6.39672 - 4.4.4.4.646; MD5 on
 Password: required, option 1, in use
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 5.5.5.5.40136 - 4.4.4.4.646; MD5 on
 Password: required, neighbor, in use

R5#show mpls ldp neighbor detail | include Peer LDP Ident|MD5|Password
    Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 5.5.5.5:0
        TCP connection: 6.6.6.6.54049 - 5.5.5.5.646; MD5 on
 Password: required, fallback, in use
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 5.5.5.5:0
        TCP connection: 4.4.4.4.646 - 5.5.5.5.29501; MD5 on
 Password: required, fallback, in use
    Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 5.5.5.5:0
        TCP connection: 19.19.19.19.24927 - 5.5.5.5.646; MD5 on
 Password: required, fallback, in use
R6#show mpls ldp neighbor detail | include Peer LDP Ident|MD5|Password
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 3.3.3.3.646 - 6.6.6.6.12509; MD5 on
 Password: required, option 1, in use
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 5.5.5.5.646 - 6.6.6.6.54049; MD5 on
 Password: required, neighbor, in use
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 4.4.4.4.646 - 6.6.6.6.38312; MD5 on
 Password: required, option 1, in use
```

```
    Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 19.19.19.19.29593 - 6.6.6.6.646; MD5 on
 Password: required, fallback, in use
RP/0/0/CPU0:XR1#show mpls ldp neighbor detail
Fri May  1 00:48:10.624 UTC

Peer LDP Identifier: 5.5.5.5:0 TCP connection: 5.5.5.5:646 - 19.19.19.19:20747; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 25/25; Downstream-Unsolicited
  Up time: 00:02:59
  LDP Discovery Sources:
      GigabitEthernet0/0/0/0.519
  Addresses bound to this peer:
      5.5.5.5        20.4.5.5       20.5.6.5       20.5.19.5
  Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
  NSR: Disabled
  Capabilities:
    Sent:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
    Received:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)

Peer LDP Identifier: 6.6.6.6:0 TCP connection: 6.6.6.6:646 - 19.19.19.19:18275; MD5 on

  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 25/25; Downstream-Unsolicited
  Up time: 00:02:55
  LDP Discovery Sources:
      GigabitEthernet0/0/0/0.619
  Addresses bound to this peer:
      6.6.6.6        20.3.6.6       20.4.6.6       20.5.6.6
      20.6.19.6
  Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
  NSR: Disabled
  Capabilities:
    Sent:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
    Received:
```

```
0x508  (MP: Point-to-Multipoint (P2MP))
0x509  (MP: Multipoint-to-Multipoint (MP2MP))
0x50b  (Typed Wildcard FEC)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP Label Allocation Filtering

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Configure LDP filtering so that labels are only allocated for the Loopback0 networks of R2 and XR1.

Configuration

```
R2:
ip prefix-list LABELS seq 5 permit 2.2.2.2/32
ip prefix-list LABELS seq 10 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list LABELS
!
router ospf 1
 mpls ldp autoconfig area 0

R3:
ip prefix-list LABELS seq 5 permit 2.2.2.2/32
ip prefix-list LABELS seq 10 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list LABELS
!
router ospf 1
 mpls ldp autoconfig area 0

R4:
ip prefix-list LABELS seq 5 permit 2.2.2.2/32
```

```
ip prefix-list LABELS seq 10 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list LABELS
!
router ospf 1
 mpls ldp autoconfig area 0

R5:
ip prefix-list LABELS seq 5 permit 2.2.2.2/32
ip prefix-list LABELS seq 10 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list LABELS
!
router ospf 1
 mpls ldp autoconfig area 0

R6:
ip prefix-list LABELS seq 5 permit 2.2.2.2/32
ip prefix-list LABELS seq 10 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list LABELS
!
router ospf 1
 mpls ldp autoconfig area 0

XR1:
ipv4 access-list 1
 10 permit ipv4 host 19.19.19.19 any
 20 permit ipv4 host 2.2.2.2 any
!
router ospf 1
 mpls ldp auto-config
!
mpls ldp
 label
  allocate for 1
```

Verification

By default, LDP allocates labels for all IGP learned prefixes and connected interfaces that run LDP. For scalability reasons it may be desirable to limit which prefixes have labels generated, as opposed to generating labels for everything. Typically labels can be limited to just those of the Loopbacks of the PE routers that service either L2VPN or L3VPN customers.

From the below output we can see that label values are only bound for the Loopback networks of R2 and XR1.

```
R2#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
22         23         19.19.19.19/32   0             Gi1.23     20.2.3.3
           23         19.19.19.19/32   0             Gi1.24     20.2.4.4
R2#show mpls ldp binding
  lib entry: 1.1.1.1/32, rev 39
        no local binding
  lib entry: 2.2.2.2/32, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 3.3.3.3:0, label: 17
        remote binding: lsr: 4.4.4.4:0, label: 17
  lib entry: 3.3.3.3/32, rev 40
        no local binding
  lib entry: 4.4.4.4/32, rev 41
        no local binding
  lib entry: 5.5.5.5/32, rev 42
        no local binding
  lib entry: 6.6.6.6/32, rev 43
        no local binding
  lib entry: 10.1.2.0/24, rev 44
        no local binding
  lib entry: 10.19.20.0/24, rev 45
        no local binding
  lib entry: 19.19.19.19/32, rev 18
        local binding:  label: 22
        remote binding: lsr: 3.3.3.3:0, label: 23
        remote binding: lsr: 4.4.4.4:0, label: 23
  lib entry: 20.2.3.0/24, rev 46
        no local binding
  lib entry: 20.2.4.0/24, rev 47
        no local binding
  lib entry: 20.3.4.0/24, rev 48
        no local binding
  lib entry: 20.3.6.0/24, rev 49
        no local binding
  lib entry: 20.4.5.0/24, rev 50
        no local binding
  lib entry: 20.4.6.0/24, rev 51
```

```
        no local binding
  lib entry: 20.5.6.0/24, rev 52
        no local binding
  lib entry: 20.5.19.0/24, rev 53
        no local binding
  lib entry: 20.6.19.0/24, rev 54
        no local binding
  lib entry: 20.20.20.20/32, rev 55
        no local binding
```

R5#show mpls forwarding-table

```
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
17         17         2.2.2.2/32       0             Gi1.45     20.4.5.4
23         Pop Label  19.19.19.19/32   0             Gi1.519    20.5.19.19
```

```
R5#show mpls ldp bindingsb#
  lib entry: 2.2.2.2/32, rev 4
        local binding:  label: 17
        remote binding: lsr: 4.4.4.4:0, label: 17
        remote binding: lsr: 6.6.6.6:0, label: 17
        remote binding: lsr: 19.19.19.19:0, label: 16005
  lib entry: 19.19.19.19/32, rev 18
        local binding:  label: 23
        remote binding: lsr: 4.4.4.4:0, label: 23
        remote binding: lsr: 6.6.6.6:0, label: 23
        remote binding: lsr: 19.19.19.19:0, label: imp-null
RP/0/0/CPU0:XR1#show mpls forwarding
Fri May  1 23:05:20.238 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16005  16          2.2.2.2/32         Gi0/0/0/0.519 20.5.19.5       0
       16          2.2.2.2/32         Gi0/0/0/0.619 20.6.19.6       0
RP/0/0/CPU0:XR1#show mpls ldp bindings
Fri May  1 23:06:51.932 UTC
2.2.2.2/32, rev 33
        Local binding: label: 16005
        Remote bindings: (2 peers)
            Peer                Label
            -----------------   ---------
            5.5.5.5:0           16
            6.6.6.6:0           16
19.19.19.19/32, rev 2
        Local binding: label: ImpNull
        Remote bindings: (2 peers)
            Peer                Label
            -----------------   ---------
            5.5.5.5:0           17
        6.6.6.6:0           17
```

Filtering the labels that are allocated to the Loopbacks of PE devices is common is SP environments. IOS and IOS-XR provide a shortcut for doing this task:

```
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.R5(config)#mpls ldp label
R5(config-ldp-lbl)#allocate global host-routes
R5(config-ldp-lbl)#end
R5#
%SYS-5-CONFIG_I: Configured from console by consoleR5#show mpls ldp bindings
  lib entry: 1.1.1.1/32, rev 6 local binding:  label: 18
  lib entry: 2.2.2.2/32, rev 2 local binding:  label: 16
        remote binding: lsr: 6.6.6.6:0, label: 16
        remote binding: lsr: 4.4.4.4:0, label: 16
        remote binding: lsr: 19.19.19.19:0, label: 16005
  lib entry: 3.3.3.3/32, rev 8 local binding:  label: 19
  lib entry: 4.4.4.4/32, rev 10 local binding:  label: 20
  lib entry: 5.5.5.5/32, rev 12 local binding:  label: imp-null
  lib entry: 6.6.6.6/32, rev 14 local binding:  label: 21
  lib entry: 19.19.19.19/32, rev 4 local binding:  label: 17
        remote binding: lsr: 6.6.6.6:0, label: 17
        remote binding: lsr: 4.4.4.4:0, label: 17
        remote binding: lsr: 19.19.19.19:0, label: imp-null
  lib entry: 20.20.20.20/32, rev 16 local binding:  label: 22
```

The 'allocate global host-routes' command ensures that labels are only allocated for /32 host routes learned via IGP or directly connected. Note that applying this command removes the previous filter.

```
RP/0/0/CPU0:XR1(config)#mpls ldp
RP/0/0/CPU0:XR1(config-ldp)#address-family ipv4
RP/0/0/CPU0:XR1(config-ldp-af)#label local
 RP/0/0/CPU0:XR1(config-ldp-af-lbl-lcl)#allocate for host-routes
 RP/0/0/CPU0:XR1(config-ldp-af-lbl-lcl)#show config
Fri May  1 23:02:42.059 UTC
Building configuration...
!! IOS XR Configuration 5.2.0
mpls ldp
 address-family ipv4
  label
   local    allocate for host-routes
   !
  !
 !
!
end
RP/0/0/CPU0:XR1(config-ldp-af-lbl-lcl)#commit
```

Note that this filtering is different from the IOS command **mpls ldp advertise-labels** or the IOS XR command **label advertise** under the **mpls ldp** sub-configuration mode. These commands are used to filter LDP advertisements as they are sent out or received inbound globally or to/from an individual peer. Allocation filtering, as seen in this example, globally controls which prefixes are sent from the IGP routing table to the LDP process for label generation to begin with.

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP IGP Synchronization

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Basic L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2; at this point R1 and XR2 should have reachability to each other's Loopback0 networks.
- In the core of the SP network change the OSPF cost of every transit link to 100 with the exception of the links between R2 & R3, R3 & R6, and R6 & XR1.
- Configure LDP and IGP Synchronization with OSPF on all routers in the core of the SP network.
- To test this, filter out all LDP traffic that R6 is receiving and ensure that labeled traffic through the core reroutes around the unsynchronized links of R6.

Configuration

```
R2:
interface GigabitEthernet1.24
 ip ospf cost 100
!
router ospf 1
 mpls ldp autoconfig area 0
 mpls ldp sync

R3:
interface GigabitEthernet1.34
 ip ospf cost 100
!
router ospf 1
```

```
 mpls ldp autoconfig area 0
 mpls ldp sync

R4:
interface GigabitEthernet1.24
 ip ospf cost 100
!
interface GigabitEthernet1.34
 ip ospf cost 100
!
interface GigabitEthernet1.45
 ip ospf cost 100
!
interface GigabitEthernet1.46
 ip ospf cost 100
!
router ospf 1
 mpls ldp autoconfig area 0
 mpls ldp sync

R5:
interface GigabitEthernet1.45
 ip ospf cost 100
!
interface GigabitEthernet1.56
 ip ospf cost 100
!
interface GigabitEthernet1.519
 ip ospf cost 100
!
router ospf 1
 mpls ldp autoconfig area 0
 mpls ldp sync

R6:
interface GigabitEthernet1.46
 ip ospf cost 100
!
interface GigabitEthernet1.56
 ip ospf cost 100
!
router ospf 1
 mpls ldp autoconfig area 0
 mpls ldp sync

XR1:
```

```
mpls ldp
 router-id 19.19.19.19
!
router ospf 1
 mpls ldp sync
 mpls ldp auto-config
 area 0
  interface GigabitEthernet0/0/0/0.519
  cost 100
```

Verification

MPLS LDP IGP Synchronization is used to prevent traffic blackholes in the core of the MPLS network when an error in LDP configuration or operation causes IGP to attempt to route labeled traffic over a non-labeled path. LDP Sync prevents these blackholes by configuring the IGP process (either OSPF or IS-IS) to advertise the highest possible cost values for links that do not have their LDP adjacencies established and properly converged.

The idea is that if LDP fails on an interface, the router will begin advertising a very high IGP cost for that link, which ideally should cause the IGP network to reroute and avoid the link on which LDP is broken. This feature is also helps prevents blackholes when a router reloads. If IGP comes up before LDP has fully exchanged labels, then traffic could end up being blackholed.

To see this feature in action in this particular scenario, we first need to see which way the end customer traffic is routing through the core of the Service Provider network. This can be seen through the following traceroute output.

```
R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec   2 20.2.3.3 [MPLS: Labels 20/16007 Exp 0]
 12 msec 8 msec 9 msec   3 20.3.6.6 [MPLS: Labels 20/16007 Exp 0]
 18 msec 31 msec 31 msec
  4 20.6.19.19 22 msec 14 msec 15 msec
  5 10.19.20.20 15 msec *  10 msec

RP/0/3/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
Fri May  1 23:52:14.596 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1
```

```
 1  10.19.20.19 9 msec  0 msec  0 msec   2 20.6.19.6 [MPLS: Labels 16/31 Exp 0]
29 msec  9 msec  0 msec   3 20.3.6.3 [MPLS: Labels 16/31 Exp 0]
0 msec  9 msec  9 msec
 4  10.1.2.2 [MPLS: Label 31 Exp 0] 0 msec  0 msec  0 msec
 5  10.1.2.1 9 msec  *  9 msec
```

For both traffic from R1 to XR2 and back, the links between R3 and R6 are preferred in the transit path of the core of the network. This is due to the fact that all other links in the core of the OSPF network have their cost raised to 100, as seen below.

```
R2#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               2.2.2.2/32         1     LOOP  0/0
Gi1.24       1     0               20.2.4.2/24 100
   BDR   1/1
Gi1.23       1     0               20.2.3.2/24        1     BDR   1/1
R3#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               3.3.3.3/32         1     LOOP  0/0
Gi1.36       1     0               20.3.6.3/24        1     BDR   1/1
Gi1.34       1     0               20.3.4.3/24 100
   BDR   1/1
Gi1.23       1     0               20.2.3.3/24        1     DR    1/1
R4#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               4.4.4.4/32         1     LOOP  0/0
Gi1.46       1     0               20.4.6.4/24 100
   BDR   1/1 Gi1.45       1     0            20.4.5.4/24 100
   BDR   1/1 Gi1.34       1     0            20.3.4.4/24 100
   DR    1/1 Gi1.24       1     0            20.2.4.4/24 100
   DR    1/1
R5#show ip ospf interface brief

Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               5.5.5.5/32         1     LOOP  0/0
Gi1.519      1     0               20.5.19.5/24 100
   BDR   1/1 Gi1.56       1     0            20.5.6.5/24 100
   BDR   1/1 Gi1.45       1     0            20.4.5.5/24 100
   DR    1/1
R6#show ip ospf interface brief

Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               6.6.6.6/32         1     LOOP  0/0
Gi1.619      1     0               20.6.19.6/24       1     BDR   1/1
```

```
Gi1.56        1      0                20.5.6.6/24 100
   DR     1/1 Gi1.46        1      0                20.4.6.6/24 100
   DR     1/1
Gi1.36        1      0                20.3.6.6/24        1      DR     1/1
RP/0/0/CPU0:XR1#show ip ospf interface brief
Fri May  1 23:56:25.278 UTC

* Indicates MADJ interface, (P) Indicates fast detect hold down state

Interfaces for OSPF 1

Interface          PID    Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0                1      0               19.19.19.19/32     1      LOOP  0/0
Gi0/0/0/0.519      1      0               20.5.19.19/24 100
   DR     1/1
Gi0/0/0/0.619      1      0               20.6.19.19/24      1      DR     1/1
```

Additionally at this point LDP IGP Sync is enabled, and all interfaces running OSPF also have LDP enabled, since LDP autoconfig was enabled. This means that the IGP and LDP domains should be synchronized, as seen below.

```
R2#show mpls ldp igp sync
    GigabitEthernet1.23: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 3.3.3.3:0
        IGP enabled: OSPF 1
    GigabitEthernet1.24: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 4.4.4.4:0
        IGP enabled: OSPF 1
R3#show mpls ldp igp sync
    GigabitEthernet1.23: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 2.2.2.2:0
        IGP enabled: OSPF 1
    GigabitEthernet1.34: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
```

```
        Peer LDP Ident: 4.4.4.4:0
        IGP enabled: OSPF 1
    GigabitEthernet1.36: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 6.6.6.6:0
        IGP enabled: OSPF 1
R4#show mpls ldp igp sync
    GigabitEthernet1.24: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 2.2.2.2:0
        IGP enabled: OSPF 1
    GigabitEthernet1.34: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 3.3.3.3:0
        IGP enabled: OSPF 1
    GigabitEthernet1.45: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 5.5.5.5:0
        IGP enabled: OSPF 1
    GigabitEthernet1.46: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 6.6.6.6:0
        IGP enabled: OSPF 1
R5#show mpls ldp igp sync
    GigabitEthernet1.45: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 4.4.4.4:0
        IGP enabled: OSPF 1
    GigabitEthernet1.56: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 6.6.6.6:0
        IGP enabled: OSPF 1
```

```
    GigabitEthernet1.519: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 19.19.19.19:0
        IGP enabled: OSPF 1
```

R6#show mpls ldp igp sync

```
    GigabitEthernet1.36: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 3.3.3.3:0
        IGP enabled: OSPF 1
    GigabitEthernet1.46: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 4.4.4.4:0
        IGP enabled: OSPF 1
    GigabitEthernet1.56: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 5.5.5.5:0
        IGP enabled: OSPF 1
    GigabitEthernet1.619: LDP configured; LDP-IGP Synchronization enabled.
        Sync status: sync achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 19.19.19.19:0
        IGP enabled: OSPF 1
```

RP/0/0/CPU0:XR1#show mpls ldp igp sync

```
Fri May  1 23:58:02.882 UTC

GigabitEthernet0/0/0/0.519:
  VRF: 'default' (0x60000000)
  Sync delay: Disabled Sync status: Ready
    Peers:
      5.5.5.5:0

GigabitEthernet0/0/0/0.619:
  VRF: 'default' (0x60000000)
  Sync delay: Disabled Sync status: Ready

    Peers:
```

```
6.6.6.6:0
```

Since synchronization has been achieved it means that OSPF will be advertising the normal cost value for its connected links. Below we see that R6 is advertising a cost of 1 for the links to R3 and XR1, while advertising a cost of 100 on the links to R4 and R5.

```
RP/0/0/CPU0:XR1#show ospf database router 6.6.6.6
Sat May  2 00:00:36.841 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 1)

                    Router Link States (Area 0)

Routing Bit Set on this LSA
LS age: 551
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 6.6.6.6
Advertising Router: 6.6.6.6
LS Seq Number: 80000007
Checksum: 0x96f9
Length: 84
 Number of Links: 5

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 6.6.6.6
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.6.19.6     (Link Data) Router Interface address: 20.6.19.6
       Number of TOS metrics: 0        TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.5.6.6     (Link Data) Router Interface address: 20.5.6.6
       Number of TOS metrics: 0        TOS 0 Metrics: 100

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.4.6.6     (Link Data) Router Interface address: 20.4.6.6
       Number of TOS metrics: 0         TOS 0 Metrics: 100

    Link connected to: a Transit Network
```

```
    (Link ID) Designated Router address: 20.3.6.6      (Link Data) Router Interface address: 20.3.6.6

      Number of TOS metrics: 0         TOS 0 Metrics: 1
```

LDP IGP Sync is now protecting the network against a failure of LDP that would normally blackhole traffic. For example suppose that R6 has an access-list configured to filter traffic in the data plane that arrives inbound on its local interfaces. Additionally, someone misconfigures this filter so that LDP traffic (TCP port 646) is dropped. Since the LDP holdtime is very long (180 seconds by default), they wouldn't notice that the problems occurs immediately. Instead about 3 minutes after the filter is configured the LDP adjacencies of R6 would drop, causing traffic to blackhole. However with LDP IGP Sync on, the IGP process of R6 would detect that LDP Synchronization has been lost, and would start advertising a very high cost for its local links in the attempt to reroute traffic around its links and/or node.

Below we see an ACL configured on R6 to filter out the LDP adjacencies. This filter is applied in on all interfaces at around time index 00:04:40.236.

```
R6#config t
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#access-list   100 deny tcp any any eq 646
R6(config)#access-list   100 deny tcp any eq 646 any
R6(config)#access-list  100 permit ip any anyR6(config)#int Gig1.36
    R6(config-subif)#ip access-group 100 in
R6(config-subif)#int Gig1.46
R6(config-subif)#ip access-group 100 in
R6(config-subif)#int Gig1.56
R6(config-subif)#ip access-group 100 in
R6(config-subif)#int Gig1.619
R6(config-subif)#ip access-group 100 in
R6(config)#end
R6#     *May  2 00:04:40.236
: %SYS-5-CONFIG_I: Configured from console by console
R6#show mpls ldp neighbor 3.3.3.3 detail
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 3.3.3.3.646 - 6.6.6.6.46449
        Password: not required, none, in use
        State: Oper; Msgs sent/rcvd: 52/52; Downstream; Last TIB rev sent 30
        Up time: 00:29:50; UID: 27; Peer Id 0
        LDP discovery sources:
          GigabitEthernet1.36; Src IP addr: 20.3.6.3
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          3.3.3.3         20.2.3.3        20.3.4.3        20.3.6.3
```

```
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

        NSR: Not Ready
        Capabilities Sent:
          [ICCP (type 0x0405) MajVer 1 MinVer 0]
          [Dynamic Announcement (0x0506)]
          [mLDP Point-to-Multipoint (0x0508)]
          [mLDP Multipoint-to-Multipoint (0x0509)]
          [Typed Wildcard (0x050B)]
        Capabilities Received:
          [ICCP (type 0x0405) MajVer 1 MinVer 0]
          [Dynamic Announcement (0x0506)]
      [mLDP Point-to-Multipoint (0x0508)]
      [mLDP Multipoint-to-Multipoint (0x0509)]
      [Typed Wildcard (0x050B)]
```

At this point the LDP adjacencies of R6 are still up, so traffic is routed through the normal lowest cost path in the core.

```
R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec   2 20.2.3.3 [MPLS: Labels 20/16007 Exp 0]
 9 msec 6 msec 6 msec   3 20.3.6.6 [MPLS: Labels 20/16007 Exp 0]
 27 msec 31 msec 37 msec
  4 20.6.19.19 22 msec 15 msec 15 msec
  5 10.19.20.20 16 msec *  12 msec

R2#show ip route 19.19.19.19
Routing entry for 19.19.19.19/32
  Known via "ospf 1", distance 110, metric 4, type intra area
  Last update from 20.2.3.3 on GigabitEthernet1.23, 00:14:55 ago
  Routing Descriptor Blocks:   * 20.2.3.3, from 19.19.19.19, 00:14:55 ago, via GigabitEthernet1.23

      Route metric is 4, traffic share count is 1
```

About 3 minutes later R6 starts to lose its LDP adjacencies.

```
R6#
*May  2 00:06:19.645: %LDP-5-NBRCHG: LDP Neighbor 19.19.19.19:0 (4) is DOWN (Session KeepAlive Timer expired)
R6#
*May  2 00:06:37.089: %LDP-5-NBRCHG: LDP Neighbor 5.5.5.5:0 (2) is DOWN (Session KeepAlive Timer expired)
R6#
*May  2 00:07:25.856: %LDP-5-NBRCHG: LDP Neighbor 4.4.4.4:0 (3) is DOWN (Session KeepAlive Timer expired)
```

```
R6#
*May  2 00:07:32.016: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (1) is DOWN (Session KeepAlive Timer expired)
```

This causes IGP Sync to be lost.

```
R6#show mpls ldp igp sync
    GigabitEthernet1.36:
        LDP configured; LDP-IGP Synchronization enabled. Sync status: sync not achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        IGP enabled: OSPF 1
    GigabitEthernet1.46:
        LDP configured; LDP-IGP Synchronization enabled. Sync status: sync not achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        IGP enabled: OSPF 1
    GigabitEthernet1.56:
        LDP configured; LDP-IGP Synchronization enabled. Sync status: sync not achieved; peer reachable.
        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        IGP enabled: OSPF 1
    GigabitEthernet1.619:
        LDP configured; LDP-IGP Synchronization enabled. Sync status: sync not achieved; peer reachable.

        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        IGP enabled: OSPF 1
```

R6 now advertises a high cost for its connected links.

```
RP/0/0/CPU0:XR1#show ospf database router 6.6.6.6
Mon Mar 26 15:05:54.541 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 1)

                Router Link States (Area 0)

Routing Bit Set on this LSA LS age: 366
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 6.6.6.6
Advertising Router: 6.6.6.6
LS Seq Number: 8000000b
Checksum: 0x88ce
```

```
Length: 84
 Number of Links: 5

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 6.6.6.6
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.6.19.6     (Link Data) Router Interface address: 20.6.19.6
      Number of TOS metrics: 0       TOS 0 Metrics: 65535

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.5.6.6     (Link Data) Router Interface address: 20.5.6.6
      Number of TOS metrics: 0        TOS 0 Metrics: 65535

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.4.6.6     (Link Data) Router Interface address: 20.4.6.6

      Number of TOS metrics: 0       TOS 0 Metrics: 65535

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 20.3.6.6      (Link Data) Router Interface address: 20.3.6.6
      Number of TOS metrics: 0        TOS 0 Metrics: 65535
```

The final result is that the end customer’s traffic is transparently rerouted around the LDP failure.

```
R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 1 msec 2 msec 0 msec   2 20.2.4.4 [MPLS: Labels 20/16007 Exp 0]
 10 msec 8 msec 8 msec   3 20.4.5.5 [MPLS: Labels 20/16007 Exp 0]
 20 msec 31 msec 31 msec
  4 20.5.19.19 21 msec 16 msec 13 msec
  5 10.19.20.20 15 msec *  10 msec

R2#show ip route 19.19.19.19

Routing entry for 19.19.19.19/32
  Known via "ospf 1", distance 110, metric 301, type intra area
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:02:37 ago
```

```
    Routing Descriptor Blocks:   * 20.2.4.4, from 19.19.19.19, 00:02:37 ago, via GigabitEthernet1.24

        Route metric is 301, traffic share count is 1
```

Now let’s examine the problem *without* LDP IGP Sync. All routers remove the LDP IGP Sync feature, and R6 removes its filter that is breaking LDP.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.R2(config)#router ospf 1
R2(config-router)#no mpls ldp sync

R2(config-router)#end
R2#

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.R3(config)#router ospf 1
R3(config-router)#no mpls ldp sync

R3(config-router)#end
R3#

R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.R4(config)#router ospf 1
R4(config-router)#no mpls ldp sync

R4(config-router)#end
R4#

R5#conf t
Enter configuration commands, one per line. End with CNTL/Z.R5(config)#router ospf 1
R5(config-router)#no mpls ldp sync

R5(config-router)#end
R5#

R6#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.R6(config)#no access-list 100
R6(config)#router ospf 1 R6(config-router)#no mpls ldp sync

R6(config-router)#end
00:41:22: %SYS-5-CONFIG_I: Configured from console by console
00:41:23: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (1) is UP
00:41:23: %LDP-5-NBRCHG: LDP Neighbor 5.5.5.5:0 (2) is UP
00:41:24: %LDP-5-NBRCHG: LDP Neighbor 19.19.19.19:0 (3) is UP
00:41:27: %LDP-5-NBRCHG: LDP Neighbor 4.4.4.4:0 (4) is UP
RP/0/0/CPU0:XR1#config t
Mon Mar 26 15:10:30.219 UTCRP/0/0/CPU0:XR1(config)#router ospf 1
RP/0/0/CPU0:XR1(config-ospf)#no mpls ldp sync
RP/0/0/CPU0:XR1(config-ospf)#commit
Sat May  2 00:11:45.865 UTC
```

At this point all LDP adjacencies are working and traffic is routing as normal via the R2 > R3 > R6 > XR1 path and back.

```
R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec  2 20.2.3.3 [MPLS: Labels 20/16007 Exp 0]
 6 msec 4 msec 7 msec  3 20.3.6.6 [MPLS: Labels 20/16007 Exp 0]
 30 msec 31 msec 31 msec
  4 20.6.19.19 20 msec 16 msec 15 msec
  5 10.19.20.20 14 msec *  8 msec
```

Now R6 configures its ACL filter again which breaks LDP. The ACL is still applied from before.

```
R6#config t
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#access-list 100 deny  tcp any any eq 646
 R6(config)#access-list 100 deny  tcp any eq 646 any
*May  2 00:14:07.832: %LDP-5-NBRCHG: LDP Neighbor 19.19.19.19:0 (4) is DOWN (Discovery Hello Hold Timer expired)
*May  2 00:14:08.137: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (1) is DOWN (Discovery Hello Hold Timer expired)
R6(config)#access-list 100 permit ip any any
R6(config)#
*May  2 00:14:10.304: %LDP-5-NBRCHG: LDP Neighbor 5.5.5.5:0 (3) is DOWN (Discovery Hello Hold Timer expired)
*May  2 00:14:10.975: %LDP-5-NBRCHG: LDP Neighbor 4.4.4.4:0 (2) is DOWN (Discovery Hello Hold Timer expired)
```

Without LDP IGP Sync enabled, OSPF does not react to this change in the LDP topology.

```
R2#show ip route 19.19.19.19
Routing entry for 19.19.19.19/32
  Known via "ospf 1", distance 110, metric 4, type intra area
  Last update from 20.2.3.3 on GigabitEthernet1.23, 00:02:58 ago
  Routing Descriptor Blocks:  * 20.2.3.3, from 19.19.19.19, 00:02:58 ago, via GigabitEthernet1.23
      Route metric is 4, traffic share count is 1
```

This means that traffic within the core is fine, but end customer traffic transiting the core is blackholed because of the failed Label Switch Path.

```
R2#ping 19.19.19.19 source 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.19, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!! Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/3/8 ms
R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
 1 10.1.2.2 4 msec 0 msec 0 msec   2  *   *   *
 3  *   *   *
 4  *   *   *
<snip>
RP/0/0/CPU0:XR2#ping 1.1.1.1 source 20.20.20.20
Sat May  2 00:18:40.357 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
U.U.U Success rate is 0 percent
 (0/5)
```

Although pings work between the PE's loopbacks, the LSP between them is broken. This can be further verified by using the MPLS ping utility.

```
R2#ping mpls ipv4 19.19.19.19/32 verbose source 2.2.2.2

Sending 5, 72-byte MPLS Echos to Target FEC Stack TLV descriptor,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,  'L' - labeled output interface,
'B' - unlabeled output interface,

  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.B
    size 72, reply addr 20.2.3.3, return code 9B
    size 72, reply addr 20.2.3.3, return code 9B
    size 72, reply addr 20.2.3.3, return code 9B
    size 72, reply addr 20.2.3.3, return code 9B
    size 72, reply addr 20.2.3.3, return code 9
Success rate is 0 percent (0/5)
 Total Time Elapsed 30 ms
```

The LSP breaks at R3:

```
R2#traceroute mpls ipv4 19.19.19.19/32 verbose source 2.2.2.2 ttl 4

more work needed here to demux the tfs subtlv and to display the right output
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
  0 20.2.3.2 20.2.3.3 MRU 1500 [Labels: 20 Exp: 0]
B 1 20.2.3.3 20.3.6.6 MRU 1500 [No Label] 14 ms, ret code 9
B 2 20.2.3.3 20.3.6.6 MRU 1500 [No Label] 7 ms, ret code 9
B 3 20.2.3.3 20.3.6.6 MRU 1500 [No Label] 2 ms, ret code 9
B 4 20.2.3.3 20.3.6.6 MRU 1500 [No Label] 2 ms, ret code 9
R3#show mpls forwarding-table 19.19.19.19 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface              20 No Label   19.19.19.19/32
   1265 Gi1.36     20.3.6.6

        MAC/Encaps=18/18, MRU=1504, Label Stack{}
        0050569E5CEC0050569E6E6A810000240800
        No output feature configured
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP Session Protection

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- Configure LDP Session Protection so that if a connected link between any of the routers goes down a unicast targeted LDP session remains up.

Configuration

```
R2:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp session protection

R3:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp session protection

R4:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp session protection

R5:
router ospf 1
 mpls ldp autoconfig
!
```

```
mpls ldp session protection

R6:
router ospf 1
 mpls ldp autoconfig
!
mpls ldp session protection

XR1:
router ospf 1
 mpls ldp auto-config
  !
 !
!
mpls ldp
 session protection
!
```

Verification

MPLS LDP Session Protection allows routers to maintain their label bindings with each other even if the connected link between them fails. The goal of this feature is to speed up reconvergence time when then link between them is restored, as label bindings do not need to be re-exchanged once the link comes back. To accomplish this, a targeted LDP session is established between two directly connected LDP peers. If the directly connected link between the peers goes down, the targeted LDP remains up as long as there is an alternate path between the loopbacks (LDP IDs) of the peers. This is similar to what takes place with an iBGP session between Loopbacks - the iBGP session remains up between the peers even if there is a link failure, as IGP converges and finds an alternate path between the peering's sources.

The LDP adjacency between R6 and R3 has been established as a Targeted session with protection enabled.

```
R6#show mpls ldp neighbor 3.3.3.3 detail
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 3.3.3.3.646 - 6.6.6.6.13683
        Password: not required, none, in use
        State: Oper; Msgs sent/rcvd: 32/32; Downstream; Last TIB rev sent 38
        Up time: 00:09:23; UID: 36; Peer Id 1
        LDP discovery sources:
          GigabitEthernet1.36; Src IP addr: 20.3.6.3
            holdtime: 15000 ms, hello interval: 5000 ms
Targeted Hello 6.6.6.6 -> 3.3.3.3, active, passive;
```

```
    holdtime: infinite, hello interval: 10000 ms
  Addresses bound to peer LDP Ident:
    3.3.3.3         20.2.3.3        20.3.4.3        20.3.6.3
  Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
  Clients: Dir Adj Client LDP Session Protection enabled, state: Ready

    duration: 86400 seconds
  NSR: Not Ready
  Capabilities Sent:
    [ICCP (type 0x0405) MajVer 1 MinVer 0]
    [Dynamic Announcement (0x0506)]
    [mLDP Point-to-Multipoint (0x0508)]
    [mLDP Multipoint-to-Multipoint (0x0509)]
    [Typed Wildcard (0x050B)]
  Capabilities Received:
    [ICCP (type 0x0405) MajVer 1 MinVer 0]
    [Dynamic Announcement (0x0506)]
    [mLDP Point-to-Multipoint (0x0508)]
    [mLDP Multipoint-to-Multipoint (0x0509)]
    [Typed Wildcard (0x050B)]
```

Protection occurs once the connected link between the neighbors goes down.

```
R6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#service time debug date ms
R6(config)#service time log date ms  R6(config)#do debug mpls ldp session protection
LDP session protection events debugging is onR6(config)#interface Gig1.36
R6(config-subif)#shutdown
R6(config-subif)#
*May  2 04:14:23.612: LDP SP: 3.3.3.3:0: last primary adj lost; starting session protection holdup timer
*May  2 04:14:23.612: LDP SP: 3.3.3.3:0: LDP session protection holdup timer started, 86400 seconds
*May  2 04:14:23.612: LDP SP: 3.3.3.3:0: state change (Ready -> Protecting)

R6(config-subif)#end
R6#
*May  2 04:14:23.612: %LDP-5-SP: 3.3.3.3:0: session hold up initiated
*May  2 04:14:23.612: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on GigabitEthernet1.36 from FULL to DOWN, Neighbor Down
R6#
*May  2 04:14:24.696: %SYS-5-CONFIG_I: Configured from console by console
```

Notice that the LDP adjacency remains up after the link failure:

```
R6#show mpls ldp neighbor 3.3.3.3 detail
```

```
Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 6.6.6.6:0
    TCP connection: 3.3.3.3.646 - 6.6.6.6.13683
    Password: not required, none, in use
    State: Oper; Msgs sent/rcvd: 36/35; Downstream; Last TIB rev sent 38
    Up time: 00:11:47; UID: 36; Peer Id 1
    LDP discovery sources: Targeted Hello 6.6.6.6 -> 3.3.3.3, active, passive;
        holdtime: infinite, hello interval: 10000 ms
    Addresses bound to peer LDP Ident:
      3.3.3.3         20.2.3.3        20.3.4.3        20.3.6.3
    Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Clients: Dir Adj Client LDP Session Protection enabled, state: Protecting

        duration: 86400 seconds
        holdup time remaining: 86372 seconds
    NSR: Not Ready
    Capabilities Sent:
      [ICCP (type 0x0405) MajVer 1 MinVer 0]
      [Dynamic Announcement (0x0506)]
      [mLDP Point-to-Multipoint (0x0508)]
      [mLDP Multipoint-to-Multipoint (0x0509)]
      [Typed Wildcard (0x050B)]
    Capabilities Received:
      [ICCP (type 0x0405) MajVer 1 MinVer 0]
      [Dynamic Announcement (0x0506)]
      [mLDP Point-to-Multipoint (0x0508)]
      [mLDP Multipoint-to-Multipoint (0x0509)]
      [Typed Wildcard (0x050B)]
```

Even though the routers no longer install each other’s labels in the LFIB, the bindings are still stored in the label database.

```
R6#show mpls ldp bindings neighbor 3.3.3.3
  lib entry: 1.1.1.1/32, rev 2
        remote binding: lsr: 3.3.3.3:0, label: 16
  lib entry: 2.2.2.2/32, rev 4
        remote binding: lsr: 3.3.3.3:0, label: 17
  lib entry: 3.3.3.3/32, rev 6
        remote binding: lsr: 3.3.3.3:0, label: imp-null
  lib entry: 4.4.4.4/32, rev 32
        remote binding: lsr: 3.3.3.3:0, label: 23
  lib entry: 5.5.5.5/32, rev 8
        remote binding: lsr: 3.3.3.3:0, label: 22
  lib entry: 6.6.6.6/32, rev 10
        remote binding: lsr: 3.3.3.3:0, label: 21
  lib entry: 10.1.2.0/24, rev 12
```

```
        remote binding: lsr: 3.3.3.3:0, label: 18
  lib entry: 10.19.20.0/24, rev 36
        remote binding: lsr: 3.3.3.3:0, label: 29
  lib entry: 19.19.19.19/32, rev 14
        remote binding: lsr: 3.3.3.3:0, label: 20
  lib entry: 20.2.3.0/24, rev 16
        remote binding: lsr: 3.3.3.3:0, label: imp-null
  lib entry: 20.2.4.0/24, rev 33
        remote binding: lsr: 3.3.3.3:0, label: 19
  lib entry: 20.3.4.0/24, rev 34
        remote binding: lsr: 3.3.3.3:0, label: imp-null
  lib entry: 20.3.6.0/24, rev 40
        remote binding: lsr: 3.3.3.3:0, label: imp-null
  lib entry: 20.4.5.0/24, rev 20
        remote binding: lsr: 3.3.3.3:0, label: 27
  lib entry: 20.4.6.0/24, rev 22
        remote binding: lsr: 3.3.3.3:0, label: 28
  lib entry: 20.5.6.0/24, rev 24
        remote binding: lsr: 3.3.3.3:0, label: 26
  lib entry: 20.5.19.0/24, rev 26
        remote binding: lsr: 3.3.3.3:0, label: 24
  lib entry: 20.6.19.0/24, rev 28
        remote binding: lsr: 3.3.3.3:0, label: 25
  lib entry: 20.20.20.20/32, rev 38
        remote binding: lsr: 3.3.3.3:0, label: 30
R6#show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         16         1.1.1.1/32       0             Gi1.46     20.4.6.4
17         17         2.2.2.2/32       0             Gi1.46     20.4.6.4
18         18         3.3.3.3/32       0             Gi1.46     20.4.6.4
19         Pop Label  5.5.5.5/32       2152          Gi1.56     20.5.6.5
20         21         10.1.2.0/24      0             Gi1.46     20.4.6.4
21         Pop Label  19.19.19.19/32   116           Gi1.619    20.6.19.19
22         23         20.2.3.0/24      0             Gi1.46     20.4.6.4
23         Pop Label  20.4.5.0/24      0             Gi1.46     20.4.6.4
           Pop Label  20.4.5.0/24      0             Gi1.56     20.5.6.5
24         Pop Label  20.5.19.0/24     0             Gi1.56     20.5.6.5
           Pop Label  20.5.19.0/24     0             Gi1.619    20.6.19.19
25         Pop Label  4.4.4.4/32       0             Gi1.46     20.4.6.4
26         Pop Label  20.2.4.0/24      0             Gi1.46     20.4.6.4
27         Pop Label  20.3.4.0/24      0             Gi1.46     20.4.6.4
28         Pop Label  10.19.20.0/24    0             Gi1.619    20.6.19.19
29         16015      20.20.20.20/32   0             Gi1.619    20.6.19.19
```

```
30         24         20.3.6.0/24      0             Gi1.46     20.4.6.4
```

Once the link between them is restored, protection ceases and the LFIB can be repopulated with the labels that were maintained in the database. The LDP adjacency does not have to be restored, as it never went down to begin with.

```
R6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.R6(config)#interface Gig1.36
                  R6(config-subif)#no shut
R6(config-subif)#
*May  2 04:16:38.791: LDP SP: 3.3.3.3:0: primary adj restored; stopping session protection holdup timer
*May  2 04:16:38.791: LDP SP: 3.3.3.3:0: state change (Protecting -> Ready)
R6(config-subif)#end
R6#
*May  2 04:16:38.791: %LDP-5-SP: 3.3.3.3:0: session recovery succeeded
*May  2 04:16:39.643: %SYS-5-CONFIG_I: Configured from console by console

R6#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface            16         16
1.1.1.1/32       0             Gi1.36     20.3.6.3

           16         1.1.1.1/32       0             Gi1.46     20.4.6.4    17         17
2.2.2.2/32       0             Gi1.36     20.3.6.3

           17         2.2.2.2/32       0             Gi1.46     20.4.6.4    18         Pop Label
3.3.3.3/32       0             Gi1.36     20.3.6.3

19         Pop Label  5.5.5.5/32       2152          Gi1.56     20.5.6.5    20         18
10.1.2.0/24      0             Gi1.36     20.3.6.3

           21         10.1.2.0/24      0             Gi1.46     20.4.6.4
21         Pop Label  19.19.19.19/32   116           Gi1.619    20.6.19.19  22         Pop Label
20.2.3.0/24      0             Gi1.36     20.3.6.3

23         Pop Label  20.4.5.0/24      0             Gi1.46     20.4.6.4
           Pop Label  20.4.5.0/24      0             Gi1.56     20.5.6.5
24         Pop Label  20.5.19.0/24     0             Gi1.56     20.5.6.5
           Pop Label  20.5.19.0/24     0             Gi1.619    20.6.19.19
25         Pop Label  4.4.4.4/32       0             Gi1.46     20.4.6.4
26         Pop Label  20.2.4.0/24      0             Gi1.46     20.4.6.4    27         Pop Label
20.3.4.0/24      0             Gi1.36     20.3.6.3

           Pop Label  20.3.4.0/24      0             Gi1.46     20.4.6.4
28         Pop Label  10.19.20.0/24    0             Gi1.619    20.6.19.19
```

29	16015	20.20.20.20/32	0	Gi1.619	20.6.19.19

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 3: MPLS v4

LDP TTL Propagation

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Basic L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure MPLS Label Distribution with LDP on all links connecting R2, R3, R4, R5, R6, and XR1.
- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2; at this point R1 and XR2 should have reachability to each other's Loopback0 networks.
- Configure the core of the SP network so that the TTL of packets coming from the customer's network is not copied into the MPLS label.

Configuration

```
R2:
no mpls ip propagate-ttl forwarded
!
router ospf 1
 mpls ldp autoconfig area 0

R3:
router ospf 1
 mpls ldp autoconfig area 0

R4:
router ospf 1
 mpls ldp autoconfig area 0

R5:
router ospf 1
 mpls ldp autoconfig area 0
```

```
R6:
router ospf 1
 mpls ldp autoconfig area 0

XR1:
router ospf 1
 mpls ldp auto-config
  !
 !
!
mpls ldp
!
mpls ip-ttl-propagate disable forwarded
```

Verification

Normally when unlabeled IP traffic is received on edge of the MPLS provider network the Time To Live (TTL) of the IP packet is copied into the MPLS header. Since just like in IP routing, the MPLS TTL is decremented on a hop-by-hop basis, the default behavior is that a customer's traceroute packets will see the individual hops in the service provider's core. This can be seen below in the traceroutes of R1 and XR2 before the default behavior is changed.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 5 msec 1 msec 0 msec
  2 20.2.3.3 [MPLS: Labels 20/16007 Exp 0] 5 msec 4 msec 4 msec
  3 20.3.6.6 [MPLS: Labels 20/16007 Exp 0] 9 msec 21 msec 18 msec
  4 20.6.19.19 20 msec 13 msec 15 msec
  5 10.19.20.20 16 msec *  8 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Sat May  2 04:53:15.069 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.5.19.5 [MPLS: Labels 16/43 Exp 0] 29 msec  9 msec  0 msec
 3  20.4.5.4 [MPLS: Labels 16/43 Exp 0] 0 msec  0 msec  0 msec
 4  10.1.2.2 [MPLS: Label 43 Exp 0] 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  9 msec
```

Even though the customer routers R1 and XR2 do not have routes for the provider routers R3 or R6, nor do R3 and R6 have routes to either R1 or XR2, these hops can still appear in the traceroute path due to exceptions of how traceroute is treated in MPLS differently than regular IP Routing. For more information on this refer to the INE Blog article MPLS Ping and Traceroute and to the Cisco Design Technote The Traceroute Command in MPLS.

The key point of this example is that when the default behavior of copying the IP TTL into the MPLS TTL is disabled with the IOS command **no mpls ip propagate-ttl** and the IOS XR command **mpls ip-ttl-propagate**, the customer routers are no longer able to see the detailed hops inside the service provider network. Instead of copying the TTL from the IP header into the label, the edge router doing label imposition uses a TTL of 255 on the labels. Below is the output of the traceroutes after TTL propagation has been disabled. Note that this command is only required on the PE routers doing label imposition. It is not necessary to enable this command on P routers.

```
R1#traceroute 20.20.20.20
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
```

```
  1 10.1.2.2 3 msec 1 msec 1 msec
  2 20.6.19.19 8 msec 7 msec 5 msec
  3 10.19.20.20 8 msec *  8 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Sat May  2 04:56:23.376 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 9 msec  0 msec  0 msec
 2  10.1.2.2 [MPLS: Label 43 Exp 0] 0 msec  0 msec  0 msec
 3  10.1.2.1 0 msec  *  0 msec
```

From the above output of the customer routers they simply see the PE routers and the other customer routers in the traceroute hops. The **forwarded** option of the IOS and IOS XR command allows locally generated IP packets to still have the IP TTL copied to the MPLS TTL, which means that traceroutes originated from inside the SP network will still see the details of the path. This is useful for when the service provider network is trying to troubleshoot or verify its own internal topology. As seen below R2's traceroute output still shows the hops in the MPLS Label Switch Path of R3 and R6 on the way to XR1's Loopback0 network.

```
R2#traceroute 19.19.19.19

Type escape sequence to abort.
Tracing the route to 19.19.19.19
VRF info: (vrf in name/id, vrf out name/id)
  1 20.2.3.3 [MPLS: Label 20 Exp 0] 12 msec
    20.2.4.4 [MPLS: Label 20 Exp 0] 6 msec
    20.2.3.3 [MPLS: Label 20 Exp 0] 6 msec
  2 20.4.6.6 [MPLS: Label 20 Exp 0] 2 msec
    20.3.6.6 [MPLS: Label 20 Exp 0] 8 msec
    20.4.6.6 [MPLS: Label 20 Exp 0] 15 msec
  3 20.6.19.19 21 msec *  7 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

Basic MPLS Tunnels

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Disable OSPF on R1 and XR2.
- Configure LDP on all of the transit links between R2, R3, R4, R5, R6, and XR1.
- Configure BGP on R1, R2, XR1, and XR2 as follows:
  - R1 should be in AS 1.
  - R2 and XR1 should be in AS 100.
  - XR2 should be in AS 20.
  - R1 and R2 should peer EBGP using their connected link.
  - R2 and XR1 should peer iBGP using the Loopback0 interfaces, and use **next-hop-self**.
  - XR1 and XR2 should peer EBGP using their connected link.
  - Advertise the prefix 1.1.1.1/32 into BGP on R1.
  - Advertise the prefix 20.20.20.20/32 into BGP on XR2.
- Once complete R1 and XR2 should be able to reach each other's Loopback0 interfaces when sourcing traffic from their own Loopback0 interface.

Configuration

```
R1:
no router ospf 1
!
router bgp 1
 network 1.1.1.1 mask 255.255.255.255
 neighbor 10.1.2.2 remote-as 100

R2:
mpls label protocol ldp
!
```

```
interface GigabitEthernet1.23
 mpls ip
!
interface GigabitEthernet1.24
 mpls ip
!
router bgp 100
 neighbor 10.1.2.1 remote-as 1
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 neighbor 19.19.19.19 next-hop-self

R3:
mpls label protocol ldp
!
interface GigabitEthernet1.23
 mpls ip
!
interface GigabitEthernet1.34
 mpls ip
!
interface GigabitEthernet1.36
 mpls ip
!
mpls ldp router-id Loopback0

R4:
mpls label protocol ldp
!
interface GigabitEthernet1.24
 mpls ip
!
interface GigabitEthernet1.34
 mpls ip
!
interface GigabitEthernet1.45
 mpls ip
!
interface GigabitEthernet1.46
 mpls ip
!
mpls ldp router-id Loopback0

R5:
mpls label protocol ldp
!
```

```
interface GigabitEthernet1.45
 mpls ip
!
interface GigabitEthernet1.56
 mpls ip
!
interface GigabitEthernet1.519
 mpls ip
!
mpls ldp router-id Loopback0

R6:
mpls label protocol ldp
!
interface GigabitEthernet1.36
 mpls ip
!
interface GigabitEthernet1.46
 mpls ip
!
interface GigabitEthernet1.56
 mpls ip
!
interface GigabitEthernet1.619
 mpls ip
!
 mpls ldp router-id Loopback0

XR1:
route-policy PASS
  pass
end-policy
!
router bgp 100
 address-family ipv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
 !
 neighbor 10.19.20.20
  remote-as 20
  address-family ipv4 unicast
```

```
   route-policy PASS in
   route-policy PASS out
   !
  !
 !
 mpls ldp
  router-id 19.19.19.19
  interface GigabitEthernet0/0/0/0.519
  !
  interface GigabitEthernet0/0/0/0.619
  !
 !

 XR2:
 no router ospf 1
 !
 route-policy PASS
   pass
 end-policy
 !
 router bgp 20
  address-family ipv4 unicast
   network 20.20.20.20/32
  !
 neighbor 10.19.20.19
  remote-as 100
  address-family ipv4 unicast
    route-policy PASS in
    route-policy PASS out
    !
  !
 !
 end
```

Verification

All devices in the core of the network have IGP routes and MPLS labels to each other. The only important labels in this example is the Loopback interfaces of R2 and XR1.

```
R2#show mpls forwarding-table
Local      Outgoing    Prefix           Bytes Label   Outgoing     Next Hop
Label      Label       or Tunnel Id     Switched      interface
16         23          19.19.19.19/32   0             Gi1.23       20.2.3.3
```

```
23          19.19.19.19/32    0              Gi1.24      20.2.4.4

18          22          10.19.20.0/24     0              Gi1.23      20.2.3.3
            22          10.19.20.0/24     0              Gi1.24      20.2.4.4
19          29          20.6.19.0/24      0              Gi1.23      20.2.3.3
            28          20.6.19.0/24      0              Gi1.24      20.2.4.4
32          20          6.6.6.6/32        0              Gi1.23      20.2.3.3
            20          6.6.6.6/32        0              Gi1.24      20.2.4.4
33          19          5.5.5.5/32        0              Gi1.24      20.2.4.4
34          Pop Label   4.4.4.4/32        0              Gi1.24      20.2.4.4
35          Pop Label   3.3.3.3/32        0              Gi1.23      20.2.3.3
36          27          20.5.6.0/24       0              Gi1.23      20.2.3.3
            26          20.5.6.0/24       0              Gi1.24      20.2.4.4
37          Pop Label   20.4.6.0/24       0              Gi1.24      20.2.4.4
38          27          20.5.19.0/24      0              Gi1.24      20.2.4.4
39          Pop Label   20.3.4.0/24       0              Gi1.23      20.2.3.3
            Pop Label   20.3.4.0/24       0              Gi1.24      20.2.4.4
40          Pop Label   20.3.6.0/24       0              Gi1.23      20.2.3.3
41          Pop Label   20.4.5.0/24       0              Gi1.24      20.2.4.4
R2#show ip cef 19.19.19.19 detail

19.19.19.19/32, epoch 2, per-destination sharing
  local label info: global/16
  1 RR source [no flags] nexthop 20.2.3.3 GigabitEthernet1.23 label 23
nexthop 20.2.4.4 GigabitEthernet1.24 label 23
RP/0/0/CPU0:XR1#show mpls forwarding
Sun May  3 14:27:48.208 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16002  18          3.3.3.3/32         Gi0/0/0/0.619 20.6.19.6       0
16003  19          4.4.4.4/32         Gi0/0/0/0.519 20.5.19.5       0
       19          4.4.4.4/32         Gi0/0/0/0.619 20.6.19.6       0
16004  Pop         5.5.5.5/32         Gi0/0/0/0.519 20.5.19.5       2256
16005  17          2.2.2.2/32         Gi0/0/0/0.519 20.5.19.5       2357
        17          2.2.2.2/32         Gi0/0/0/0.619 20.6.19.6       0

16006  Pop         6.6.6.6/32         Gi0/0/0/0.619 20.6.19.6       211072
16008  Pop         20.3.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16009  24          20.2.3.0/24        Gi0/0/0/0.619 20.6.19.6       816
16010  Pop         20.5.6.0/24        Gi0/0/0/0.519 20.5.19.5       0
       Pop         20.5.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16011  Pop         20.4.5.0/24        Gi0/0/0/0.519 20.5.19.5       0
16012  Pop         20.4.6.0/24        Gi0/0/0/0.619 20.6.19.6       0
16013  26          20.3.4.0/24        Gi0/0/0/0.519 20.5.19.5       0
       26          20.3.4.0/24        Gi0/0/0/0.619 20.6.19.6       0
```

```
16014  25          20.2.4.0/24       Gi0/0/0/0.519 20.5.19.5       0
       25          20.2.4.0/24       Gi0/0/0/0.619 20.6.19.6       0
16015  21          10.1.2.0/24       Gi0/0/0/0.519 20.5.19.5       0
       21          10.1.2.0/24       Gi0/0/0/0.619 20.6.19.6       0
```

R2 and XR1 peer iBGP with each other, along with EBGP to R1 and XR2 respectively.

```
R2#show bgp ipv4 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 4, main routing table version 4
2 network entries using 496 bytes of memory
2 path entries using 240 bytes of memory
2/2 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1280 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.2.1        4            1      18      17        4    0    0 00:12:32        1
19.19.19.19     4          100      13      15        4    0    0 00:10:03        1
RP/0/0/CPU0:XR1#show bgp ipv4 unicast summary

Sun May  3 14:20:49.277 UTC
BGP router identifier 19.19.19.19, local AS number 100
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000   RD version: 4
BGP main routing table version 4
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker               4          4          4          4           4           4

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
2.2.2.2           0   100      16      13        4    0    0 00:10:26          1
10.19.20.20       0    20       9       9        4    0    0 00:05:49          1
```

R1 and XR2 advertise their Loopback0 networks into BGP, which are then exchanged through the MPLS core via R2 and XR1.

```
R1#show bgp ipv4 unicast

 BGP table version is 4, local router ID is 1.1.1.1
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
 RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight Path
  *>  1.1.1.1/32       0.0.0.0                  0         32768 i
  *>  20.20.20.20/32   10.1.2.2                                0 100 20 i
 RP/0/0/CPU0:XR2#show bgp ipv4 unicast

 Sun May  3 14:21:35.944 UTC
 BGP router identifier 20.20.20.20, local AS number 20
 BGP generic scan interval 60 secs
 BGP table state: Active
 Table ID: 0xe0000000   RD version: 4
 BGP main routing table version 4
 BGP scan interval 60 secs

 Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
 Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
 *> 1.1.1.1/32         10.19.20.19                             0 100 1 i
 *> 20.20.20.20/32     0.0.0.0                  0         32768 i

 Processed 2 prefixes, 2 paths
```

Note that R1 and XR2 do not run MPLS.

```
R1#show mpls forwarding-table
 no MPLS apps enabled or MPLS not enabled on any interfaces
 R1#show ip cef 20.20.20.20
 20.20.20.20/32
   nexthop 10.1.2.2 GigabitEthernet1.12
 RP/0/3/CPU0:XR2#show mpls forwarding
 Sun May  3 14:22:23.560 UTC
 RP/0/0/CPU0:XR2#show cef ipv4 1.1.1.1/32

 Sun May  3 14:22:35.960 UTC
```

```
1.1.1.1/32, version 1399, internal 0x14000001 0x0 (ptr 0xa0edc674) [1], 0x0 (0x0), 0x0 (0x0)
 Updated May  3 14:15:05.181
 local adjacency 10.19.20.19
 Prefix Len 32, traffic index 0, precedence n/a, priority 4
   via 10.19.20.19, 2 dependencies, recursive, bgp-ext [flags 0x6020]
    path-idx 0 NHID 0x0 [0xa0edb874 0x0]
    next hop 10.19.20.19 via 10.19.20.19/32
```

When R2 and XR1 exchange the BGP routes from R1 and XR2, the next-hop value is set to their local Loopback0 interfaces.

```
R2#show bgp ipv4 unicast 20.20.20.20/32
BGP routing table entry for 20.20.20.20/32, version 4
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  20 19.19.19.19
 (metric 4) from 19.19.19.19 (19.19.19.19)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
RP/0/0/CPU0:XR1#show bgp ipv4 unicast 1.1.1.1/32
Sun May  3 14:39:37.349 UTC
BGP routing table entry for 1.1.1.1/32
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  3           3
Last Modified: May  3 14:12:22.451 for 00:27:15
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    10.19.20.20
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    10.19.20.20
  1 2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, best, group-best, import-candidate
      Received Path ID 0, Local Path ID 1, version 3
```

Since R2 has an MPLS label for 19.19.19.19, and likewise XR1 has an MPLS label for 2.2.2.2, traffic is MPLS encapsulated when going to 1.1.1.1 and 20.20.20.20 using label values seen below.

```
R2#show ip cef 20.20.20.20 detail
```

```
20.20.20.20/32, epoch 2, flags [rib only nolabel, rib defined all labels] recursive via 19.19.19.19
    nexthop 20.2.3.3 GigabitEthernet1.23 label 23
    nexthop 20.2.4.4 GigabitEthernet1.24 label 23
```

R2#show ip cef 19.19.19.19 detail

```
 19.19.19.19/32
, epoch 2, per-destination sharing
  local label info: global/16
  1 RR source [no flags]  nexthop 20.2.3.3 GigabitEthernet1.23 label 23
  nexthop 20.2.4.4 GigabitEthernet1.24 label 23
```

R2#show mpls forwarding-table 19.19.19.19

```
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface              16
23         19.19.19.19/32   0            Gi1.23      20.2.3.3
    23         19.19.19.19/32   0            Gi1.24      20.2.4.4
```

RP/0/0/CPU0:XR1#show cef ipv4 1.1.1.1/32 detail

```
Sun May  3 14:40:10.927 UTC
1.1.1.1/32, version 3133, internal 0x14000001 0x0 (ptr 0xa0edbe74) [1], 0x0 (0x0), 0x0 (0x0)
 Updated May  3 14:26:35.123
 local adjacency 20.5.19.5
 Prefix Len 32, traffic index 0, precedence n/a, priority 4
  gateway array (0xa0d30310) reference count 1, flags 0x4030, source rib (6), 0 backups
              [1 type 3 flags 0x680a1 (0xa0df1a28) ext 0x218 (0xa16600a8)]
  LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0] via 2.2.2.2
, 2 dependencies, recursive [flags 0x6000]
    path-idx 0 NHID 0x0 [0xa0edbaf4 0x0] next hop 2.2.2.2 via 2.2.2.2/32



    Load distribution: 0 1 (refcount 1)

    Hash  OK  Interface                 Address     0      Y GigabitEthernet0/0/0/0.519 20.5.19.5
          1      Y GigabitEthernet0/0/0/0.619 20.6.19.6
```

RP/0/0/CPU0:XR1#show ip cef 2.2.2.2/32 detail

```
Sun May  3 14:43:13.674 UTC
2.2.2.2/32, version 601, internal 0x4004001 0x0 (ptr 0xa0edbaf4) [2], 0x0 (0xa0ea7878), 0x228 (0xa16601b0)
 Updated May  3 14:10:18.089
 local adjacency 20.5.19.5
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
  gateway array (0xa0d309a0) reference count 15, flags 0x68, source lsd (4), 1 backups
              [6 type 5 flags 0x8081 (0xa14106e0) ext 0x0 (0x0)]
  LW-LDI[type=5, refc=3, ptr=0xa0ea7878, sh-ldi=0xa14106e0]
   via 20.5.19.5, GigabitEthernet0/0/0/0.519, 8 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0xa16c80cc 0x0]
```

```
    next hop 20.5.19.5
    tx adjacency local label 16005      labels imposed {17}
   via 20.6.19.6, GigabitEthernet0/0/0/0.619, 10 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 1 NHID 0x0 [0xa16c8228 0x0]
    next hop 20.6.19.6
    tx adjacency local label 16005      labels imposed {17}


    Load distribution: 0 1 (refcount 6)

    Hash  OK  Interface                 Address    0     YGigabitEthernet0/0/0/0.519 20.5.19.5
         1     YGigabitEthernet0/0/0/0.619 20.6.19.6

RP/0/0/CPU0:XR1#show mpls forwarding prefix 2.2.2.2/32
Sun May  3 14:40:59.984 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------16005
17           2.2.2.2/32         Gi0/0/0/0.519 20.5.19.5       3792
       17           2.2.2.2/32         Gi0/0/0/0.619 20.6.19.6       0
```

Multiple outgoing labels are shown because R2 and XR1 have multiple equal cost paths to reach each other's Loopback0 interfaces. The final result of this configuration is that R1 and XR2 have IP reachability to each other, even though the devices in the core (R3, R4, R5, & R6) do not have IP routing information about 1.1.1.1/32 or 20.20.20.20/32.

```
R1#ping 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/13 ms
RP/0/0/CPU0:XR2#ping 1.1.1.1 source 20.20.20.20
Sun May  3 14:45:29.435 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/29 ms

R3#show ip route 1.1.1.1
% Network not in table

R3#show ip route 20.20.20.20% Network not in table
R4#show ip route 1.1.1.1
% Network not in table
R4#show ip route 20.20.20.20% Network not in table
```

```
R5#show ip route 1.1.1.1
% Network not in table
R5#show ip route 20.20.20.20
% Network not in table

R6#show ip route 1.1.1.1
% Network not in table
R6#show ip route 20.20.20.20
% Network not in table
```

MPLS forwarding table counters show that traffic between the Loopback0 networks of R1 and XR2 is using a Labeled Switch Path (LSP) between R2 and XR1's Loopback0 networks.

```
RP/0/0/CPU0:XR2#ping 1.1.1.1 source 20.20.20.20 count 100
Sun May  3 15:03:20.092 UTC
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/17/29 ms
R4#show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
17         Pop Label  2.2.2.2/32       27709         Gi1.24     20.2.4.2

18         Pop Label  3.3.3.3/32       0             Gi1.34     20.3.4.3
19         Pop Label  5.5.5.5/32       0             Gi1.45     20.4.5.5
20         Pop Label  6.6.6.6/32       0             Gi1.46     20.4.6.6
21         Pop Label  10.1.2.0/24      0             Gi1.24     20.2.4.2
22         22         10.19.20.0/24    0             Gi1.45     20.4.5.5
           22         10.19.20.0/24    0             Gi1.46     20.4.6.6
23         23         19.19.19.19/32   0             Gi1.45     20.4.5.5
23         19.19.19.19/32   1756          Gi1.46     20.4.6.6

24         Pop Label  20.2.3.0/24      0             Gi1.24     20.2.4.2
           Pop Label  20.2.3.0/24      0             Gi1.34     20.3.4.3
25         Pop Label  20.3.6.0/24      0             Gi1.34     20.3.4.3
           Pop Label  20.3.6.0/24      0             Gi1.46     20.4.6.6
26         Pop Label  20.5.6.0/24      0             Gi1.45     20.4.5.5
           Pop Label  20.5.6.0/24      0             Gi1.46     20.4.6.6
27         Pop Label  20.5.19.0/24     0             Gi1.45     20.4.5.5
```

```
28          Pop Label  20.6.19.0/24     0              Gi1.46     20.4.6.6
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with Static Routing

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2 and LDP**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure routing for the VRF as follows:
  - R1 should have a default route pointing towards R2.
  - R2 should have a static route for 1.1.1.1/32 pointing towards R1.
  - XR1 should have a static route for 20.20.20.20/32 pointing towards XR2.
  - XR2 should have a default route pointing towards XR1.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
  - Advertise the static routes towards R1 and XR2 into BGP on R2 and XR1 respectively.
- Once complete R1 and XR2 should have reachability to each other's Loopback0 interfaces when sourcing traffic from their own Loopback0 interfaces.

Configuration

```
R1:
ip route 0.0.0.0 0.0.0.0 10.1.2.2


R2:
```

```
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  network 1.1.1.1 mask 255.255.255.255
 exit-address-family
 !
 ip route vrf VPN_A 1.1.1.1 255.255.255.255 10.1.2.1

XR1:

vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
router static
 vrf VPN_A
```

```
 address-family ipv4 unicast
   20.20.20.20/32 GigabitEthernet0/0/0/0.1920 10.19.20.20
  !
 !
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf VPN_A
  rd 100:1
  address-family ipv4 unicast
   network 20.20.20.20/32
  !
 !
!

XR2:
router static
 address-family ipv4 unicast
  0.0.0.0/0 GigabitEthernet0/0/0/0.1920 10.19.20.19
 !
!
```

Verification

show vrf detail is useful to quickly verify configured VRFs names, RDs, RT import and export policy, and assigned links.

```
R2#show vrf detail
VRF VPN_A (VRF Id = 3); default RD 100:1
; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces: Gi1.12

Address family ipv4 unicast (Table ID = 0x3):
  Flags: 0x0
  Export VPN route-target communities
```

```
RT:100:1

  Import VPN route-target communities RT:100:1

  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 unicast not active
Address family ipv4 multicast not active
RP/0/0/CPU0:XR1#show vrf VPN_A detail
Sun May  3 15:36:57.384 UTC
VRF VPN_A; RD 100:1
; VPN ID not set
VRF mode: Regular
Description not set
Interfaces: GigabitEthernet0/0/0/0.1920
Address family IPV4 Unicast
  Import VPN route-target communities: RT:100:1
  Export VPN route-target communities: RT:100:1

  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
```

Note that in IOS XR, once an interface is removed from the global routing table and assigned to a VRF table, it no longer appears in the **show ipv4 interface brief** output, as seen below. Instead, interfaces can be verified with the command **show ipv4 vrf all interface brief**.

```
RP/0/0/CPU0:XR1#show ip interface brief
Sun May  3 15:37:45.400 UTC

Interface                      IP-Address      Status                Protocol
Loopback0                      19.19.19.19     Up                    Up
MgmtEth0/0/CPU0/0              unassigned      Up                    Up
GigabitEthernet0/0/0/0         unassigned      Up                    Up
GigabitEthernet0/0/0/0.519     20.5.19.19      Up                    Up
GigabitEthernet0/0/0/0.619     20.6.19.19      Up                    Up
```

```
RP/0/0/CPU0:XR1#show ipv4 vrf all interface brief

Sun May  3 15:38:16.118 UTC

Interface                      IP-Address      Status          Protocol Vrf-Name
Loopback0                      19.19.19.19     Up              Up       default
MgmtEth0/0/CPU0/0              unassigned      Up              Up       default
GigabitEthernet0/0/0/0         unassigned      Up              Up       default
GigabitEthernet0/0/0/0.519     20.5.19.19      Up              Up       default
GigabitEthernet0/0/0/0.619     20.6.19.19      Up              Up       default
GigabitEthernet0/0/0/0.1920    10.19.20.19     Up              Up       VPN_A

RP/0/0/CPU0:XR1#show ipv4 vrf VPN_A interface brief

Sun May  3 15:38:44.146 UTC

Interface                      IP-Address      Status                Protocol
GigabitEthernet0/0/0/0.1920    10.19.20.19     Up                    Up
```

In this example, the CE routers R1 and XR2 simply have default routes pointing to the PE routers R2 and XR1, resulting in one of the simplest MPLS L3VPN designs. From the CE routers perspective these are just normal static routes in the global routing table.

```
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 10.1.2.2
RP/0/3/CPU0:XR2#show route ipv4 static
Sun May  3 15:39:48.222 UTC
S*   0.0.0.0/0 [1/0] via 10.19.20.19, 00:04:48, GigabitEthernet0/0/0/0.1920
```

From the PE routers’ R2 and XR1’s perspective, their static routes to the customers exist in the VRF table.

```
R2#show ip route vrf VPN_A static
 Routing Table: VPN_A
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnetsS         1.1.1.1 [1/0] via 10.1.2.1
RP/0/0/CPU0:XR1#show route vrf VPN_A ipv4 static
Sun May  3 15:40:49.918 UTC
 S    20.20.20.20/32 [1/0] via 10.19.20.20, 00:06:12, GigabitEthernet0/0/0/0.1920
```

R2 and XR1 then advertise these static routes into the VPNv4 BGP topology. In this case it is done with the network statement, but it could also be done with redistribution.

```
R2#show bgp vpnv4 unicast all
BGP table version is 5, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A) *> 1.1.1.1/32        10.1.2.1
                0         32768 i *>i 20.20.20.20/32   19.19.19.19
             0    100      0 i

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast
Sun May  3 15:41:22.385 UTC
BGP router identifier 19.19.19.19, local AS number 100
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
```

```
BGP main routing table version 5
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)*>i 1.1.1.1/32         2.2.2.2
                  0    100      0 i*> 20.20.20.20/32     10.19.20.20
              0         32768 i

Processed 2 prefixes, 2 paths
```

Note that R2 and XR1 use the Loopback0 interfaces of each other as the next-hop value for the VPNv4 learned routes, since this is the **update-source** of the iBGP session. In addition to the next-hop value, the VPN label derived from VPNv4 BGP can be seen in the below output. This is the label value that the PE routers use to find the final customer route in the VRF.

```
R2#show bgp vpnv4 unicast all 20.20.20.20/32
BGP routing table entry for 100:1:20.20.20.20/32, version 5
Paths: (1 available, best #1, table VPN_A)
  Not advertised to any peer
  Refresh Epoch 1
  Local 19.19.19.19
 (metric 4) (via default) from 19.19.19.19 (19.19.19.19)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 mpls labels in/out nolabel/16000
      rx pathid: 0, tx pathid: 0x0
R2#show bgp vpnv4 unicast all labels
    Network          Next Hop In label/Out label
Route Distinguisher: 100:1 (VPN_A) 1.1.1.1/32       10.1.2.1 31
/nolabel 20.20.20.20/32    19.19.19.19     nolabel/16000
RP/0/0/CPU0:XR1#show bgp vrf VPN_A ipv4 unicast 1.1.1.1/32
Sun May  3 15:42:08.092 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  5           5
Last Modified: May  3 15:34:43.451 for 00:07:24
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
```

```
2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2) Received Label 31
      Origin IGP, metric 0, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 5
      Extended community: RT:100:1
      Source VRF: VPN_A, Source Route Distinguisher: 100:1
```

RP/0/0/CPU0:XR1#show bgp vrf VPN_A ipv4 unicast labels

```
Sun May  3 15:42:43.450 UTC
BGP VRF VPN_A, state: Active
BGP Route Distinguisher: 100:1
VRF ID: 0x60000005
BGP router identifier 19.19.19.19, local AS number 100
BGP table state: Active
Table ID: 0xe0000014   RD version: 5
BGP main routing table version 5

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete   Network            Next Hop Rcvd Label Local Label
Route Distinguisher: 100:1 (default for vrf VPN_A) *>i 1.1.1.1/32         2.2.2.2 31
              nolabel         *> 20.20.20.20/32      10.19.20.20     nolabel 16000


Processed 2 prefixes, 2 paths
```

R2 and XR1 then combine this VPN label with the transport label used to reach each other's Loopback0 interfaces (the next-hop for the VPNv4 route). In this case the transport label is derived from OSPF + LDP. The transport label is used to tell the MPLS core what the exit PE is out of the network.

R2#show ip route 19.19.19.19

```
Routing entry for 19.19.19.19/32
  Known via "ospf 1", distance 110, metric 4, type intra area
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:21:54 ago
  Routing Descriptor Blocks: 20.2.4.4, from 19.19.19.19, 00:21:54 ago, via GigabitEthernet1.24
      Route metric is 4, traffic share count is 1   *
20.2.3.3, from 19.19.19.19, 00:21:54 ago, via GigabitEthernet1.23
      Route metric is 4, traffic share count is 1
```

R2#show mpls forwarding-table 19.19.19.19

```
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface              29
26          19.19.19.19/32    0              Gi1.23      20.2.3.3
    25          19.19.19.19/32    0              Gi1.24      20.2.4.4
```

```
RP/0/0/CPU0:XR1#show route ipv4 2.2.2.2


Sun May  3 15:44:12.624 UTC


Routing entry for 2.2.2.2/32
  Known via "ospf 1", distance 110, metric 4, type intra area
  Installed May  3 15:21:39.646 for 00:22:33
  Routing Descriptor Blocks 20.5.19.5, from 2.2.2.2, via GigabitEthernet0/0/0/0.519
      Route metric is 4 20.6.19.6, from 2.2.2.2, via GigabitEthernet0/0/0/0.619
      Route metric is 4
  No advertising protos.
RP/0/0/CPU0:XR1#show mpls forwarding prefix 2.2.2.2/32
Sun May  3 15:44:41.522 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------16005
18            2.2.2.2/32         Gi0/0/0/0.519 20.5.19.5       4454
        19            2.2.2.2/32         Gi0/0/0/0.619 20.6.19.6       0
```

The two of these together, the VPN label and the transport label, make up the full label stack that is imposed when the PE routers receive traffic from the CE. This can be verified in the CEF table on the PE routers. The below cef table output of R2 indicates that the VPN label is 16000, and the transport label is either 25 or 26, depending which interface the traffic is CEF switched to.

```
R2#show ip cef vrf VPN_A 20.20.20.20 detail
20.20.20.20/32, epoch 0, flags [rib defined all labels] recursive via 19.19.19.19 label 16000
nexthop 20.2.3.3 GigabitEthernet1.23 label 26
nexthop 20.2.4.4 GigabitEthernet1.24 label 25
```

In XR1's case, the label stack consists of 31 as the VPN label, and either 18 or 19 as the transport label.

```
RP/0/0/CPU0:XR1#show cef vrf VPN_A 1.1.1.1/32 detail


Sun May  3 15:46:07.026 UTC
1.1.1.1/32, version 11, internal 0x14004001 0x0 (ptr 0xa0edc8f4) [1], 0x0 (0x0), 0x208 (0xa13f6348)
 Updated May  3 15:34:43.533
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
  gateway array (0xa0d300b8) reference count 1, flags 0x4038, source rib (6), 0 backups
                [1 type 1 flags 0x48089 (0xa141044c) ext 0x0 (0x0)]
  LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0]
```

```
via 2.2.2.2, 3 dependencies, recursive
 [flags 0x6000]
    path-idx 0 NHID 0x0 [0xa145e574 0x0]
    next hop VRF - 'default', table - 0xe0000000 next hop 2.2.2.2 via 16005/0/21
 next hop 20.5.19.5/32 Gi0/0/0/0.519 labels imposed {18 31}
 next hop 20.6.19.6/32 Gi0/0/0/0.619 labels imposed {19 31}



    Load distribution: 0 (refcount 1)

    Hash  OK  Interface                 Address
    0     Y   Unknown                   16005/0
```

The full label stack can also be verified by looking at a traceroute output from the CE. Note that the transport label changes on a hop-by-hop basis, but the VPN label remains the same end-to-end. R4 is the Penultimate hop for R2, so the top label 17 is being removed for packets going to R2. Likewise on the other side R5 is the Penultimate hop for XR1, as the transport label 24 is being popped for traffic going towards XR1.

```
RP/0/0/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
 Sun May  3 15:48:51.955 UTC

 Type escape sequence to abort.
 Tracing the route to 1.1.1.1

  1  10.19.20.19 0 msec  0 msec  0 msec
  2  20.5.19.5 [MPLS: Labels 18/31 Exp 0] 9 msec  0 msec  0 msec   3  20.4.5.4 [MPLS: Labels 17
/31 Exp 0] 0 msec  9 msec  0 msec
  4  10.1.2.2 [MPLS: Label 31 Exp 0] 0 msec  0 msec  0 msec
  5  10.1.2.1 0 msec  *  0 msec
 R4#show mpls forwarding-table 2.2.2.2
 Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
 Label      Label      or Tunnel Id     Switched      interface           17 Pop Label
   2.2.2.2/32       13237         Gi1.24     20.2.4.2
 R1#traceroute 20.20.20.20 source 1.1.1.1
 Type escape sequence to abort.
 Tracing the route to 20.20.20.20
 VRF info: (vrf in name/id, vrf out name/id)
   1 10.1.2.2 4 msec 2 msec 1 msec
   2 20.2.4.4 [MPLS: Labels 25/16000 Exp 0] 10 msec 6 msec 6 msec   3 20.4.5.5 [MPLS: Labels 24
/16000 Exp 0] 14 msec 8 msec 24 msec
   4 20.5.19.19 19 msec 14 msec 14 msec
   5 10.19.20.20 14 msec *  10 msec
```

```
R5#show mpls forwarding-table 19.19.19.19

Local      Outgoing   Prefix           Bytes Label    Outgoing    Next Hop
Label      Label      or Tunnel Id     Switched       interface            24 Pop Label
  19.19.19.19/32   7188          Gi1.519    20.5.19.19
```

The final result is that even though the devices in the core, i.e. R3, R4, R5, & R6, do not have routes for the customer VRF VPN_A, they are able to transport label switched packets that go between the PE routers of R2 and XR1.

```
R3#show ip route 1.1.1.1
% Network not in table
R3#show ip route 20.20.20.20
% Subnet not in table
R4#show ip route 1.1.1.1
% Network not in tableR4#show ip route 20.20.20.20
% Subnet not in table
R5#show ip route 1.1.1.1
% Network not in tableR5#show ip route 20.20.20.20
% Subnet not in table
R6#show ip route 1.1.1.1
% Network not in tableR6#show ip route 20.20.20.20

% Subnet not in table
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with RIPv2

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2 and LDP**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure RIPv2 routing for the VRF as follows:
  - Enable RIPv2 between R1 & R2.
  - Enable RIPv2 between XR1 & XR2.
  - Advertise the Loopback0 networks of R1 & XR2 into RIP.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
- Redistribute between BGP and the RIPv2 as follows:
  - RIPv2 routes learned by the PEs from the CEs should have their metric transparently redistributed via the BGP MED attribute.
  - The connected PE to CE links should appear with a metric of 1 on the remote CEs
- Once complete R1 and XR2 should have reachability to each other's Loopback0 interfaces and PE-CE links.

Configuration

```
R1:
router rip
 version 2
 network 1.0.0.0
 network 10.0.0.0
 no auto-summary

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric transparent
  network 10.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 100
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family
```

```
!

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
route-policy BGP_TO_RIP
  if destination in (10.1.2.0/24) then
    set rip-metric 1
  else
    pass
  endif
end-policy
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf VPN_A
  rd 100:1
  address-family ipv4 unicast
   redistribute rip
  !
 !
!
router rip
 vrf VPN_A
  interface GigabitEthernet0/0/0/0.1920
  !
  redistribute bgp 100 route-policy BGP_TO_RIP
```

```
 !
!
end

XR2:
router rip
 interface Loopback0
 !
 interface GigabitEthernet0/0/0/0.1920
 !
!
```

Verification

VRF aware RIP routing uses one global process, with sub-processes on a per VRF basis. When routes are redistributed from a VRF aware RIP process into BGP, the RIP metric is automatically copied into the BGP MED field. This can be seen in the BGP output below.

```
R2#show bgp vpnv4 unicast all
BGP table version is 23, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
 *>  1.1.1.1/32       10.1.2.1                 1         32768 ?
 *>  10.1.2.0/24      0.0.0.0                  0         32768 ?
 *>i 10.19.20.0/24    19.19.19.19              0    100      0 ?
 *>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast

Sun May  3 16:35:30.493 UTC
BGP router identifier 19.19.19.19, local AS number 100
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 25
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
```

```
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
*>i1.1.1.1/32       2.2.2.2                  1    100      0 ?
*>i10.1.2.0/24      2.2.2.2                  0    100      0 ?
*> 10.19.20.0/24    0.0.0.0                  0         32768 ?
*> 20.20.20.20/32   10.19.20.20              1         32768 ?

Processed 4 prefixes, 4 paths
```

This can be further verified if an offset list is applied to the RIP process to modify the metric values, as seen below.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ripR1(config-router)#offset-list 0 out 7 Gig1.12
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#clear ip route *
R1#
R2#show ip route vrf VPN_A rip

Routing Table: VPN_A
Codes: L - local, 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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnetsR         1.1.1.1 [120/8]
 via 10.1.2.1, 00:00:10, GigabitEthernet1.12
```

The new RIP metric of 8 is copied into the BGP MED of the VPNv4 route.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
BGP routing table entry for 100:1:1.1.1.1/32, version 24
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
```

```
      1
   Refresh Epoch 1
   Local
     10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)      Origin incomplete, metric 8
, localpref 100, weight 32768, valid, sourced, best
       Extended Community: RT:100:1
       mpls labels in/out 43/nolabel
       rx pathid: 0, tx pathid: 0x0
```

When BGP is redistributed back into RIP on the remote side, the BGP MED is copied back into the RIP metric.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32

Sun May  3 16:38:10.922 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 26          26
Last Modified: May  3 16:36:37.451 for 00:01:33
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
      Received Label 43       Origin incomplete, metric 8
, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 26
      Extended community: RT:100:1
      Source VRF: VPN_A, Source Route Distinguisher: 100:1
RP/0/0/CPU0:XR1#show rip vrf VPN_A database

Sun May  3 16:38:50.439 UTC

Routes held in RIP's topology database: 1.1.1.1/32
    [ 9 ] distance: 200 redistributed

1.0.0.0/8    auto-summary
10.1.2.0/24
    [1] distance: 200    redistributed
10.19.20.0/24
    [0]    directly connected, GigabitEthernet0/0/0/0.1920
10.0.0.0/8    auto-summary
20.20.20.20/32
    [1] via 10.19.20.20, next hop 10.19.20.20, Uptime: 5s, GigabitEthernet0/0/0/0.1920
20.0.0.0/8    auto-summary
```

The final result is the remote CE router sees the RIP metric maintained and incremented once across the MPLS VPN network.

```
RP/0/3/CPU0:XR2#show route ipv4 rip

Sun May  3 16:39:29.967 UTC
R    1.1.1.1/32 [120/9]
 via 10.19.20.19, 00:02:53, GigabitEthernet0/0/0/0.1920
R    10.1.2.0/24 [120/1] via 10.19.20.19, 00:05:11, GigabitEthernet0/0/0/0.1920
```

One potential "bug" in this configuration is that if the BGP MED is zero, some version of IOS XR do not redistribute the route from BGP into the RIP database unless the metric is manually set. This is why the additional Routing Policy Language is used to match the prefix connected between R1 and R2, and manually set the metric as the route is redistributed into RIP. With the RPL policy applied, the route appears in the RIP database of XR1, and hence the routing table of XR2. Note that this bug does not appear to be present in the version of IOS-XR used during these labs - IOS-XR 5.2.0.

```
RP/0/0/CPU0:XR1#show run router rip
Sun May  3 16:40:23.943 UTC
router rip
 vrf VPN_A
  interface GigabitEthernet0/0/0/0.1920
  ! redistribute bgp 100 route-policy BGP_TO_RIP
 !
!
RP/0/0/CPU0:XR1#show rpl
Sun May  3 16:40:45.811 UTC
route-policy BGP_TO_RIP if destination in (10.1.2.0/24) then
set rip-metric 1
  else
    pass
  endif
end-policy
!
RP/0/0/CPU0:XR1#show rip vrf VPN_A database 10.1.2.0/24
Sun May  3 16:41:07.430 UTC

10.1.2.0/24    [1
] distance: 200    redistributed
```

If the Routing Policy is removed, the route continues being advertised on the current version of IOS-XR. On earlier versions of IOS-XR, such as 3.9, the removal of the Routing Policy would prevent the route from being redistributed.

```
RP/0/0/CPU0:XR1#config t
Sun May  3 16:41:30.308 UTC
RP/0/0/CPU0:XR1(config)#router rip
RP/0/0/CPU0:XR1(config-rip)# vrf VPN_A
RP/0/0/CPU0:XR1(config-rip-vrf)#no redistribute bgp 100 route-policy BGP_TO_RIP
RP/0/0/CPU0:XR1(config-rip-vrf)#redistribute bgp 100
RP/0/0/CPU0:XR1(config-rip-vrf)#show config
Sun May  3 16:42:08.056 UTC
Building configuration...
!! IOS XR Configuration 5.2.0
router rip
 vrf VPN_A no redistribute bgp 100 route-policy BGP_TO_RIP
 redistribute bgp 100
  !
 !
end
RP/0/0/CPU0:XR1(config-rip-vrf)#commit
Sun May  3 16:42:39.674 UTC
RP/0/0/CPU0:XR1(config-rip-vrf)#end
RP/0/0/CPU0:XR1#show rip vrf VPN_A database 10.1.2.0/24
Sun May  3 16:52:13.694 UTC

10.1.2.0/24
    [1] distance: 200    redistributed

RP/0/3/CPU0:XR2#show route ipv4 rip

Sun May  3 16:52:46.202 UTC

R    1.1.1.1/32 [120/9] via 10.19.20.19, 00:05:12, GigabitEthernet0/0/0/0.1920
R    10.1.2.0/24 [120/1] via 10.19.20.19, 00:05:12, GigabitEthernet0/0/0/0.1920
```

An alternate fix to this would be to manually set the BGP MED on the remote side as redistribution from RIP to BGP is occurring, such as the following.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.R2(config)#route-map RIP_TO_BGP
R2(config-route-map)#set metric 5
R2(config-route-map)#router bgp 100
R2(config-router)#address-family ipv4 vrf VPN_A
R2(config-router-af)#redistribute rip route-map RIP_TO_BGP
```

```
R2(config-router-af)#end
R2#
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#R2#show bgp vpnv4 unicast all
BGP table version is 38, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A) *>  1.1.1.1/32       10.1.2.15
         32768 ? *>  10.1.2.0/24      0.0.0.05
         32768 ?
 *>i 10.19.20.0/24    19.19.19.19              0    100      0 ?
 *>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
RP/0/3/CPU0:XR2#show route ipv4 rip

Sun May  3 16:54:38.555 UTC

R    1.1.1.1/32 [120/6] via 10.19.20.19, 00:00:35, GigabitEthernet0/0/0/0.1920
R    10.1.2.0/24 [120/6] via 10.19.20.19, 00:00:35, GigabitEthernet0/0/0/0.1920
```

In either case the final result should be that the customer sites have full reachability to each other.

```
R1#ping 20.20.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5)
, round-trip min/avg/max = 9/12/18 ms
R1#ping 10.19.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.19.20.20, timeout is 2 seconds:
!!!!!Success rate is 100 percent (5/5)
, round-trip min/avg/max = 7/9/12 ms
R1#traceroute 10.19.20.20

Type escape sequence to abort.
Tracing the route to 10.19.20.20
VRF info: (vrf in name/id, vrf out name/id)
```

```
  1 10.1.2.2 1 msec 2 msec 1 msec   2 20.2.3.3 [MPLS: Labels 26
/16000 Exp 0] 9 msec 7 msec 4 msec   3 20.3.6.6 [MPLS: Labels 25
/16000 Exp 0] 8 msec 14 msec 22 msec
  4 20.6.19.19 28 msec 8 msec 8 msec
  5 10.19.20.20 16 msec *  9 msec

RP/0/3/CPU0:XR2#ping 1.1.1.1
Sun May  3 16:55:24.091 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
RP/0/3/CPU0:XR2#ping 10.1.2.1
Sun May  3 16:55:29.091 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
RP/0/0/CPU0:XR2#traceroute 10.1.2.1
Sun May  3 17:02:16.753 UTC

Type escape sequence to abort.
Tracing the route to 10.1.2.1

 1  10.19.20.19 0 msec  0 msec  0 msec   2  20.5.19.5 [MPLS: Labels 18
/44 Exp 0] 0 msec  0 msec  0 msec   3  20.4.5.4 [MPLS: Labels 17
/44 Exp 0] 0 msec  0 msec  9 msec
 4  10.1.2.2 0 msec  0 msec  9 msec
 5  10.1.2.1 0 msec  *  0 msec
```

Inside the core of the network this traffic is label switched towards the Loopback0 interfaces of the PE routers, R2 and XR1.

```
R5#show mpls forwarding-table 2.2.2.2
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface          18 17
        2.2.2.2/32       32743         Gi1.45     20.4.5.4
R6#show mpls forwarding-table 19.19.19.19
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface              25
        Pop Label  19.19.19.19/32   28624         Gi1.619    20.6.19.19
```

The inner label values of 1600 and 44 come from the origination of the VPNv4 routes on R2 and XR1.

```
R2#show bgp vpnv4 unicast all 10.19.20.0
 BGP routing table entry for 100:1:10.19.20.0/24, version 34
 Paths: (1 available, best #1, table VPN_A)
   Not advertised to any peer
   Refresh Epoch 1
   Local
     19.19.19.19 (metric 4) (via default) from 19.19.19.19 (19.19.19.19)
       Origin incomplete, metric 0, localpref 100, valid, internal, best
       Extended Community: RT:100:1 mpls labels in/out nolabel/16000
   rx pathid: 0, tx pathid: 0x0
 RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 10.1.2.0/24


 Sun May  3 16:58:56.027 UTC
 BGP routing table entry for 10.1.2.0/24, Route Distinguisher: 100:1
 Versions:
   Process           bRIB/RIB  SendTblVer
   Speaker                 42          42
 Last Modified: May  3 16:54:02.451 for 00:04:53
 Paths: (1 available, best #1)
   Not advertised to any peer
   Path #1: Received by speaker 0
   Not advertised to any peer
   Local
     2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2) Received Label 44

       Origin incomplete, metric 5, localpref 100, valid, internal, best, group-best, import-candidate, imported
       Received Path ID 0, Local Path ID 1, version 42
       Extended community: RT:100:1
       Source VRF: VPN_A, Source Route Distinguisher: 100:1
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with EIGRP

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2 and LDP**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure EIGRP routing for the VRF as follows:
  - Use EIGRP AS 1.
  - Enable EIGRP between R1 & R2.
  - Enable EIGRP between XR1 & XR2.
  - Advertise the Loopback0 networks of R1 & XR2 into RIP.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
- Redistribute between BGP and the EIGRP.
- Once complete R1 and XR2 should have reachability to each other’s Loopback0 interfaces and PE-CE links.

Configuration

```
R1:
router eigrp 1
 network 1.0.0.0
 network 10.0.0.0
 no auto-summary
```

```
R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router eigrp PE_CE
 !
 address-family ipv4 unicast vrf VPN_A autonomous-system 1
  !
  topology base
   redistribute bgp 100
  exit-af-topology
  network 10.0.0.0
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
!
address-family vpnv4
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 redistribute eigrp 1
exit-address-family
!

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
```

```
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
 !
!
vrf VPN_A
 rd 100:1
 address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
router eigrp PE_CE
 vrf VPN_A
  address-family ipv4
   autonomous-system 1
   redistribute bgp 100
   interface GigabitEthernet0/0/0/0.1920
   !
  !
 !
!
end

XR2:
router eigrp 1
  address-family ipv4
   no auto-summary
   interface Loopback0
   !
   interface GigabitEthernet0/0/0/0.1920
  !
 !
```

```
!
```

Verification

Like RIP, the VRF aware EIGRP process uses one global process, with sub-processes for each VRF table. In this example, since EIGRP is not used for routing in the global table, an arbitrary global EIGRP AS number of PE_CE is used. The only AS number that matters in this example is the one assigned to the VRF VPN_A address family, as this is the one that must match on the PE to CE link.

Similar to the verification of a global EIGRP process, the first step in making sure that this configuration is functional is to verify that the EIGRP adjacencies have occurred. In this case this would be on the PE-CE links.

```
R1#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   10.1.2.2                Gi1.12
                  14 04:48:00    1   100  0  5
R2#show eigrp address-family ipv4 vrf VPN_A neighbors

EIGRP-IPv4 VR(PE_CE) Address-Family Neighbors for AS(1)
           VRF(VPN_A)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   10.1.2.1                Gi1.12
                  13 04:48:34    2   100  0  4
RP/0/0/CPU0:XR1#show eigrp vrf VPN_A ipv4 neighbors

Sun May  3 22:37:47.444 UTC

IPv4-EIGRP VR(PE_CE) Neighbors for AS(1) VRF VPN_A

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.19.20.20             Gi0/0/0/0.1920
    13 04:42:03   23   200  0  3
RP/0/3/CPU0:XR2#show eigrp ipv4 neighbors

Sun May  3 22:38:19.142 UTC

IPv4-EIGRP Neighbors for AS(1) VRF default

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.19.20.19             Gi0/0/0/0.1920
    11 04:42:35   24   200  0  3
```

Redistribution of VPNv4 BGP to EIGRP and vice versa does not require a metric to be set, because the individual vectors of the EIGRP composite metric are encoded in the VPNv4 BGP update as extended communities. This can be seen on the PE routers as follows.

```
R2#show ip eigrp vrf VPN_A topology
EIGRP-IPv4 VR(PE_CE) Topology Table for AS(1)/ID(10.1.2.2)
           Topology(base) TID(0) VRF(VPN_A)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.19.20.0/24, 1 successors, FD is 1310720
        via VPNv4 Sourced (1310720/0)
P 20.20.20.20/32, 1 successors, FD is 1966080
        via VPNv4 Sourced (1966080/0)
P 10.1.2.0/24, 1 successors, FD is 1310720
        via Connected, GigabitEthernet1.12
P 1.1.1.1/32, 1 successors, FD is 328990720     via 10.1.2.1 (328990720/327761920), GigabitEthernet1.12
```

The EIGRP topology consists of four prefixes, two from the R1 & R2 side and two from the XR1 & XR2 side. The details of one of these prefixes is verified as follows.

```
R2#show eigrp address-family ipv4 vrf VPN_A topology 1.1.1.1/32
EIGRP-IPv4 VR(PE_CE) Topology Entry for AS(1)/ID(10.1.2.2)
           Topology(base) TID(0) VRF(VPN_A)
EIGRP-IPv4(1): Topology base(0) entry for 1.1.1.1/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 328990720, RIB is 2570240
  Descriptor Blocks:
  10.1.2.1 (GigabitEthernet1.12), from 10.1.2.1, Send flag is 0x0
      Composite metric is (328990720/327761920), route is Internal Vector metric:
Minimum bandwidth is 1000000 Kbit
Total delay is 5010000000 picoseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500

        Hop count is 1
        Originating router is 1.1.1.1
```

The individual vector attributes are then encoded as BGP extended communities in the VPNv4 prefix.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
BGP routing table entry for 100:1:1.1.1.1/32, version 44
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
      Origin incomplete, metric 2570240, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:100:1
```

```
Cost:pre-bestpath:128:2570240 (default-2144913407) 0x8800:32768:0
  0x8801:1:128256 0x8802:65281:2560 0x8803:65281:1500 0x8806:0:16843009

      mpls labels in/out 17/nolabel
  rx pathid: 0, tx pathid: 0x0
```

The following table describes what the individual values within the extended communities represent:

Attributes	Usage	Values
Type 0x8800	EIGRP General Route Information	Route Flag and Tag
Type 0x8801	EIGRP Route Metric Information and Autonomous System	Autonomous System and Delay
Type 0x8802	EIGRP Route Metric Information	Reliability, Next Hop, and Bandwidth
Type 0x8803	EIGRP Route Metric Information	Reserve, Load and MTU
Type 0x8804	EIGRP External Route Information	Remote Autonomous System and Remote ID
Type 0x8805	EIGRP External Route Information	Remote Protocol and Remote Metric
Type 0x8806	EIGRP Vector Metric Information	Vector Metric, Reserved, and Router-ID

This encoding is maintained as the routes are advertised to the remote PE routers.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32
```

```
Sun May  3 22:53:23.890 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 49          49
Last Modified: May  3 17:47:47.451 for 05:05:36
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
      Received Label 17
      Origin incomplete, metric 2570240, localpref 100, valid, internal, best, group-best, import-candidate, importe
      Received Path ID 0, Local Path ID 1, version 49
Extended community: COST:128:128:2570240 EIGRP route-info:0x8000:0 EIGRP AD:1:128256 EIGRP RHB:255:1:2560 EIGRP LM:0
      Source VRF: VPN_A, Source Route Distinguisher: 100:1
```

These individual vector attributes are then copied back into the EIGRP topology when BGP is redistributed back into EIGRP. This is the reason the metric does not need to be manually set, and why the routes appear as Internal EIGRP even though they went through redistribution.

```
RP/0/0/CPU0:XR2#show route ipv4 eigrp
Sun May  3 23:05:50.209 UTC

D    1.1.1.1/32 [90/2575360] via 10.19.20.19, 05:09:47, GigabitEthernet0/0/0/0.1920
D    10.1.2.0/24 [90/15360] via 10.19.20.19, 05:09:47, GigabitEthernet0/0/0/0.1920

RP/0/3/CPU0:XR2#show eigrp ipv4 topology 1.1.1.1/32
Sun May  3 23:06:15.577 UTC

IPv4-EIGRP AS(1): Topology entry for 1.1.1.1/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 329646080, RIB is 2575360
  Routing Descriptor Blocks:
  10.19.20.19 (GigabitEthernet0/0/0/0.1920), from 10.19.20.19, Send flag is 0x0
      Composite metric is (329646080/328990720), Route is Internal Vector metric:
Minimum bandwidth is 1000000 Kbit
Total delay is 5020000000 picoseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 2
```

```
    Originating router is 19.19.19.19
```

Notice that the MPLS network is transparent to the CE devices. R2 sees 1.1.1.1/32 with a hop count of 1, and XR2 sees it with a hop count of 2. Additionally, the delay increased from 5010000000 to 5020000000 picoseconds - indicative of the update traversing through a single GigE link.

The final result is that both customer sites have full reachability to each other.

```
R1#ping 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/12/16 ms

RP/0/0/CPU0:XR2#ping 1.1.1.1 source 20.20.20.20
Sun May  3 23:09:40.063 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with OSPF

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2 and LDP**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
    - VRF Name: VPN_A
    - Route Distinguisher: 100:1
    - Route Target Import: 100:1
    - Route Target Export: 100:1
    - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure OSPF routing for the VRF as follows:
    - Use Process-ID 100.
    - Enable OSPF Area 0 between R1 & R2.
    - Enable OSPF Area 0 between XR1 & XR2.
    - Advertise the Loopback0 networks of R1 & XR2 into OSPF Area 0.
- Configure BGP on R2 and XR1 as follows:
    - Use BGP AS 100.
    - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
    - Use their Loopback0 interfaces as the source of the BGP session.
- Redistribute between BGP and OSPF.
- Once complete R1 and XR2 should have reachability to each other's Loopback0 interfaces and PE-CE links.

Configuration

```
R1:
router ospf 100
 network 0.0.0.0 255.255.255.255 area 0

R2:
```

```
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router ospf 100 vrf VPN_A
 network 0.0.0.0 255.255.255.255 area 0
 redistribute bgp 100 subnets
!
router bgp 100
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute ospf 100
 exit-address-family

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
```

```
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
 !
!
vrf VPN_A
 rd 100:1
 address-family ipv4 unicast
   redistribute ospf 100
  !
 !
!
router ospf 100
 vrf VPN_A
  redistribute bgp 100
  area 0
   interface GigabitEthernet0/0/0/0.1920
  !
 !
!
end

XR2:
router ospf 100
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0.1920
  !
 !
!
```

Verification

In regular IOS OSPF requires one unique process for the global table and each subsequent VRF table. However in IOS XR multiple VRF tables can share the same

OSPF process, similar to how RIP or EIGRP works in IOS XR.

The first step in verifying that this design works is to ensure that the OSPF adjacencies are functional. Since we now have both a global OSPF process for the core of the MPLS network and an OSPF process for VRF VPN_A, R2 should reference the unique OSPF Process-ID during verification to clarify which attributes apply to the global table and which apply to the VRF table, as seen below.

OSPF Process-ID 1 is used for the global table, while 100 is used for VRF VPN_A. If we were to look at the **show ip ospf neighbor** command without referencing a PID, it is very difficult to determine which options apply to the global table vs. the VRF. Hence the verification should include the PID.

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         00:00:39    20.2.4.4        GigabitEthernet1.24
3.3.3.3           1   FULL/DR         00:00:34    20.2.3.3        GigabitEthernet1.23
1.1.1.1           1   FULL/BDR        00:00:30    10.1.2.1        GigabitEthernet1.12
R2#show ip ospf 1 neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         00:00:39    20.2.4.4        GigabitEthernet1.24
3.3.3.3           1   FULL/DR         00:00:34    20.2.3.3        GigabitEthernet1.23

R2#show ip ospf 100 neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:34    10.1.2.1        GigabitEthernet1.12
```

In IOS XR this verification is clearer as the VRF’s name is referenced in the show commands.

```
RP/0/0/CPU0:XR1#show ospf vrf VPN_A neighbor

Sun May  3 23:28:38.935 UTC

* Indicates MADJ interface

Neighbors for OSPF 100, VRF VPN_A

Neighbor ID     Pri   State           Dead Time   Address         Interface
20.20.20.20     1     FULL/BDR        00:00:34    10.19.20.20     GigabitEthernet0/0/0/0.1920

    Neighbor is up for 00:06:26

Total neighbor count: 1
```

Since the PE routers participate in the same area as the CE router's advertisements, the PEs should be learning their attached CE's routes as OSPF Intra-Area prefixes.

```
R2#show ip route vrf VPN_A ospf



Routing Table: VPN_A
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/2] via 10.1.2.1, 00:10:01, GigabitEthernet1.12
RP/0/0/CPU0:XR1#show route vrf VPN_A ospf

Sun May  3 23:30:08.239 UTC

O    20.20.20.20/32 [110/2] via 10.19.20.20, 00:07:25, GigabitEthernet0/0/0/0.1920
```

OSPF is then redistributed from the PE’s VRF aware OSPF process into VPNv4 BGP.

```
R2#show bgp vpnv4 unicast all

 BGP table version is 66, local router ID is 2.2.2.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
 RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight Path
 Route Distinguisher: 100:1 (default for vrf VPN_A)
 *>  1.1.1.1/32       10.1.2.1                 2         32768 ?
 *>  10.1.2.0/24      0.0.0.0                  0         32768 ?

  *>i 10.19.20.0/24    19.19.19.19              0    100      0 ?
  *>i 20.20.20.20/32   19.19.19.19              2    100      0 ?
 RP/0/0/CPU0:XR1#show bgp vpnv4 unicast
```

Sun May 3 23:31:11.284 UTC BGP router identifier 19.19.19.19, local AS number 100 BGP generic scan interval 60 secs BGP table state: Active Table ID: 0x0 RD version: 0 BGP main routing table version 66 BGP scan interval 60 secs

```
 Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
 Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
 Route Distinguisher: 100:1 (default for vrf VPN_A)
 *>i1.1.1.1/32         2.2.2.2                  2    100      0 ?
 *>i10.1.2.0/24        2.2.2.2                  0    100      0 ?
 *> 10.19.20.0/24      0.0.0.0                  0         32768 ?
 *> 20.20.20.20/32     10.19.20.20              2         32768 ?



 Processed 4 prefixes, 4 paths
```

Like EIGRP, certain attributes of the routes are maintained and encoded as BGP extended communities. This can be seen in the details of the VPNv4 tables of the PE routers below. Note that in addition to the next-hop and the VPN label values, which are ultimately used to build the label stack in the data plane, OSPF specific attributes such as the OSPF Domain-ID, Route Type, and Router-ID are encoded.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32

BGP routing table entry for 100:1:1.1.1.1/32, version 62
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, sourced, best
Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
 OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.1.2.2:0
mpls labels in/out 37/nolabel
      rx pathid: 0, tx pathid: 0x0
R2#show bgp vpnv4 unicast all 20.20.20.20/32
BGP routing table entry for 100:1:20.20.20.20/32, version 7
Paths: (1 available, best #1, table VPN_A)
    Not advertised to any peer
    Local 19.19.19.19
 (metric 4) from 19.19.19.19 (19.19.19.19)
            Origin incomplete, metric 2, localpref 100, valid, internal, best
Extended Community: RT:100:1 OSPF RT:0.0.0.0:2:0
OSPF ROUTER ID:19.19.19.19:0
mpls labels in/out nolabel/16013
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32
Sun May  3 23:33:27.475 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 62          62
Last Modified: May  3 23:19:23.451 for 00:14:04
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local 2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2)
      Received Label 37
      Origin incomplete, metric 2, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 62
Extended community: OSPF domain-id:0x5:0x000000640200 OSPF route-type:0:2:0x0 OSPF router-id:10.1.2.2 RT:100:1

      Source VRF: VPN_A, Source Route Distinguisher: 100:1
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 20.20.20.20/32
Sun May  3 23:34:04.582 UTC
BGP routing table entry for 20.20.20.20/32, Route Distinguisher: 100:1
```

```
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 66          66
    Local Label: 16001
Last Modified: May  3 23:22:43.451 for 00:11:21
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    2.2.2.2
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    2.2.2.2
  Local 10.19.20.20
 from 0.0.0.0 (19.19.19.19)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, redistributed, best, group-best, import-candi
      Received Path ID 0, Local Path ID 1, version 66
 Extended community: OSPF route-type:0:1:0x0 OSPF router-id:19.19.19.19 RT:100:1
```

The most notable of these encoded attributes is the OSPF Domain-ID, which is used to determine if the MPLS VPNv4 BGP network should be considered as the OSPF “super backbone”, which is treated as one hierarchy above OSPF area 0. In the case that the OSPF Domain-ID of a received VPNv4 route matches the OSPF Domain-ID of the local VRF aware OSPF process, then the OSPF Route-Type is examined to determine how the OSPF LSA should be encoded in the database when BGP to OSPF redistribution occurs. In other words, the OSPF Domain-ID makes the determination if the PE router should be treated as an OSPF ABR, which originates Type-3 Network Summary LSAs (Inter Area Routes) or an OSPF ASBR, which would originate Type-5 External LSAs for the redistributed routes, regardless if the route-type attribute is set to 1 or 2 (for internal routes).

Note that in the case of regular IOS the OSPF Domain-ID is automatically encoded from the OSPF Process-ID, but in IOS XR it is not - following RFC 4577 more closely than IOS. RFC 4577 states that each OSPF instance MUST be associated with one or more Domain IDs - which MUST be configurable - and the default value (if none is configured) SHOULD be NULL. As can be observed, IOS has automatically configured a Domain-ID value which is not NULL. However, IOS-XR has defaulted to NULL. Additionally, the RFC states that when the Domain-ID value is set to NULL, it is not necesary to include the value in the BGP update. Once again, IOS-XR follows the RFC closely and does not attach the Domain-ID community to the BGP update as the value is NULL.

R2 is currently setting the Domain-ID as follows:

```
DOMAIN ID:0x0005:0x000000640200
```

The first 4 bytes, 0x00000064, can be decoded into decimal to derive the OSPF process ID (100).

The OSPF Route Type Extended Communities Attribute is encoded as: 'Type-Field - Area Number - Route-Type - Options'. The table below describes the possible values found in the route-type portion of the extended community value.

Encoding	Route Type
1 or 2	Intra-Area routes
3	Inter-Area routes
5	External routes
7	NSSA routes

More details can be found in RFC-4577

This means that in the current network setup the OSPF Domain-IDs do not match (R2 set it as DOMAIN ID:0x0005:0x000000640200, and XR1 as NULL), even though the OSPF Process-IDs are the same. The final result of this is that the CE routers see each other's routes as Type-5 External LSAs, not Inter-Area routes.

```
R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2     10.19.20.0/24 [110/1] via 10.1.2.2, 00:28:27, GigabitEthernet1.12
     20.0.0.0/32 is subnetted, 1 subnets
O E2     20.20.20.20 [110/2] via 10.1.2.2, 00:27:13, GigabitEthernet1.12

RP/0/0/CPU0:XR2#show route ipv4 ospf

Mon May  4 00:07:10.387 UTC

O E2 1.1.1.1/32 [110/2] via 10.19.20.19, 00:44:27, GigabitEthernet0/0/0/0.1920
O E2 10.1.2.0/24 [110/1] via 10.19.20.19, 00:44:27, GigabitEthernet0/0/0/0.1920
```

In the OSPF database the CE routers view the PE routers as ASBRs.

```
R1#show ip ospf database

           OSPF Router with ID (1.1.1.1) (Process ID 100)

               Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         930         0x80000003 0x00B343 2
10.1.2.2        10.1.2.2        906         0x80000003 0x00E011 1

               Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        10.1.2.2        906         0x80000002 0x000FF8

               Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.19.20.0      10.1.2.2        906         0x80000002 0x002A92 3489661028
20.20.20.20     10.1.2.2        645         0x80000002 0x00DCBF 3489661028
RP/0/0/CPU0:XR2#show ospf database
Mon May  4 00:08:07.463 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
19.19.19.19     19.19.19.19     777         0x80000003 0x00fc10 1
20.20.20.20     20.20.20.20     714         0x80000003 0x005451 2
```

```
                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.19.20.19     19.19.19.19     777         0x80000002 0x00d239

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
1.1.1.1         19.19.19.19     777         0x80000002 0x008a21 3489661028
10.1.2.0        19.19.19.19     777         0x80000002 0x000a99 3489661028
```

Note that this does not affect connectivity, as the customer sites still have reachability to each other as seen below, it simply affects how the OSPF path selection occurs.

```
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
R1#ping 10.19.20.20


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.19.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/12 ms
```

If the OSPF Domain-IDs would match, the PE routers would appear as ABRs instead of ASBRs, and the CEs would see each other's routes as Type-3 Network Summary LSAs (Inter-Area routes). This can be accomplished in this case by manually defining the Domain-ID on IOS XR to match what the regular IOS process is encoding, as seen below. Note that the 0x00000064 portion of the Domain-ID is the OSPF Process-ID 100 represented in hexadecimal.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32
Mon May  4 00:34:18.435 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
 Process           bRIB/RIB  SendTblVer
```

```
  Speaker                 62          62
 Last Modified: May  3 23:19:23.451 for 01:14:55
 Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
      Received Label 37
      Origin incomplete, metric 2, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 62     Extended community:
 OSPF domain-id:0x5:0x000000640200
  OSPF route-type:0:2:0x0 OSPF router-id:10.1.2.2 RT:100:1
      Source VRF: VPN_A, Source Route Distinguisher: 100:1



 RP/0/0/CPU0:XR1#
 RP/0/0/CPU0:XR1#conf t
 Mon May  4 00:35:41.039 UTC
 RP/0/0/CPU0:XR1(config)#router ospf 100
 RP/0/0/CPU0:XR1(config-ospf)#vrf VPN_A
RP/0/0/CPU0:XR1(config-ospf-vrf)#domain-id type 0005 value 000000640200

 RP/0/0/CPU0:XR1(config-ospf-vrf)#commit
 Mon May  4 00:36:00.778 UTC
 RP/0/0/CPU0:May  4 00:36:01.088 : config[65813]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
 RP/0/0/CPU0:XR1(config-ospf-vrf)#end
 RP/0/0/CPU0:May  4 00:36:06.138 : config[65813]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin
 RP/0/0/CPU0:XR1#
 RP/0/0/CPU0:XR1#
```

Now all routes that were redistributed from OSPF to VPNv4 BGP on either R2 or XR1 have the same OSPF Domain-ID, as seen below.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32 | include DOMAIN
    Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
 R2#show bgp vpnv4 unicast all 20.20.20.20/32 | include DOMAIN
    Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
 RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32 | include domain
```

Mon May 4 00:37:50.130 UTC Extended community: **OSPF domain-id:0x5:0x000000640200** OSPF route-type:0:2:0x0 OSPF router-id:10.1.2.2 RT:100:1

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 20.20.20.20/32 | include domain
Mon May  4 00:38:17.709 UTC     Extended community: OSPF domain-id:0x5:0x000000640200
 OSPF route-type:0:1:0x0 OSPF router-id:19.19.19.19 RT:100:1
```

The final result of this is that the CE routers now see the PE routers as ABRs for these prefixes instead of ASBRs.

```
R1#show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1032        0x80000004 0x00B144 2
10.1.2.2        10.1.2.2        986         0x80000004 0x00DE12 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        10.1.2.2        986         0x80000003 0x000DF9

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.19.20.0      10.1.2.2        399         0x80000001 0x004B30
20.20.20.20     10.1.2.2        399         0x80000001 0x00FD5D
R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O IA     10.19.20.0/24 [110/2] via 10.1.2.2, 00:07:33, GigabitEthernet1.12
```

```
      20.0.0.0/32 is subnetted, 1 subnets
O IA     20.20.20.20 [110/3] via 10.1.2.2, 00:07:33, GigabitEthernet1.12

RP/0/3/CPU0:XR2#show ospf database
Mon May  4 00:46:27.855 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
19.19.19.19     19.19.19.19     1073        0x80000004 0x00fa11 1
20.20.20.20     20.20.20.20     1001        0x80000004 0x005252 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.19.20.19     19.19.19.19     1073        0x80000003 0x00d03a

            Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
1.1.1.1         19.19.19.19     627         0x80000001 0x00abbe
10.1.2.0        19.19.19.19     627         0x80000001 0x002b37

RP/0/3/CPU0:XR2#show route ipv4 ospf
Mon May  4 00:46:55.083 UTC
O IA 1.1.1.1/32
 [110/3] via 10.19.20.19, 00:10:53, GigabitEthernet0/0/0/0.1920O IA 10.1.2.0/24
 [110/2] via 10.19.20.19, 00:10:53, GigabitEthernet0/0/0/0.1920
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with BGP

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **OSPFv2 and LDP**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **IPv4 Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
- Configure BGP on R1 and XR2 as follows:
  - Use BGP AS 1.
  - R1 and R2 should peer EBGP.
  - XR1 and XR2 should peer EBGP.
  - Advertise the Loopback0 interfaces of R1 and XR2 into BGP.
- Once complete R1 and XR2 should have reachability to each other's Loopback0 interfaces when sourcing traffic from their Loopback0 networks.

Configuration

```
R1:
router bgp 1
 network 1.1.1.1 mask 255.255.255.255
 neighbor 10.1.2.2 remote-as 100

R2:
```

```
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEtherne1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 neighbor 10.1.2.1 remote-as 1
 neighbor 10.1.2.1 as-override
exit-address-family
!

XR1:
 vrf VPN_A
  address-family ipv4 unicast
   import route-target 100:1
  !
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
route-policy PASS
 pass
end-policy
!
```

```
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
vrf VPN_A
 rd 100:1
 address-family ipv4 unicast
 !
neighbor 10.19.20.20
 remote-as 1
 address-family ipv4 unicast
  route-policy PASS in
  route-policy PASS out
  as-override

XR2:
route-policy PASS
 pass
end-policy
!
router bgp 1
 address-family ipv4 unicast
  network 20.20.20.20/32
 !
 neighbor 10.19.20.19
  remote-as 100
  address-family ipv4 unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
!
```

Verification

BGP as the PE-CE routing protocol uses one global BGP process, with the VRF specific peers defined under the **address-family ipv4 vrf** in regular IOS, and under the vrf BGP sub mode in IOS XR. Two things should be noted about this specific configuration. The first is that since the IOS XR routers are EBGP neighbors with each other, a Routing Policy is required in order to define which prefixes are allowed to be advertised and received. This is a fairly obvious requirement of IOS XR's configuration, because if the peering is committed without the RPL policy applied, a log message appears saying that the configuration is not functional without RPL. This can be seen as follows.

```
RP/0/0/CPU0:XR2#show run router bgp
Tue May  5 21:45:54.230 UTC
router bgp 1
 address-family ipv4 unicast
  network 20.20.20.20/32
 !
 neighbor 10.19.20.19
  remote-as 100
  address-family ipv4 unicast  route-policy PASS in
 route-policy PASS out
RP/0/0/CPU0:XR2(config)#no router bgp 1
RP/0/0/CPU0:XR2(config)#commit
Tue May  5 21:45:56.230 UTC
RP/0/0/CPU0:May  5 21:45:56.360 : bpm[1062]: %ROUTING-BGP-5-ASYNC_IPC_STATUS : bpm-default:(A)inst-id 0, Connection
RP/0/0/CPU0:May  5 21:45:56.610 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR2(config)#    router bgp 1
RP/0/0/CPU0:XR2(config-bgp)#     address-family ipv4 unicast
RP/0/0/CPU0:XR2(config-bgp-af)#      network 20.20.20.20/32
RP/0/0/CPU0:XR2(config-bgp-af)#     !
RP/0/0/CPU0:XR2(config-bgp-af)#     neighbor 10.19.20.19
RP/0/0/CPU0:XR2(config-bgp-nbr)#      remote-as 100
RP/0/0/CPU0:XR2(config-bgp-nbr)#      address-family ipv4 unicast
RP/0/0/CPU0:XR2(config-bgp-nbr-af)#commit
Tue May  5 21:46:03.909 UTC
RP/0/0/CPU0:May  5 21:46:04.399 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR2(config-bgp-nbr-af)#RP/0/0/CPU0:May  5 21:46:04.759 : bpm[1062]: %ROUTING-BGP-5-ASYNC_IPC_STATUS : bp
RP/0/0/CPU0:May  5 21:46:04.979 : bgp[1047]: %ROUTING-BGP-5-ASYNC_IPC_STATUS : default, process instance 1:(A)inst-i
RP/0/0/CPU0:May  5 21:46:06.799 : bgp[1047]: %ROUTING-BGP-5-ASYNC_IPC_STATUS : default:(A)inst-id 0, Initial Config
RP/0/0/CPU0:May  5 21:46:10.669 : bgp[1047]:
%ROUTING-BGP-5-ADJCHANGE : neighbor 10.19.20.19 Up (VRF: default) (AS: 100)
 RP/0/0/CPU0:May  5 21:46:10.669 : bgp[1047]: %ROUTING-BGP-6-NBR_NOPOLICY :
No inbound IPv4 Unicast policy is configured for eBGP neighbor 10.19.20.19. No IPv4 Unicast prefixes will be accepte
 RP/0/0/CPU0:May  5 21:46:10.669 : bgp[1047]: %ROUTING-BGP-6-NBR_NOPOLICY :
No outbound IPv4 Unicast policy is configured for eBGP neighbor 10.19.20.19. No IPv4 Unicast prefixes will be sent t
```

If you were to miss this log message, for example if logging is disabled, you would also see it when you verify the BGP peering status with the neighbor as follows.

```
RP/0/3/CPU0:XR2#show bgp ipv4 unicast summary
Tue May  5 22:00:20.600 UTC
BGP router identifier 20.20.20.20, local AS number 1
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000   RD version: 3
BGP main routing table version 3
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.



Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker               3          3          3          3           3           3

 Some configured eBGP neighbors (under default or non-default vrfs)
do not have both inbound and outbound policies configured for IPv4 Unicast
address family. These neighbors will default to sending and/or
receiving no routes and are marked with '!' in the output below.
Use the 'show bgp neighbor <nbr_address>' command for details.

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.19.20.19       0   100      18      17        3    0    0 00:14:10          0 !
```

The second portion of this config that should be noted is the **as-override** keyword used on the PE’s peering sessions towards the CEs. In cases where multiple customer sites are using the same BGP AS number, the default BGP filtering rule to not allow prefixes with the router’s own AS number in the AS-Path will prevent prefixes from being exchanged between sites. The **as- override** feature prevents prefixes from being filtered on the CE by editing the AS-Path information and replacing all occurrences of the customer's ASN with the PE's ASN, as the route is advertised towards the CE. Without AS Override, prefixes are dropped as they are received on the CE, as seen in the following output.

R2 removes the AS Override feature configured to its CE router, R1.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 100
R2(config-router)#address-family ipv4 vrf VPN_A
R2(config-router-af)#no neighbor 10.1.2.1 as-override
R2(config-router-af)#end
```

```
R2#clear bgp vrf VPN_A ipv4 unicast *
R2#
```

When new UPDATE messages are received in on R1 from R2 they contain the AS "1" in the path, which means that R1 cannot accept them.

```
R1#debug ip bgp updates

BGP updates debugging is on for address family: IPv4 Unicast
R1#
BGP(0): 10.1.2.2 rcv UPDATE about 1.1.1.1/32 -- withdrawn
BGP(0): 10.1.2.2 rcv UPDATE w/ attr: nexthop 10.1.2.2, origin i, originator 0.0.0.0, merged path 100 1, AS_PATH , co
BGPSSA ssacount is 0
BGP(0): 10.1.2.2 rcv UPDATE about 20.20.20.20/32 -- DENIED due to: AS-PATH contains our own AS;
BGP(0): no valid path for 20.20.20.20/32
BGP: topo global:IPv4 Unicast:base Remove_fwdroute for 20.20.20.20/32
R1#
%BGP-3-NOTIFICATION: received from neighbor 10.1.2.2 6/4 (Administrative Reset) 0 bytes
%BGP-5-NBR_RESET: Neighbor 10.1.2.2 reset (BGP Notification received)
%BGP-5-ADJCHANGE: neighbor 10.1.2.2 Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor 10.1.2.2 IPv4 Unicast topology base removed from session  BGP Notification receiv
%BGP-5-ADJCHANGE: neighbor 10.1.2.2 Up
R1#
BGP(0): (base) 10.1.2.2 send UPDATE (format) 1.1.1.1/32, next 10.1.2.1, metric 0, path Local
BGP(0): 10.1.2.2 rcv UPDATE w/ attr: nexthop 10.1.2.2, origin i, originator 0.0.0.0,
merged path 100 1, AS_PATH
 , community , extended community , SSA attribute
BGPSSA ssacount is 0
BGP(0): 10.1.2.2 rcv UPDATE about 20.20.20.20/32 -- DENIED due to: AS-PATH contains our own AS;
```

Even though R2 is still advertising 20.20.20.20/32 to R1, R1 cannot install it.

```
R2#show bgp vpnv4 unicast vrf VPN_A neighbors 10.1.2.1 advertised-routes
BGP table version is 10, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
*>i 20.20.20.20/32   19.19.19.19              0    100      0 1 i
```

```
Total number of prefixes 1
R1#show ip bgp

BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
             r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
             x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop            Metric LocPrf Weight Path
*>  1.1.1.1/32       0.0.0.0                  0         32768 i
```

Another alternative solution to this problem would be to configure the CE routers to allow prefixes that have their own AS in the path, such as the following.

```
R1#debug ip bgp update
BGP updates debugging is on for address family: IPv4 Unicast
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 1R1(config-router)#neighbor 10.1.2.2 allowas-in 1
R1(config-router)#end
BGP: nbr_topo global 10.1.2.2 IPv4 Unicast:base (0x7FF7B7E9CCA0:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 10.1.2.2 IPv4 Unicast:base (0x7FF7B7E9CCA0:1) refresh_epoch is 2 BGP(0): 10.1.2.2
 rcvd UPDATE w/ attr: nexthop 10.1.2.2, origin i, merged path 100 1, AS_PATH
BGP(0): 10.1.2.2 rcvd 20.20.20.20/32
BGP: nbr_topo global 10.1.2.2 IPv4 Unicast:base (0x7FF7B7E9CCA0:1) rcvd Refresh End-of-RIB BGP(0):
 Revise route installing 1 of 1 routes for 20.20.20.20/32 -> 10.1.2.2(global) to main IP table

R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Even though the prefix 20.20.20.20/32 contains R1's own AS number in the path, the allowas- in command permits an exception for this.

```
R1#show ip bgp
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
```

```
*>  1.1.1.1/32       0.0.0.0                  0         32768 i
*>  20.20.20.20/32   10.1.2.2                                0 100 1 i

R1#show bgp ipv4 unicast 20.20.20.20/32

BGP routing table entry for 20.20.20.20/32, version 8
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 2
  100 1
    10.1.2.2 from 10.1.2.2 (2.2.2.2)
      Origin IGP, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0
```

The final result should be that R1 and XR2 have reachability to each other's Loopbacks, but only when sourcing traffic from the Loopbacks, as the transit links from the PE-CEs have not been advertised.

```
R1#ping 20.20.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
.....Success rate is 0 percent
 (0/5)
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!Success rate is 100 percent (5/5)
, round-trip min/avg/max = 12/12/14 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN with Policy Routing

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Multisite L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Multisite L3VPN Diagram Diagram** in order to complete this task.

- Configure three new Loopback interfaces on R1 with addresses 1.1.1.7/32, 1.1.1.8/32, and 1.1.1.20/32.
- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - On XR1 assign the VRF to the link connecting to XR2.
- Configure a VRF on R2 and R4 as follows:
  - VRF Name: VPN_B
  - Route Distinguisher: 100:2
  - Route Target Import: 100:2
  - Route Target Export: 100:2
  - On R4 assign the VRF to the link connecting to R7.
- Configure a VRF on R2 and R5 as follows:
  - VRF Name: VPN_C
  - Route Distinguisher: 100:3
  - Route Target Import: 100:3
  - Route Target Export: 100:3
  - On R5 assign the VRF to the link connecting to R8.
- Configure Customer Edge routing as follows:
  - R1 should have a default route pointing towards R2.
  - R7 should have a default route pointing towards R4.
  - R8 should have a default route pointing towards R5.

    - XR2 should have a default route pointing towards XR1.
- Configure Provider Edge routing as follows:
    - R2 should have the following static routes towards R1:
        - 1.1.1.20/32 via 10.1.2.1 in VRF VPN_A
        - 1.1.1.7/32 via 10.1.2.1 in VRF VPN_B
        - 1.1.1.8/32 via 10.1.2.1 in VRF VPN_C
    - R4 should have a static route to 7.7.7.7/32 via R7.
    - R5 should have a static route to 8.8.8.8/32 via R8.
    - XR1 should have a static route to 20.20.20.20/32 via XR2.
- Configure BGP on R2, R4, R5, and XR1 as follows:
    - Use BGP AS 100.
    - R2 should peer with R4, R5, and XR1 via iBGP for the VPNv4 Address Family.
    - Use their Loopback0 interfaces as the source of the BGP session.
    - Advertise the static routes VRF routes on R2, R4, R5, and XR1 into VPNv4 BGP.
- Configure MPLS VPN VRF Selection using Policy Based Routing on R2 as follows:
    - Traffic coming from R1’s network 1.1.1.20/32 should belong to VRF VPN_A.
    - Traffic coming from R1’s network 1.1.1.7/32 should belong to VRF VPN_B.
    - Traffic coming from R1’s network 1.1.1.8/32 should belong to VRF VPN_C.
- Once complete, only the following reachability should be achieved:
    - R1 should be able to reach R7’s 7.7.7.7/32 when sourcing traffic from 1.1.1.7/32
    - R1 should be able to reach R8’s 8.8.8.8/32 when sourcing traffic from 1.1.1.8/32
    - R1 should be able to reach XR2’s 20.20.20.20/32 when sourcing traffic from 1.1.1.20/32

Configuration

```
R1:
interface Loopback1117
 ip address 1.1.1.7 255.255.255.255
!
interface Loopback1118
 ip address 1.1.1.8 255.255.255.255
!
interface Loopback11120
 ip address 1.1.1.20 255.255.255.255
!
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.2

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
vrf definition VPN_B
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
vrf definition VPN_C
 rd 100:3
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family

!
router bgp 100
 no bgp default ipv4-unicast
 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 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 network 1.1.1.20 mask 255.255.255.255
```

```
exit-address-family
!
address-family ipv4 vrf VPN_B
 network 1.1.1.7 mask 255.255.255.255
exit-address-family
!
address-family ipv4 vrf VPN_C
 network 1.1.1.8 mask 255.255.255.255
exit-address-family
!
ip access-list standard VPN_A_SOURCES
 permit host 1.1.1.20
ip access-list standard VPN_B_SOURCES
 permit host 1.1.1.7
ip access-list standard VPN_C_SOURCES
 permit host 1.1.1.8

route-map VRF_SELECTION_WITH_PBR permit 10
 match ip address VPN_A_SOURCES
 set vrf VPN_A
 !
route-map VRF_SELECTION_WITH_PBR permit 20
 match ip address VPN_B_SOURCES
set vrf VPN_B
!
route-map VRF_SELECTION_WITH_PBR permit 30
 match ip address VPN_C_SOURCES
 set vrf VPN_C
!
interface GigabitEthernet1.12
 ip policy route-map VRF_SELECTION_WITH_PBR
 ip vrf receive VPN_A
 ip vrf receive VPN_B
 ip vrf receive VPN_C
!
ip route vrf VPN_A 1.1.1.20 255.255.255.255 Gig1.12 10.1.2.1
ip route vrf VPN_B 1.1.1.7 255.255.255.255 Gig1.12 10.1.2.1
ip route vrf VPN_C 1.1.1.8 255.255.255.255 Gig1.12 10.1.2.1

R4:
vrf definition VPN_B
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 !
 address-family ipv4
```

```
 exit-address-family
!
interface GigabitEthernet1.47
 vrf forwarding VPN_B
 ip address 10.4.7.4 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_B
  network 7.7.7.7 mask 255.255.255.255
 exit-address-family
 !
!
ip route vrf VPN_B 7.7.7.7 255.255.255.255 10.4.7.7

R5:
vrf definition VPN_C
 rd 100:3
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
!
!
interface GigabitEthernet1.58
 vrf forwarding VPN_C
 ip address 10.5.8.5 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
exit-address-family
```

```
!
address-family ipv4 vrf VPN_C
 network 8.8.8.8 mask 255.255.255.255
exit-address-family
 !
!
ip route vrf VPN_C 8.8.8.8 255.255.255.255 10.5.8.8

R7:
ip route 0.0.0.0 0.0.0.0 10.4.7.4

R8:
ip route 0.0.0.0 0.0.0.0 10.5.8.5

XR1:
vrf VPN_A
  address-family ipv4 unicast
   import route-target 100:1
   !
   export route-target
    100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 no ipv4 address
 vrf VPN_A
 ipv4 address 10.19.20.19 255.255.255.0
!
router static
 vrf VPN_A
  address-family ipv4 unicast
   20.20.20.20/32 10.19.20.20
  !
 !
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
vrf VPN_A
```

```
 rd 100:1
 address-family ipv4 unicast
   network 20.20.20.20/32
  !
 !
!

XR2:
router static
  address-family ipv4 unicast
   0.0.0.0/0 GigabitEthernet0/0/0/0.1920 10.19.20.19
 !
!
```

Verification

VRF Selection Using Policy Based Routing feature allows an interface to have multiple VRF memberships assigned, and then have traffic placed into a specific VRF instance based on classification that occur through a route-map. In this example, the PE router R2 has three separate VRFs configured, VRFs VPN_A, VPN_B, and VPN_C. From the below output we can see that none of these VRFs are directly attached to the interface connecting to the CE.

```
R2#show vrf
Name                Default RD          Protocols Interfaces

VPN_A               100:1               ipv4
VPN_B               100:2               ipv4
VPN_C               100:3               ipv4
```

Instead, the route-map *VRF_SELECTION_WITH_PBR* is applied to the CE facing link, along with the **ip vrf receive** command, which instructs the router to consult the route-map for VRF assignment in the data plane.

```
R2#sh run int Gig1.12
Building configuration...

Current configuration : 206 bytes
!
interface FastEthernet1/0  ip vrf receive VPN_A
 ip vrf receive VPN_B
  ip vrf receive VPN_C
```

```
 ip address 10.1.2.2 255.255.255.0 ip policy route-map VRF_SELECTION_WITH_PBR

end
```

In this case the route-map has three selection criteria. If traffic matches the standard ACL *VPN_A_SOURCES*, it is placed into VRF VPN_A. Likewise the same occurs for matches against ACLs *VPN_B_SOURCES* and *VPN_C_SOURCES* for VRFs VPN_B and VPN_C respectively. This feature enhances the standard Policy Based Routing (PBR) feature set with a new action: 'set vrf'.

```
R2#show route-map
route-map VRF_SELECTION_WITH_PBR, permit, sequence 10 Match clauses:
ip address (access-lists): VPN_A_SOURCES
Set clauses:
vrf VPN_A

  Policy routing matches: 10 packets, 1140 bytes
route-map VRF_SELECTION_WITH_PBR, permit, sequence 20
  Match clauses:
   ip address (access-lists): VPN_B_SOURCES
  Set clauses:
   vrf VPN_B
  Policy routing matches: 15 packets, 1710 bytes
route-map VRF_SELECTION_WITH_PBR, permit, sequence 30
  Match clauses:
   ip address (access-lists): VPN_C_SOURCES
  Set clauses:
   vrf VPN_C
 Policy routing matches: 25 packets, 2850 bytes
```

Specifically these access-lists match traffic being sourced from networks 1.1.1.20/32, 1.1.1.7/32, and 1.1.1.8/32 respectively.

```
R2#show access-list
Standard IP access list VPN_A_SOURCES
 10 permit 1.1.1.20 (5 matches)

Standard IP access list VPN_B_SOURCES
    10 permit 1.1.1.7 (15 matches)
Standard IP access list VPN_C_SOURCES
    10 permit 1.1.1.8 (35 matches)
```

Since the policy-routing only applies to packets being received inbound on the interface, R2 still needs a reverse outbound route to tell it which routing table these sources exist in. This is accomplished with the following static routes.

```
R2#sh ip route vrf * | include VPN|^S_
Routing Table: VPN_A
S 1.1.1.20 [1/0] via 10.1.2.1, GigabitEthernet1.12
Routing Table: VPN_BS 1.1.1.7 [1/0] via 10.1.2.1, GigabitEthernet1.12
Routing Table: VPN_CS 1.1.1.8 [1/0] via 10.1.2.1, GigabitEthernet1.12
```

These static routes are then advertised into the separate VRF tables of the VPNv4 BGP topology.

```
R2#show bgp vpnv4 unicast all
BGP table version is 11, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop    Metric LocPrf   Weight Path  Route Distinguisher: 100:1 (default for
vrf VPN_A
)*> 1.1.1.20/32     10.1.2.1         0            32768  i
*>i20.20.20.20/32   19.19.19.19     0   100         0  iRoute Distinguisher: 100:2 (default for
vrf VPN_B
)*> 1.1.1.7/32      10.1.2.1         0            32768  i
*>i7.7.7.7/32       4.4.4.4         0   100         0  iRoute Distinguisher: 100:3 (default for
vrf VPN_C
)*> 1.1.1.8/32      10.1.2.1         0            32768  i

*>i8.8.8.8/32       5.5.5.5         0   100         0  i
```

The CSR1000v routers used for this lab do not support debugging of policy routing. To glean into the decision making process that is going on, a platform debug will need to be done.

```
R2#debug platform packet-trace enable
Please remember to turn on 'debug platform condition start' for packet-trace to work
R2#debug platform packet-trace packet 1024 fia-trace
R2#debug platform condition interface g1.12 ingress
R2#debug platform condition start

R1#ping 8.8.8.8 source 1.1.1.8 repeat 2
```

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.8 !!
Success rate is 100 percent (2/2), round-trip min/avg/max = 2/4/6 ms

R2#show platform packet-trace summary

Pkt   Input            Output           State  Reason 0      Gi1.12           Gi1.24           FWD
    1      Gi1.12           Gi1.24           FWD
```

This debug shows all of the decisions that are made internally by the router as the packet is processed.

```
R2#show platform packet-trace packet 1

Packet: 1           CBUG ID: 5
Summary Input       : GigabitEthernet1.12
Output      : GigabitEthernet1.24
State       : FWD

  Timestamp
    Start   : 1409294078686990 ns (05/05/2015 23:05:22.484691 UTC)
    Stop    : 1409294078702150 ns (05/05/2015 23:05:22.484706 UTC)
Path Trace
  Feature: IPV4 Source       : 1.1.1.8
Destination : 8.8.8.8
    Protocol    : 1 (ICMP)
  Feature: FIA_TRACE
    Entry      : 0x80880270 - DEBUG_COND_INPUT_PKT
    Lapsed time: 4560 ns
  Feature: FIA_TRACE
    Entry      : 0x8041cf00 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time: 2266 ns
  Feature: FIA_TRACE
    Entry      : 0x800e28a0 - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time: 1600 ns
  Feature: FIA_TRACE Entry      : 0x805ca780 - IPV4_INPUT_PBR
    Lapsed time: 34853 ns
  Feature: FIA_TRACE
    Entry      : 0x8041b080 - IPV4_OUTPUT_LOOKUP_PROCESS
    Lapsed time: 21173 ns
  Feature: FIA_TRACE
    Entry      : 0x8041f4b0 - IPV4_INPUT_IPOPTIONS_PROCESS
    Lapsed time: 2240 ns
```

```
    Feature: FIA_TRACE
      Entry      : 0x800af6b0 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
      Lapsed time: 7120 ns
    Feature: FIA_TRACE
      Entry      : 0x8045bd00 - IPV4_VFR_REFRAG
      Lapsed time: 2586 ns
    Feature: FIA_TRACE
      Entry      : 0x80466d20 - IPV6_MC_INPUT_VFR_REFRAG
      Lapsed time: 1413 ns
    Feature: FIA_TRACE Entry      : 0x807bf9a0 - MPLS_OUTPUT_ADD_LABEL

      Lapsed time: 3706 ns
    Feature: FIA_TRACE
      Entry      : 0x807b7030 - IPV6_OUTPUT_L2_REWRITE
      Lapsed time: 6586 ns
    Feature: FIA_TRACE
      Entry      : 0x804aadf0 - MPLS_OUTPUT_FRAG
      Lapsed time: 3253 ns
    Feature: FIA_TRACE
      Entry      : 0x8060bc80 - MPLS_OUTPUT_DROP_POLICY
      Lapsed time: 13200 ns
    Feature: FIA_TRACE
      Entry      : 0x80954900 - MARMOT_SPA_D_TRANSMIT_PKT
      Lapsed time: 23440 ns
```

For classification that does not meet the route-map criteria, the policy-routing is rejected and the traffic is dropped.

```
R1#ping 7.7.7.7 source 1.1.1.20 rep 2



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.20
.. Success rate is 0 percent
 (0/2)

R2#show platform packet-trace summary

Pkt   Input             Output            State  Reason
0     Gi1.12            Gi1.24            FWD
1     Gi1.12            Gi1.24            FWD
2     Gi1.12            Gi1.12            DROP   19  (Ipv4NoRoute)
3     Gi1.12            Gi1.12            DROP   19  (Ipv4NoRoute)
```

Note that the packet is not switched between the interfaces and is dropped.

```
R2#show platform packet-trace packet 3
Packet: 3           CBUG ID: 7
Summary Input      : GigabitEthernet1.12
 Output     : GigabitEthernet1.12
 State      : DROP 19  (Ipv4NoRoute)
  Timestamp
    Start   : 1409469943902513 ns (05/05/2015 23:08:18.349906 UTC)
    Stop    : 1409469943942561 ns (05/05/2015 23:08:18.349946 UTC)
Path Trace
  Feature: IPV4 Source      : 1.1.1.20
 Destination : 7.7.7.7
    Protocol    : 1 (ICMP)
  Feature: FIA_TRACE
    Entry      : 0x80880270 - DEBUG_COND_INPUT_PKT
    Lapsed time: 12000 ns
  Feature: FIA_TRACE
    Entry      : 0x8041cf00 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time: 5200 ns
  Feature: FIA_TRACE
    Entry      : 0x800e28a0 - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time: 4240 ns
  Feature: FIA_TRACE Entry      : 0x805ca780 - IPV4_INPUT_PBR
    Lapsed time: 78026 ns
  Feature: FIA_TRACE
```

```
Entry      : 0x806c7450 - STILE_LEGACY_DROP


    Lapsed time: 6773 ns
  Feature: FIA_TRACE
    Entry      : 0x802acdf0 - INPUT_FNF_AOR_DROP
    Lapsed time: 6240 ns
  Feature: FIA_TRACE
    Entry      : 0x80292be0 - INPUT_FNF_DROP
    Lapsed time: 11013 ns
  Feature: FIA_TRACE
    Entry      : 0x802b05f0 - OUTPUT_FNF_AOR_RELEASE_CLRT
    Lapsed time: 6373 ns
  Feature: FIA_TRACE Entry      : 0x807fc8c0 - INPUT_DROP


    Lapsed time: 533 ns
  Feature: FIA_TRACE
    Entry      : 0x8041b080 - IPV4_OUTPUT_LOOKUP_PROCESS
    Lapsed time: 286826 ns
```

The final result is that traffic forwarding is limited to the exact policy that is defined by the route-map.

```
R1#ping 20.20.20.20 source 1.1.1.20


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
R1#ping 7.7.7.7 source 1.1.1.7


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping 8.8.8.8 source 1.1.1.8


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

All other variations besides these are dropped.

```
R1#ping 8.8.8.8 source 1.1.1.7


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.7
.....
Success rate is 0 percent (0/5)
```

Another verification of these feature is to check the hits on the route-map.

```
R2#show route-map
```

route-map VRF_SELECTION_WITH_PBR, permit, sequence 10 Match clauses: ip address (access-lists): VPN_A_SOURCES Set clauses: vrf VPN_A **Policy routing matches: 36 packets, 3384 bytes** route-map VRF_SELECTION_WITH_PBR, permit, sequence 20 Match clauses: ip address (access-lists): VPN_B_SOURCES Set clauses: vrf VPN_B **Policy routing matches: 25 packets, 2950 bytes** route-map VRF_SELECTION_WITH_PBR, permit, sequence 30 Match clauses: ip address (access-lists): VPN_C_SOURCES Set clauses: vrf VPN_C **Policy routing matches: 54 packets, 6372 bytes**

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

Central Services MPLS L3 VPN

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Multisite L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Multisite L3VPN Diagram Diagram** in order to complete this task.

- Configure a VRF VPN_A on R2 with Route Distinguisher 100:1 and assign it to the link connecting to R1.
- Configure a VRF VPN_B on R4 with Route Distinguisher 100:2 and assign it to the link connecting to R7.
- Configure a VRF VPN_C on R5 with Route Distinguisher 100:3 and assign it to the link connecting to R8.
- Configure a VRF VPN_D on XR1 with Route Distinguisher 100:4 and assign it to the link connecting to XR2.
- Configure RIPv2 on all the PE-CE links and advertise the CE's Loopback0 interfaces into RIP.
- Configure BGP on R2, R4, R5, and XR1 as follows:
  - Use BGP AS 100.
  - Configure a full mesh of iBGP VPNv4 peerings between the PE routers.
  - Use their Loopback0 interfaces as the source of the BGP sessions.
  - Redistribute between the VRF aware RIP processes and VPNv4 BGP.
- Configure the Route Target Export policies on the PE routers as follows:
  - R2 should export R1's Loopback0 with RT 2.2.2.2:7 and 2.2.2.2:8.
  - XR1 should export XR2's Loopback0 with RT 19.19.19.19:7 and 19.19.19.19:8.
  - R4 should export R7's Loopback0 with RT 100:7.
  - R5 should export R5's Loopback0 with RT 100:8.
  - Do not export the PE to CE links into BGP.
- Configure the Route Target Import policies on the PE routers as follows:
  - R2 and XR1 should both import RTs 100:7 and 100:8.

- R4 should import RTs 2.2.2.2:7 and 19.19.19.19:7.
- R5 should import RTs 2.2.2.2:8 and 19.19.19.19:8.

- Once complete, only the following reachability should be achieved:
  - R7 should be able to reach R1 and XR2's Loopback0 networks when sourcing traffic from its own Loopback0.
  - R8 should be able to reach R1 and XR2's Loopback0 networks when sourcing traffic from its own Loopback0.

Configuration

```
R1:
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 1.0.0.0

R7:
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 7.0.0.0

R8:
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 8.0.0.0

R2:
vrf definition VPN_A
 rd 100:1
 route-target import 100:7
 route-target import 100:8
 !
 address-family ipv4
 export map R2_EXPORT_MAP
 exit-address-family
!
ip prefix-list R1_LOOPBACK seq 5 permit 1.1.1.1/32
!
```

```
route-map R2_EXPORT_MAP permit 10
 match ip address prefix-list R1_LOOPBACK
 set extcommunity rt 2.2.2.2:7 2.2.2.2:8
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric transparent
  network 10.0.0.0
  no auto-summary
  version 2
exit-address-family
!
router bgp 100
 template peer-session VPNv4_IBGP_SESSION
  remote-as 100
  update-source Loopback0
 exit-peer-session
 !
 bgp log-neighbor-changes
 neighbor 4.4.4.4 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 5.5.5.5 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 19.19.19.19 inherit peer-session VPNv4_IBGP_SESSION
 !
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family

R4:
vrf definition VPN_B
 rd 100:2
 route-target import 2.2.2.2:7
 route-target import 19.19.19.19:7
```

```
 !
 address-family ipv4
 export map R4_EXPORT_MAP
 exit-address-family
!
ip prefix-list R7_LOOPBACK seq 5 permit 7.7.7.7/32
!
route-map R4_EXPORT_MAP permit 10
 match ip address prefix-list R7_LOOPBACK
 set extcommunity rt 100:7
!
!
interface GigabitEthernet1.47
 vrf forwarding VPN_B
 ip address 10.4.7.4 255.255.255.0
!
router rip
 !
address-family ipv4 vrf VPN_B
 redistribute bgp 100 metric transparent
 network 10.0.0.0
 no auto-summary
 version 2
exit-address-family
!
router bgp 100
 template peer-session VPNv4_IBGP_SESSION
  remote-as 100
  update-source Loopback0
 exit-peer-session
 !
 bgp log-neighbor-changes
 neighbor 2.2.2.2 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 5.5.5.5 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 19.19.19.19 inherit peer-session VPNv4_IBGP_SESSION
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
!
address-family ipv4 vrf VPN_B
```

```
 redistribute rip
exit-address-family

R5:
vrf definition VPN_C
 rd 100:3
 route-target import 2.2.2.2:8
 route-target import 19.19.19.19:8
 !
 address-family ipv4
 export map R5_EXPORT_MAP
 exit-address-family
!
ip prefix-list R8_LOOPBACK seq 5 permit 8.8.8.8/32
!
route-map R5_EXPORT_MAP permit 10
 match ip address prefix-list R8_LOOPBACK
 set extcommunity rt    100:8
!
interface GigabitEthernet1.58
 vrf forwarding VPN_C
 ip address 10.5.8.5 255.255.255.0
!
router rip
 !
 address-family ipv4 vrf VPN_C
 redistribute bgp 100 metric transparent
 network 10.0.0.0
 no auto-summary
 version 2
exit-address-family
!
router bgp 100
 template peer-session VPNv4_IBGP_SESSION
  remote-as 100
  update-source Loopback0
 exit-peer-session
 !
 bgp log-neighbor-changes
 neighbor 2.2.2.2 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 4.4.4.4 inherit peer-session VPNv4_IBGP_SESSION
 neighbor 19.19.19.19 inherit peer-session VPNv4_IBGP_SESSION
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
```

```
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
!
address-family ipv4 vrf VPN_C
 redistribute rip
exit-address-family

XR1:
vrf VPN_D
 address-family ipv4 unicast
  import route-target
   100:7
   100:8
  !
  export route-policy EXPORT_POLICY
 !
!
interface GigabitEthernet0/0/0/0.1920
 no ipv4 address
 vrf VPN_D
 ipv4 address 10.19.20.19 255.255.255.0
!
route-policy EXPORT_POLICY
 if destination in (20.20.20.20/32) then
    set extcommunity rt (19.19.19.19:7, 19.19.19.19:8)
 endif
end-policy
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor-group VPNv4_IBGP
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 neighbor 2.2.2.2
  use neighbor-group VPNv4_IBGP
 !
 neighbor 4.4.4.4
  use neighbor-group VPNv4_IBGP
 !
```

```
 neighbor 5.5.5.5
  use neighbor-group VPNv4_IBGP
 !
 vrf VPN_D
  rd 100:4
  address-family ipv4 unicast
   redistribute rip
  !
 !
!
router rip
 vrf VPN_D
  interface GigabitEthernet0/0/0/0.1920
  !
  redistribute bgp 100
 !
!
end

XR2:
router rip
 interface Loopback0
 !
interface GigabitEthernet0/0/0/0.1920
 !
!
```

Verification

Central Services VPNs, sometimes called overlapping VPNs, allows multiple customers of the Service Provider network to access a centralized service in the SP network, for example hosted email, while still maintaining the separation of different customer routing tables. From a technical standpoint, the reason that this design works is that a VPNv4 BGP route can have multiple Route Target values at the same time, which means that the single route can be a member of multiple VPNs at the same time.

This is where the key distinction comes in between the VPNv4 Route Distinguisher and the VPNv4 Route Target. The Route Distinguisher (RD) is used to make the route unique, which allows different customers to use the same IP addressing scheme, for example RFC 1918 space, while the Route Target (RT) defines the route's VPN membership. A VPNv4 route will always have only one Route Distinguisher, but it can have multiple Route Targets.

Specifically in this example the Central Services could be represented by the Loopback0 networks of R1 and XR2, 1.1.1.1/32 and 20.20.20.20/32 respectively. When the PE routers R2 and XR1 export these prefixes into the VPNv4 BGP network, an **export-map** is used to apply a specific policy to the Route Target values. This feature gives you more control over which prefixes get which targets, which could include more than one RT, or no RTs at all.

The first step in verifying this design is to ensure that the VPNv4 routes have been tagged with the proper RT values as they are exported from the VRF into VPNv4 BGP, as seen below.

> **Note**: BGP templates were used on IOS, and BGP neighbor groups were used on IOS-XR to accomplish the full mesh BGP configuration. Both of these methods ease large and repetitive BGP configurations, but are not required to complete this task.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
      Origin incomplete, metric 1, localpref 100, weight 32768, valid, sourced, best
Extended Community: RT:2.2.2.2:7 RT:2.2.2.2:8
      mpls labels in/out 24/nolabel
      rx pathid: 0, tx pathid: 0x0

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast rd 100:4 20.20.20.20/32
Wed May  6 03:13:37.122 UTC
BGP routing table entry for 20.20.20.20/32, Route Distinguisher: 100:4
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 11          11
    Local Label: 16016
Last Modified: May  5 23:58:00.451 for 03:15:36
Paths: (1 available, best #1)
  Advertised to update-groups (with more than one peer):
```

```
    0.2
  Path #1: Received by speaker 0
  Advertised to update-groups (with more than one peer):
    0.2
  Local
    10.19.20.20 from 0.0.0.0 (19.19.19.19)
      Origin incomplete, metric 1, localpref 100, weight 32768, valid, redistributed, best, group-best, import-candi
      Received Path ID 0, Local Path ID 1, version 11
 Extended community: RT:19.19.19.19:7 RT:19.19.19.19:8
```

On the remote PEs, the import policy matches against the Route Target values to determine whether the route should be imported from VPNv4 into a local VRF. As long as the VPNv4 route has one of the RTs matched by the import policy, the route will be imported. In this specific case R4 imports 2.2.2.2:7 and 19.19.19.19:7, while R5 imports 2.2.2.2:8 and 19.19.19.19:8. The actual values used are arbitrary since there is no hierarchy to Route Targets. In practical implementations most service providers use external applications to track the Route Distinguisher and Route Target values assigned to specific customers and services to keep their configurations more manageable.

```
R4#show bgp vpnv4 unicast all
BGP table version is 104, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1
 *>i 1.1.1.1/32       2.2.2.2                  1    100      0 ?
Route Distinguisher: 100:2 (default for vrf VPN_B)
*>i 1.1.1.1/32       2.2.2.2                  1    100      0 ?
 *>  7.7.7.7/32       10.4.7.7                 1         32768 ?
 *>  10.4.7.0/24      0.0.0.0                  0         32768 ?
*>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
Route Distinguisher: 100:4
 *>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
R4#show ip route vrf VPN_B bgp

Routing Table: VPN_B
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [200/1] via 2.2.2.2, 1d18h
      20.0.0.0/32 is subnetted, 1 subnets
B        20.20.20.20 [200/1] via 19.19.19.19, 1d21h
```

R5#show bgp vpnv4 unicast all

```
BGP table version is 100, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1
 *>i 1.1.1.1/32       2.2.2.2                  1    100      0 ?
Route Distinguisher: 100:3 (default for vrf VPN_C)
 *>i 1.1.1.1/32       2.2.2.2                  1    100      0 ?
 *>  8.8.8.8/32       10.5.8.8                 1         32768 ?
 *>  10.5.8.0/24      0.0.0.0                  0         32768 ?
 *>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
Route Distinguisher: 100:4
 *>i 20.20.20.20/32   19.19.19.19              1    100      0 ?
```

R5#show ip route vrf VPN_C bgp

```
Routing Table: VPN_C
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [200/1] via 2.2.2.2, 1d18h
      20.0.0.0/32 is subnetted, 1 subnets
B        20.20.20.20 [200/1] via 19.19.19.19, 1d21h
```

Note that since R2 is not importing the RT values that XR1 is exporting, and vice-versa, and likewise R4 is not importing the RT values that R5 is exporting, and vice-versa, these routes do not appear in their local VPNv4 topologies. For example R4 sees the route to 20.20.20.20/32 in the VPNv4 table, but R2 does not.

```
R4#show bgp vpnv4 unicast all 20.20.20.20/32
BGP routing table entry for 100:2:20.20.20.20/32, version 10
Paths: (1 available, best #1, table VPN_B)
  Not advertised to any peer
  Refresh Epoch 1
  Local, imported path from 100:4:20.20.20.20/32 (global)
    19.19.19.19 (metric 3) (via default) from 19.19.19.19 (19.19.19.19)
      Origin incomplete, metric 1, localpref 100, valid, internal, best
Extended Community: RT:19.19.19.19:7 RT:19.19.19.19:8
      mpls labels in/out nolabel/16016
      rx pathid: 0, tx pathid: 0x0
BGP routing table entry for 100:4:20.20.20.20/32, version 11
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    19.19.19.19 (metric 3) (via default) from 19.19.19.19 (19.19.19.19)
      Origin incomplete, metric 1, localpref 100, valid, internal, best
Extended Community: RT:19.19.19.19:7 RT:19.19.19.19:8
      mpls labels in/out nolabel/16016
      rx pathid: 0, tx pathid: 0x0

R2#show bgp vpnv4 unicast all 20.20.20.20/32

% Network not in table
```

This is due to an optimization of inbound VPNv4 filtering of the BGP process, and is the default and desirable behavior. Specifically what is occurring here is that when R2 receives VPNv4 routes from its peers, it looks at the Route Target values that are in the BGP extended communities fields. If none of the Route Target values of the route match a local import policy, the route is automatically discarded. This helps to keep the size of the VPNv4 BGP table smaller, as routes for customers that a local PE is not servicing can be discarded.

This filtering can be viewed in real time by observing the output of the **debug ip bgp vpnv4 unicast update**, as seen below.

```
R2#debug ip bgp vpnv4 unicast update
BGP updates debugging is on for address family: VPNv4 Unicast
R2#clear bgp vpnv4 unicast 19.19.19.19 in

R2#BGP(4): 19.19.19.19 rcvd UPDATE w/ attr: nexthop 19.19.19.19, origin ?, localpref 100, metric 1,
extended community RT:19.19.19.19:7 RT:19.19.19.19:8
BGP(4): 19.19.19.19 rcvd
100:4:20.20.20.20/32, label 16016 -- DENIED due to:  extended community not supported;
BGP(4): 19.19.19.19 rcvd UPDATE w/ attr: nexthop 19.19.19.19, origin ?, localpref 100, metric 0
BGP(4): 19.19.19.19 rcvd
100:4:10.19.20.0/24, label 16007 -- DENIED due to:  extended community not supported;
```

The output *extended community not supported* means that there is not a RT that matches a local import policy. Note that the first VPNv4 prefix, 100:4:20.20.20.20/32 has RT values 19.19.19.19:7 and 19.19.19.19:8, while the second VPNv4 prefix 100:4:10.19.20.0/24 has no RT values at all. This is due to the fact that the export route-policy configured on XR1 did not match 10.19.20.0/24, which effectively means that no other PE can import this route.

The final result of this design should be that R7 and R8's Loopback0s can reach the Loopback0s of R1 and XR2, while no other connectivity is permitted.

```
R7#ping 1.1.1.1 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 20.20.20.20 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/3/4 ms
R7#ping 1.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....Success rate is 0 percent
 (0/5)
R8#ping 1.1.1.1 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/2/4 ms
R8#ping 20.20.20.20 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/3/4 ms
R8#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....Success rate is 0 percent
 (0/5)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN VPNv4 Route Reflection

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Multisite L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Multisite L3VPN Diagram Diagram** in order to complete this task.

- Configure a VRF on R2 and R5 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF on R2 and R5 to the links connecting to R1 and R8 respectively.
- Configure a VRF on R4 and XR1 as follows:
  - VRF Name: VPN_B
  - Route Distinguisher: 100:2
  - Route Target Import: 100:2
  - Route Target Export: 100:2
  - Assign the VRF on R4 and XR1 to the links connecting to R7 and XR2 respectively.
- Configure EIGRP AS 1 on the links between the PE to CEs, and advertise the CEs' Loopback0 networks into EIGRP.
- Configure BGP on R2, R3, R4, R5, and XR1 as follows:
  - Use BGP AS 100.
  - All devices should peer with R3 via iBGP for the VPNv4 Address Family.
  - R3 should be the VPNv4 Route Reflector for these four clients.
  - Use their Loopback0 interfaces as the source of the BGP session.
  - Redistribute between BGP and the VRF aware EIGRP process on the PE routers.
- Once complete R1 should have reachability to all of R8's networks, and vice-versa,

and XR2 should have reachability to all of R7's networks, and vice-versa.

Configuration

```
R1:
router eigrp 1
 network 1.0.0.0
 network 10.0.0.0
 no auto-summary

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_A
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
 no synchronization
 no auto-summary
exit-address-family
!
address-family vpnv4
```

```
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 no synchronization
 redistribute eigrp 1
exit-address-family
!

R3:
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 ipv4
 no synchronization
 no auto-summary
exit-address-family
!
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

R4:
vrf definition VPN_B
 rd 100:2
```

```
 route-target export 100:2
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.47
 vrf forwarding VPN_B
 ip address 10.4.7.4 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
address-family ipv4 vrf VPN_B
 redistribute eigrp 1
exit-address-family
!

R5:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
```

```
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.58
 vrf forwarding VPN_A
 ip address 10.5.8.5 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_A
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
address-family ipv4 vrf VPN_A
 redistribute eigrp 1
exit-address-family
!

R7:
router eigrp 1
 network 7.0.0.0
 network 10.0.0.0
 no auto-summary

R8:
router eigrp 1
 network 8.0.0.0
```

```
 network 10.0.0.0
 no auto-summary

XR1:
vrf VPN_B
 address-family ipv4 unicast
  import route-target
   100:2
  !
  export route-target
   100:2
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_B
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf VPN_B
  rd 100:2
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
router eigrp 65535
 vrf VPN_B
   address-family ipv4
   no auto-summary
   redistribute bgp 100
   autonomous-system 1
   interface GigabitEthernet0/0/0/0.1920
   !
  !
 !
!
```

```
end

XR2:
router eigrp 1
   address-family ipv4
   no auto-summary
   interface Loopback0
   !
   interface GigabitEthernet0/0/0/0.1920
  !
 !
!
```

Verification

Similar to IPv4 Unicast BGP Route Reflectors, VPNv4 Route Reflectors help to scale the BGP topology by removing the requirement of a full mesh of iBGP sessions, and by reducing the number of possible routes that an individual BGP peer must make its best path selection on.

Configuration of route reflection for VPNv4 is identical to regular IPv4 Unicast route reflection, with the exception that the **route-reflector-client** statement goes under the **address-family vpnv4** as opposed to under the global process or under the **address-family ipv4 unicast**. Note that a router can be a route reflector for multiple address families at the same time, or independently of each other, as IPv4 Unicast, IPv6 Unicast, VPNv4, VPNv6, etc. AF configuration is independent of other address families. However, service providers locate the route reflectors for each address family on separate devices.

In this specific example, R3 is the VPNv4 route reflector for four peers, R2, R4, R5, and XR1. This means that R3 should know about all VPNv4 routes that are originated by all PE routers, even though it does not have any VRFs locally configured. This is an exception to the normal Route Target based filtering, as a Route Reflector must accept all routes from all peers in order to have a full view of the overall topology.

```
R3#show bgp vpnv4 unicast all summary
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 14, main routing table version 14
8 network entries using 2048 bytes of memory
8 path entries using 960 bytes of memory
8/8 BGP path/bestpath attribute entries using 2112 bytes of memory
8 BGP extended community entries using 2000 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
```

```
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7120 total bytes of memory
BGP activity 8/0 prefixes, 8/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2          4        100       10          14       0         0     0     00:04:20        2
4.4.4.4          4        100       10          14       0          0     0     00:03:52        2
5.5.5.5          4        100        9          14       0          0     0     00:03:40        2
19.19.19.19      4        100        5          14       0          0     0     00:00:59        2



R3#show bgp vpnv4 unicast all

BGP table version is 14, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
 Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1
*>i1.1.1.1/32       2.2.2.2             156160   100       0  ?
*>i8.8.8.8/32       5.5.5.5             156160   100       0  ?
*>i10.1.2.0/24      2.2.2.2                  0   100       0  ?
*>i10.5.8.0/24      5.5.5.5                  0   100       0  ?
Route Distinguisher: 100:2
*>i7.7.7.7/32       4.4.4.4             156160   100       0  ?
*>i10.4.7.0/24      4.4.4.4                  0   100       0  ?
*>i10.19.20.0/24    19.19.19.19              0   100       0  ?
*>i20.20.20.20/32   19.19.19.19         131584   100       0  ?
```

Note that since R3 does not have any VRF tables configured, none of the VPNv4 routes are actually associated with any routing tables. Instead R3 just maintains the BGP RIB structure, but not actual an actual routing table RIB or CEF FIB for these prefixes.

```
R3#show bgp vpnv4 unicast all 1.1.1.1/32
BGP routing table entry for 100:1:1.1.1.1/32, version 2 Paths: (1 available, best #1, no table
)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local, (Received from a RR-client)
    2.2.2.2 (metric 2) (via default) from 2.2.2.2 (2.2.2.2)
      Origin incomplete, metric 130816, localpref 100, valid, internal, best
```

```
      Extended Community: RT:100:1 Cost:pre-bestpath:128:130816
        0x8800:32768:0 0x8801:1:128256 0x8802:65281:2560 0x8803:65281:1500
        0x8806:0:16843009
      mpls labels in/out nolabel/36
      rx pathid: 0, tx pathid: 0x0
R3#show ip route vrf * 1.1.1.1

R3#show ip route vrf * 1.1.1.1
% Network not in table
```

As will be seen in later sections, a RR can insert itself in the forwarding path for all of the VPNv4 prefixes by changing the next-hop to itself. Although the RR will not have the routes in the RIB, LFIB entries will be created for all paths for which the RR set itself as the next-hop.

VPNv4 Route Reflection follows the same rules as regular IPv4 Unicast Route Reflection, in which routes are exchanged between all peers of the Route Reflector with the exception of non-clients. Routes that are received from non-client peers cannot be advertised to other non- client peers, just like in IPv4 Unicast.

In this example we see that R3 advertises routes with Route Distinguisher 100:1 and 100:2 to all peers, as it has no way of knowing which VRFs the PE routers actually want to use or which routes they want to import.

```
R3#show bgp vpnv4 unicast all neighbors 2.2.2.2 advertised-routes

BGP table version is 14, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

 Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1
*>i1.1.1.1/32       2.2.2.2     156160  100         0   ?
*>i8.8.8.8/32       5.5.5.5     156160  100         0   ?
*>i10.1.2.0/24      2.2.2.2          0   100         0   ?
*>i10.5.8.0/24      5.5.5.5          0   100         0   ?
Route Distinguisher: 100:2
*>i7.7.7.7/32       4.4.4.4     156160  100         0   ?
*>i10.4.7.0/24      4.4.4.4          0   100         0   ?
*>i10.19.20.0/24    19.19.19.19      0   100         0   ?
*>i20.20.20.20/32   19.19.19.19 131584  100         0   ?
```

```
Total number of prefixes 8
```

Once the routes are received by the remote PE routers, they can choose whether to install or discard them based on the default Route Target filtering. In the below output we see that R2 filters out VPNv4 prefixes that have the Route Target 100:2, as it does not have a local VRF with a matching import policy for 100:2. This behavior can be disabled on a non route-reflector IOS node by disabling the default RT filtering - 'no bgp default route-target filter'. This will allow a device receiving VPNv4 updates containing RT values not being imported on any VRFs to not be dropped. These routes would then stay in the BGP RIB, consuming memory. The default behavior of dropping routes that will not be imported conserves resources on the devices.

Also note that the route reflector can potentially loop routing advertisements throughout the network, but attributes such as the ORIGINATOR or CLUSTER_LIST will prevent any negative effects, similar to regular IPv4 Unicast Route Reflection.

```
R2#debug bgp vpnv4 unicast updates
BGP updates debugging is on for address family: VPNv4 UnicastR2#clear bgp vpnv4 unicast * in
BGP: nbr_topo global 3.3.3.3 VPNv4 Unicast:base (0x7F7881C267E8:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 3.3.3.3 VPNv4 Unicast:base (0x7F7881C267E8:1) refresh_epoch is 2
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 19.19.19.19, origin ?, localpref 100, metric 0, originator 19.19.19.19,
BGP(4): 3.3.3.3 rcvd 100:2:10.19.20.0/24, label 16015 --
DENIED due to: extended community not supported;
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 5.5.5.5, origin ?, localpref 100, metric 0, originator 5.5.5.5, cluster
BGP(4): 3.3.3.3 rcvd 100:1:10.5.8.0/24, label 31...duplicate ignored
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 4.4.4.4, origin ?, localpref 100, metric 0, originator 4.4.4.4, cluster
BGP(4): 3.3.3.3 rcvd 100:2:10.4.7.0/24, label 29 -- DENIED due to:  extended community not supported;
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 19.19.19.19, origin ?, localpref 100, metric 10752, originator 19.19.19
BGP(4): 3.3.3.3 rcvd 100:2:20.20.20.20/32, label 16017 --
DENIED due to:  extended community not supported;
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 4.4.4.4, origin ?, localpref 100, metric 130816, originator 4.4.4.4, cl
BGP(4): 3.3.3.3 rcvd 100:2:7.7.7.7/32, label 32 -- DENIED due to:  extended community not supported;
BGP: 3.3.3.3 Next hop is our own address 2.2.2.2
BGP: 3.3.3.3 Local router is the Originator; Discard update
 BGP(4): 3.3.3.3 rcv UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 130816, originator 2.2.2.2, cl
BGP(4): 3.3.3.3 rcv UPDATE about 100:1:1.1.1.1/32 --
DENIED due to: ORIGINATOR is us; MP_REACH NEXTHOP is our own address
;, label 36
BGP(4): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 5.5.5.5, origin ?, localpref 100, metric 130816, originator 5.5.5.5, cl
BGP(4): 3.3.3.3 rcvd 100:1:8.8.8.8/32, label 33...duplicate ignored BGP: 3.3.3.3 Next hop is our own address 2.2.2.2
BGP: 3.3.3.3 Local router is the Originator; Discard update
BGP(4): 3.3.3.3 rcv UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 0, originator 2.2.2.2, clusterl
```

```
BGPSSA ssacount is 0 BGP(4): 3.3.3.3 rcv UPDATE about 100:1:10.1.2.0/24 --
DENIED due to: ORIGINATOR is us; MP_REACH NEXTHOP is our own address
;, label 22 BGP: nbr_topo global 3.3.3.3 VPNv4 Unicast:base (0x7F7881C267E8:1) rcvd Refresh End-of-RIB
```

Another important point to note about VPNv4 Route Reflection is the next-hop processing rules. Just like in IPv4 Unicast, a Route Reflector does not modify the next-hop value of routes that are reflected. Mainly the attributes that the Route Reflector is changing are the ORIGINATOR and the CLUSTER_LIST, which are both used for additional loop prevention.

The below output indicates that the next-hop is 4.4.4.4, the route was learned from the route reflector with ID 3.3.3.3, but the router with ID 4.4.4.4 was the originator.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_B 7.7.7.7/32
Thu May  7 23:11:16.041 UTC
BGP routing table entry for 7.7.7.7/32, Route Distinguisher: 100:2
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  8           8
Last Modified: May  7 22:56:18.451 for 00:14:57
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local 4.4.4.4 (metric 3) from 3.3.3.3
 (4.4.4.4)
      Received Label 32
      Origin incomplete, metric 130816, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 8
      Extended community: COST:128:128:130816 EIGRP route-info:0x8000:0 EIGRP AD:1:128256 EIGRP RHB:255:1:2560 EIGRP
 Originator: 4.4.4.4, Cluster list: 3.3.3.3

      Source VRF: VPN_B, Source Route Distinguisher: 100:2
```

The reason that this is especially important for VPNv4 routing is that the next-hop value determines where the Label Switch Path (LSP) in the MPLS network is terminated. If the next- hop value of the VPNv4 route were to change, it means that a different Transport Label would be used in the core of the MPLS topology, which changes the LSP that is followed. This behavior becomes even more significant when we look at Inter-AS MPLS L3VPN and Multihop EBGP Peerings between VPNv4 Route Reflectors, which is commonly referred to as Inter-AS Option C or Inter-AS Option 3.

Note that in the below output since the Route Reflector did not change the next-hop value, it is not actually in the data plane path for the MPLS LSP. Instead the Route Reflector is used just to maintain the control plane of the network. The VPN label used, 32, is allocated and advertised by R4. Additionally, the next-hop for the VPNv4 route is R4, thus the LSP "tunnel" terminates on this node. If the route-reflector would have changed the next-hop to self, two LSPs would be built - one from XR1 to R3, and another from R3 to R4.

```
RP/0/0/CPU0:XR2#traceroute 7.7.7.7

Thu May  7 23:12:31.756 UTC

Type escape sequence to abort.
Tracing the route to 7.7.7.7

 1  10.19.20.19 9 msec  0 msec  0 msec
 2  20.5.19.5 [MPLS: Labels 17/32 Exp 0] 0 msec  0 msec  0 msec
 3  10.4.7.4 [MPLS: Label 32 Exp 0] 0 msec  9 msec  0 msec
 4  10.4.7.7 9 msec  *  9 msec
```

The final end result is that the customer sites of VPN_A and VPN_B have a full mesh of connectivity within their sites, but as usual routes are not leaked between different customer sites.

```
R1#show ip route eigrp
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
      8.0.0.0/32 is subnetted, 1 subnets
D        8.8.8.8 [90/131072] via 10.1.2.2, 00:22:51, GigabitEthernet1.12
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.5.8.0/24 [90/3072] via 10.1.2.2, 00:22:56, GigabitEthernet1.12
R1#ping 8.8.8.8


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping 10.5.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
RP/0/0/CPU0:XR2#show route ipv4 eigrp
Thu May  7 23:17:18.687 UTC

D    7.7.7.7/32 [90/2575360] via 10.19.20.19, 00:21:00, GigabitEthernet0/0/0/0.1920
D    10.4.7.0/24 [90/15360] via 10.19.20.19, 00:21:00, GigabitEthernet0/0/0/0.1920
RP/0/0/CPU0:XR2#ping 7.7.7.7
Thu May  7 23:17:40.535 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
RP/0/0/CPU0:XR2#ping 10.4.7.7

Thu May  7 23:17:52.134 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN VPNv4 Route Reflection w/ IOS XR

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Multisite L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Multisite L3VPN Diagram Diagram** in order to complete this task.

- Configure a VRF on R2 and R5 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF on R2 and R5 to the links connecting to R1 and R8 respectively.
- Configure a VRF on R4 and XR1 as follows:
  - VRF Name: VPN_B
  - Route Distinguisher: 100:2
  - Route Target Import: 100:2
  - Route Target Export: 100:2
  - Assign the VRF on R4 and XR1 to the links connecting to R7 and XR2 respectively.
- Configure EIGRP AS 1 on the links between the PE to CEs, and advertise the CEs' Loopback0 networks into EIGRP.
- Configure BGP on R2, R4, R5, and XR1 as follows:
  - Use BGP AS 100.
  - All devices should peer with XR1 via iBGP for the VPNv4 Address Family.
  - XR1 should be the VPNv4 Route Reflector for these three clients.
  - Use their Loopback0 interfaces as the source of the BGP session.
  - Redistribute between BGP and the VRF aware EIGRP process on the PE routers.
- Once complete R1 should have reachability to all of R8's networks, and vice-versa,

and XR2 should have reachability to all of R7’s networks, and vice-versa.

Configuration

```
R1:
router eigrp 1
 network 1.0.0.0
 network 10.0.0.0
 no auto-summary

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_A
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
```

```
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  no synchronization
  redistribute eigrp 1
  exit-address-family
!

R4:
vrf definition VPN_B
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.47
 vrf forwarding VPN_B
 ip address 10.4.7.4 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
```

```
 exit-address-family
 !
 address-family ipv4 vrf VPN_B
  no synchronization
  redistribute eigrp 1
 exit-address-family
!

R5:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.58
 vrf forwarding VPN_A
 ip address 10.5.8.5 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_A
  autonomous-system 1
  redistribute bgp 100
  network 10.0.0.0
  no auto-summary
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
```

```
 address-family ipv4 vrf VPN_A
  no synchronization
  redistribute eigrp 1
 exit-address-family
!

R7:
router eigrp 1
 network 7.0.0.0
 network 10.0.0.0
 no auto-summary

R8:
router eigrp 1
 network 8.0.0.0
 network 10.0.0.0
 no auto-summary

XR1:
vrf VPN_B
 address-family ipv4 unicast
  import route-target
   100:2
  !
  export route-target
   100:2
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_B
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0

!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 neighbor 4.4.4.4
```

```
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
    route-reflector-client
  !
 !
 neighbor 5.5.5.5
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 vrf VPN_B
  rd 100:2
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
router eigrp 65535
  vrf VPN_B
  address-family ipv4
   no auto-summary
   redistribute bgp 100
   autonomous-system 1
   interface GigabitEthernet0/0/0/0.1920
   !
  !
 !
!

XR2:
router eigrp 1
  address-family ipv4
   no auto-summary
   interface Loopback0
   !
   interface GigabitEthernet0/0/0/0.1920
  !
 !
!
```

Verification

This example is similar to the previous one which used regular IOS and the VPNv4 Route Reflector. In this case XR1 peers with all other PE routers, and is a Route Reflector for the VPNv4 address family. This means that XR1 will be receiving all VPNv4 routes, regardless if it has a local VRF configured with a matching import policy, as seen below.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast

 Thu May  7 23:38:38.838 UTC
 BGP router identifier 19.19.19.19, local AS number 100
 BGP generic scan interval 60 secs
 BGP table state: Active
 Table ID: 0x0   RD version: 0
 BGP main routing table version 11
 BGP scan interval 60 secs

 Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
 Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
 Route Distinguisher: 100:1
 *>i1.1.1.1/32       2.2.2.2         156160     100      0   ?
 *>i8.8.8.8/32       5.5.5.5         156160     100      0   ?
 *>i10.1.2.0/24      2.2.2.2              0     100      0   ?
 *>i10.5.8.0/24      5.5.5.5              0     100      0   ?
 Route Distinguisher: 100:2 (default for vrf VPN_B)
 *>i7.7.7.7/32       4.4.4.4         156160     100      0   ?
 *>i10.4.7.0/24      4.4.4.4              0     100      0   ?
 *> 10.19.20.0/24    0.0.0.0              0          32768   ?
 *> 20.20.20.20/32   10.19.20.20     131584          32768   ?
 Processed 8 prefixes, 8 paths
 RP/0/0/CPU0:XR1#
```

Note that the routes with the Route Distinguisher 100:1 do not have a VRF or routing table associated with them, but they are still kept in the BGP RIB and can be advertised.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast rd 100:1 1.1.1.1/32

 Thu May  7 23:39:40.504 UTC
 BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
```

```
Versions:
 Process           bRIB/RIB  SendTblVer
 Speaker                  3           3
Last Modified: May  7 23:38:21.451 for 00:01:19
Paths: (1 available, best #1)
 Advertised to update-groups (with more than one peer):
   0.2
 Path #1: Received by speaker 0
 Advertised to update-groups (with more than one peer):
   0.2
 Local, (Received from a RR-client)
   2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
     Received Label 18
     Origin incomplete, metric 130816, localpref 100, valid, internal, best, group-best, import-candidate, not-in-vr
     Received Path ID 0, Local Path ID 1, version 3
     Extended community: COST:128:128:130816 EIGRP route-info:0x8000:0 EIGRP AD:1:128256 EIGRP RHB:255:1:2560 EIGRP
```

By default all routes are then advertised to all peers, and it is up to them to determine which ones they want or don’t want.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast neighbors 5.5.5.5 advertised-routes

Thu May  7 23:45:28.450 UTC
Network            Next Hop        From            AS Path
Route Distinguisher: 100:1
1.1.1.1/32         2.2.2.2         2.2.2.2         ?
8.8.8.8/32         19.19.19.19     5.5.5.5         ?
10.1.2.0/24        2.2.2.2         2.2.2.2         ?
10.5.8.0/24        19.19.19.19     5.5.5.5         ?
Route Distinguisher: 100:2
7.7.7.7/32         4.4.4.4         4.4.4.4         ?
10.4.7.0/24        4.4.4.4         4.4.4.4         ?
10.19.20.0/24      19.19.19.19     Local           ?

Processed 7 prefixes, 7 paths
```

IOS XR VPNv4 Route Reflectors can also be configured to selectively accept VPNv4 routes based on their route targets by using the command **retain route-target route-policy *route-policy-name***. This could be used in a design where one RR services a certain set of PEs, while another RR services a separate set of PEs.

For example if we wanted XR1 to not accept VPNv4 routes that have the Route Target 100:1, this could be implemented as follows:

```
route-policy FILTER_ON_RT
    if extcommunity rt matches-any (100:1) then
        drop
    else
        pass
    endif
end-policy
!
router bgp 100
 address-family vpnv4 unicast
  retain route-target route-policy FILTER_ON_RT
   !
  !
```

Now XR1 denies VPNv4 routes that have the Route Target 100:1.

```
RP/0/0/CPU0:XR1#debug bgp update vpnv4 unicast in
Thu May  7 23:55:40.139 UTC
RP/0/0/CPU0:XR1#clear bgp vpnv4 unicast 2.2.2.2 soft in
Thu May  7 23:55:45.008 UTC

RP/0/0/CPU0:XR1#RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: UPDATE from 2.2.2.2 contains nh 2.2.2.2/
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=2.2.2.2/32, len=12, nlriafi=4,
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=2.2.2.2:: msg=0x10037c
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 2.2.2.2 with attributes:
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): nexthop 2.2.2.2/32, origin ?, localpref 100, met
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:100:1:1.1.1.1/32 (path ID:
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:100:1:1.1.1.1/32
 (path ID: none) received from 2.2.2.2 DENIED RT extended community is not imported locally
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: UPDATE from 2.2.2.2 contains nh 2.2.2.2/32, gw_afi 0, fl
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=2.2.2.2/32, len=12, nlriafi=4,
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=2.2.2.2:: msg=0x10037e
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 2.2.2.2 with attributes:
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): nexthop 2.2.2.2/32, origin ?, localpref 100, met
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:100:1:10.1.2.0/24 (path ID:
RP/0/0/CPU0:May  7 23:55:45.108 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:100:1:10.1.2.0/24
 (path ID: none) received from 2.2.2.2 DENIED RT extended community is not imported locally
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast

Thu May  7 23:57:55.049 UTC
BGP router identifier 19.19.19.19, local AS number 100
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 23
```

```
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:2 (default for vrf VPN_B)
*>i7.7.7.7/32       4.4.4.4         156160      100        0    ?
*>i10.4.7.0/24      4.4.4.4              0      100        0    ?
*> 10.19.20.0/24    0.0.0.0              0             32768    ?
*> 20.20.20.20/32   10.19.20.20     131584             32768    ?

Processed 4 prefixes, 4 paths
```

The normal behavior for a VPNv4 Route Reflector is the **retain route-target all**, which means that routes are not filtered based on their RT values.

Another common configuration in IOS XR for Route Reflection would be to group the client peers into a **neighbor-group** to simplify the configuration and its inheritance. This feature is similar to the **peer-group** in regular IOS. An configuration similar to this example, but with the usage of neighbor groups, could read as follows.

```
RP/0/0/CPU0:XR1#sh run router bgp

Fri Mar 9 23:39:18.919 UTC
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor-group VPNv4_CLIENTS
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 neighbor 2.2.2.2
  use neighbor-group VPNv4_CLIENTS
 !
 neighbor 4.4.4.4
  use neighbor-group VPNv4_CLIENTS
 !
 neighbor 5.5.5.5
  use neighbor-group VPNv4_CLIENTS
 !
```

```
 vrf VPN_B
  rd 100:2
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
```

The end result of either of these configurations is the same, that XR1 receives routes from all PEs and reflects them back. The final verification of this design would again be to test connectivity between the customer sites, as follows.

```
RP/0/0/CPU0:XR2#show route ipv4 eigrp
Fri May  8 00:01:37.084 UTC

D    7.7.7.7/32 [90/2575360] via 10.19.20.19, 00:02:13, GigabitEthernet0/0/0/0.1920
D    10.4.7.0/24 [90/15360] via 10.19.20.19, 00:02:13, GigabitEthernet0/0/0/0.1920
RP/0/0/CPU0:XR2#ping 7.7.7.7
Fri May  8 00:01:55.923 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms
R8#sh ip route eigrp
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      8.0.0.0/32 is subnetted, 1 subnets
D        8.8.8.8 [90/131072] via 10.1.2.2, 00:00:47, GigabitEthernet1.12
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.5.8.0/24 [90/3072] via 10.1.2.2, 00:00:47, GigabitEthernet1.12
R8#ping 1.1.1.1



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN and OSPF Sham-Links

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **L3VPN Backdoor Links**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **L3VPN Backdoor Links Diagram** in order to complete this task.

- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure OSPF routing for the VRF as follows:
  - Use Process-ID 100.
  - Enable OSPF Area 0 between R1 & R2.
  - Enable OSPF Area 0 between R1 & XR2.
  - Enable OSPF Area 0 between XR1 & XR2.
  - Advertise the Loopback0 networks of R1 & XR2 into OSPF Area 0.
  - Modify the link between R1 and XR2 to have an OSPF cost of 100.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
  - Redistribute between BGP and the VRF aware OSPF process.
- Configure an OSPF Sham Link between R2 and XR1 as follows:
  - Create a new Loopback interface on R2 with the address 10.2.2.2/32.
  - Create a new Loopback interface on XR1 with the address 10.19.19.19/32.
  - Assign these new Loopbacks to VRF VPN_A.
  - Advertise them into VPNv4 BGP, but ***not*** into the VRF aware OSPF process.
  - Configure an OSPF Sham Link in Area 0 between R2 and XR1 using these

new Loopback interfaces.

- Once complete, the following reachability should be achieved:
  - R1 and XR2 should have reachability to all of each other’s networks.
  - Traffic between the Loopback0 networks of R1 and XR2 should prefer to use the MPLS network.
  - If either R1 or XR2 lose connectivity to the MPLS cloud, traffic should be automatically be rerouted over the backdoor link.

Configuration

```
R1:
interface GigabitEthernet1.120
 ip ospf cost 100
!
router ospf 100
 network 0.0.0.0 255.255.255.255 area 0

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
interface Loopback100
 vrf forwarding VPN_A
 ip address 10.2.2.2 255.255.255.255
!
ip prefix-list SHAM_LINK_ENDPOINTS seq 5 permit 10.2.2.2/32
ip prefix-list SHAM_LINK_ENDPOINTS seq 10 permit 10.19.19.19/32
!
route-map BGP_TO_OSPF deny 10
 match ip address prefix-list SHAM_LINK_ENDPOINTS
!
route-map BGP_TO_OSPF permit 20
!
router ospf 100 vrf VPN_A
```

```
 area 0 sham-link 10.2.2.2 10.19.19.19
 redistribute bgp 100 subnets route-map BGP_TO_OSPF
 network 10.1.2.2 0.0.0.0 area 0
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  no synchronization
  redistribute ospf 100
  network 10.2.2.2 mask 255.255.255.255
 exit-address-family
!

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
 !
 export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0
!
interface Loopback100
 vrf VPN_A
 ipv4 address 10.19.19.19 255.255.255.255
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
```

```
   remote-as 100
   update-source Loopback0
   address-family vpnv4 unicast
   !
  !
  vrf VPN_A
   rd 100:1
   address-family ipv4 unicast
    redistribute ospf 100
    network 10.19.19.19/32
   !
  !
 !
 prefix-set SHAM_LINK_ENDPOINTS
   10.2.2.2,
   10.19.19.19
 end-set
 !
 route-policy BGP_TO_OSPF
   if destination in SHAM_LINK_ENDPOINTS then
     drop
   else
     pass
   endif
 end-policy
 !
 router ospf 100
  vrf VPN_A
   redistribute bgp 100 route-policy BGP_TO_OSPF
   area 0
    interface GigabitEthernet0/0/0/0.1920
    sham-link 10.19.19.19 10.2.2.2
  !
 !

 XR2:
 router ospf 100
  area 0
   interface Loopback0
   !
   interface GigabitEthernet0/0/0/0.1920
   !
   interface GigabitEthernet0/0/0/0.120
    cost 100
   !
  !
```

```
!
```

Verification

OSPF Sham Links, similar to Virtual Links, are multihop unicast adjacencies between OSPF neighbors that are used for the purpose of traffic engineering. Due to the inherent nature of OSPF Path Selection per the RFC specification, OSPF always prefers Intra Area routes over Inter Area routes over External Routes over NSSA External Routes, regardless of Administrative Distance or Metric.

OSPF Sham Links are needed in designs where backdoor connections exist between customer sites, such as legacy T1, Frame Relay, or any other point-to-point connection, in addition to the MPLS L3VPN connection, and the MPLS connections need to be preferred over the backdoor links. Due to the behavior of the OSPF “Superbackbone” of MPLS, routes on one customer site that are Intra-Area (O routes) will appear in other customer sites as Inter-Area (O IA routes) as long as the OSPF Domain-ID field matches in the BGP VPNv4 route. If the Domain-ID field does not match, the routes will appear as either External Type 1 (E1 routes) or External Type 2 (E2 routes). This means that if there is a backdoor link between the customer sites that allows routes to be exchanged as Intra-Area (O routes), these will always be preferred over the O IA, E1, or E2 routes coming from the MPLS L3VPN.

To fix this, a Sham Link, similar to a Virtual Link, extends the OSPF flooding domain of an area over a logical multi-hop adjacency. This essentially makes the PE routers no longer appear as ABRs or ASBRs in the OSPF database, but regular routers that are all in the same area. The result is that Intra-Area (O routes) can be learned from the PE routers, which can then be preferred over backdoor links simply based on changing the OSPF cost of interfaces in the topology per your desired traffic engineering goals.

Unlike virtual-links, sham-links can be assigned to any area, and a reachable IPv4 source and destination need to be manually configured in order for the adjacency to be established.

In this particular example R2 and XR1 form a Sham Link adjacency over the MPLS network. To do this, they first need a new /32 Loopback interface that is a member of the VRF, and is advertised into VPNv4 BGP. In this specific case these are the 10.2.2.2/32 and 10.19.19.19/32 prefixes.

```
R2#show ip route vrf VPN_A 10.2.2.2

Routing Table: VPN_A
Routing entry for 10.2.2.2/32
```

```
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Redistributing via ospf 100
  Advertised by bgp 100
  Routing Descriptor Blocks:
  * directly connected, via Loopback100
      Route metric is 0, traffic share count is 1
R2#show ip route vrf VPN_A 10.19.19.19

Routing Table: VPN_A
Routing entry for 10.19.19.19/32
  Known via "bgp 100", distance 200, metric 0, type internal
  Redistributing via ospf 100
  Last update from 19.19.19.19 00:22:44 ago
  Routing Descriptor Blocks:
  * 19.19.19.19 (default), from 19.19.19.19, 00:22:44 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 16000
      MPLS Flags: MPLS Required
RP/0/0/CPU0:XR1#show route vrf VPN_A 10.2.2.2
Fri May  8 01:10:30.351 UTC

Routing entry for 10.2.2.2/32
  Known via "bgp 100", distance 200, metric 0, type internal
  Installed May  8 00:47:24.236 for 00:23:06
  Routing Descriptor Blocks
    2.2.2.2, from 2.2.2.2
      Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
      Route metric is 0
  No advertising protos.

RP/0/0/CPU0:XR1#show route vrf VPN_A 10.19.19.19

Fri May  8 01:10:46.730 UTC

Routing entry for 10.19.19.19/32
 Known via "local", distance 0, metric 0 (connected)
 Installed May  8 00:46:25.840 for 00:24:20
 Routing Descriptor Blocks
   directly connected, via Loopback100
     Route metric is 0
 No advertising protos.
```

Only once connectivity is established between these new interfaces can the Sham

Link be formed.

```
R2#ping vrf VPN_A 10.19.19.19 source 10.2.2.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 10.19.19.19, timeout is 2 seconds:
 Packet sent with a source address of 10.2.2.2
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/10 ms
 RP/0/0/CPU0:XR1#ping vrf VPN_A 10.2.2.2 source 10.19.19.19

 Fri May  8 01:11:24.677 UTC
 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 9/21/29 ms
```

Similar to a Virtual Link, the Sham Link forms a unicast multi-hop adjacency between the neighbors.

```
R2#show ip ospf 100  neighbor


 Neighbor ID     Pri   State           Dead Time   Address         Interface
 1.1.1.1           1   FULL/DR         00:00:30    10.1.2.1        GigabitEthernet1.12
 19.19.19.19       0   FULL/  -            -       10.19.19.19     OSPF_SL0
 R2#show ip ospf 100 neighbor 19.19.19.19
 Neighbor 19.19.19.19, interface address 10.19.19.19 In the area 0 via interface OSPF_SL0
    Neighbor priority is 0, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x0 in Hello
    Options is 0x72 in DBD (E-bit, L-bit, DC-bit, O-bit)
    LLS Options is 0x1 (LR)
    Neighbor is up for 00:07:42
    Index 2/2, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 R2#show ip ospf 100 sham-links
  Sham Link OSPF_SL0 to address 10.19.19.19 is up
 Area 0 source address 10.2.2.2
   Run as demand circuit
   DoNotAge LSA allowed. Cost of using 1 State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40,
     Hello due in 00:00:04
```

```
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
RP/0/0/CPU0:XR1#show ospf vrf VPN_A neighbor
Fri May  8 01:12:33.992 UTC

* Indicates MADJ interface

Neighbors for OSPF 100, VRF VPN_A

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1     FULL/  -            -         10.2.2.2        OSPF_SL0
   Neighbor is up for 00:08:02
20.20.20.20     1     FULL/DR         00:00:31    10.19.20.20     GigabitEthernet0/0/0/0.1920
   Neighbor is up for 00:06:36

Total neighbor count: 2
RP/0/0/CPU0:XR1#show ospf vrf VPN_A neighbor 10.2.2.2
Fri May  8 01:13:01.381 UTC

* Indicates MADJ interface

Neighbors for OSPF 100, VRF VPN_A

 Neighbor 10.2.2.2, interface address 10.2.2.2 In the area 0 via interface OSPF_SL0

    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x72
    LLS Options is 0x1 (LR)
    Neighbor is up for 00:08:29
    Number of DBD retrans during last exchange 0
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0(0)/0(0) Next 0(0)/0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
    LS Ack list: NSR-sync pending 0, high water mark 0


Total neighbor count: 1
```

From the point of view of the CE routers, the PE routers R2 and XR1 are now all part of the same OSPF area, and hence the same flooding domain. Note that there are no Network Summary LSAs (LSA Type 3) or External LSAs (LSA Type 5) because there are no ABRs or ASBRs. The entire topology is treated as one flat area 0 now.

```
R1#show ip ospf database



            OSPF Router with ID (1.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         600         0x80000003 0x00C87B 3
10.2.2.2        10.2.2.2        681         0x80000003 0x004041 2
19.19.19.19     19.19.19.19     2     (DNA) 0x80000005 0x007177 2
20.20.20.20     20.20.20.20     565         0x80000003 0x00B22B 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.1        1.1.1.1         78          0x80000002 0x00AF63
10.1.20.1       1.1.1.1         600         0x80000001 0x001AA7
10.19.20.20     20.20.20.20     565         0x80000001 0x00AC5B

RP/0/0/CPU0:XR2#show ospf database

Fri May  8 01:16:50.615 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         659         0x80000003 0x00c87b 3
10.2.2.2        10.2.2.2        739         0x80000003 0x004041 2
19.19.19.19     19.19.19.19     623         0x80000005 0x007177 2
20.20.20.20     20.20.20.20     622         0x80000003 0x00b22b 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.1        1.1.1.1         137         0x80000002 0x00af63
10.1.20.1       1.1.1.1         659         0x80000001 0x001aa7
10.19.20.20     20.20.20.20     622         0x80000001 0x00ac5b
```

If we look at this from a route calculation and path selection point of view, R1 now performs a full SPF run over both the backdoor link and over the MPLS L3VPN network in order to reach XR2's Loopback0, and vice versa. R1 simply chooses the lowest cost path to reach XR2, and vice versa, as there is no difference in route types anymore.

Based on the Router LSAs (LSA Type 1) R1 knows that it can reach XR2 with Router-ID 20.20.20.20 two ways, directly over the backdoor link or via the MPLS L3VPN. The SPF cost via the MPLS L3VPN is lower, hence that is the shortest path.

```
R1#show ip ospf database router 1.1.1.1

           OSPF Router with ID (1.1.1.1) (Process ID 100)

               Router Link States (Area 0)

  LS age: 801
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 80000003
  Checksum: 0xC87B
  Length: 60
  Number of Links: 3

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 1.1.1.1
     (Link Data) Network Mask: 255.255.255.255
      Number of MTID metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.1.20.1
     (Link Data) Router Interface address: 10.1.20.1
      Number of MTID metrics: 0 TOS 0 Metrics: 100

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.1.2.1
     (Link Data) Router Interface address: 10.1.2.1
      Number of MTID metrics: 0 TOS 0 Metrics: 1
R1#show ip ospf database router 10.2.2.2



       OSPF Router with ID (1.1.1.1) (Process ID 100)
```

```
           Router Link States (Area 0)

LS age: 935
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 10.2.2.2
Advertising Router: 10.2.2.2
LS Seq Number: 80000003
Checksum: 0x4041
Length: 48
Area Border Router
AS Boundary Router
Number of Links: 2

Link connected to: a Transit Network
(Link ID) Designated Router address: 10.1.2.1
(Link Data) Router Interface address: 10.1.2.2
 Number of MTID metrics: 0
  TOS 0 Metrics: 1

Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 19.19.19.19
(Link Data) Router Interface address: 0.0.0.20
 Number of MTID metrics: 0 TOS 0 Metrics: 1

R1#show ip ospf database router 19.19.19.19

            OSPF Router with ID (1.1.1.1) (Process ID 100)

                Router Link States (Area 0)

  LS age: 2 (DoNotAge)
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 19.19.19.19
  Advertising Router: 19.19.19.19
  LS Seq Number: 80000005
  Checksum: 0x7177
  Length: 48
  Area Border Router
  AS Boundary Router
  Number of Links: 2

    Link connected to: another Router (point-to-point)
     (Link ID) Neighboring Router ID: 10.2.2.2
     (Link Data) Router Interface address: 0.0.0.2
```

```
      Number of MTID metrics: 0 TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.19.20.20
     (Link Data) Router Interface address: 10.19.20.19
      Number of MTID metrics: 0 TOS 0 Metrics: 1

R1#show ip ospf database router 20.20.20.20

            OSPF Router with ID (1.1.1.1) (Process ID 100)

                Router Link States (Area 0)

  LS age: 989
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 20.20.20.20
  Advertising Router: 20.20.20.20
  LS Seq Number: 80000003
  Checksum: 0xB22B
  Length: 60
  Number of Links: 3

    Link connected to: a Stub Network (Link ID) Network/subnet number: 20.20.20.20
     (Link Data) Network Mask: 255.255.255.255
      Number of MTID metrics: 0 TOS 0 Metrics: 1



    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.1.20.1
     (Link Data) Router Interface address: 10.1.20.20
      Number of MTID metrics: 0
       TOS 0 Metrics: 100

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.19.20.20
     (Link Data) Router Interface address: 10.19.20.20
      Number of MTID metrics: 0
       TOS 0 Metrics: 1
```

Notice that the BGP next-hop of routes learned over the Sham-Link is the Sham-Link endpoint, when looking at an IOS-XR device's local OSPF RIB.

```
RP/0/0/CPU0:XR1#show ospf 100 vrf VPN_A routes
```

```
Fri May  8 01:58:19.694 UTC

Topology Table for ospf 100, VRF VPN_A with ID 19.19.19.19

Codes: O - Intra area, O IA - Inter area
       O E1 - External type 1, O E2 - External type 2
       O N1 - NSSA external type 1, O N2 - NSSA external type 2

O    1.1.1.1/32, metric 3 area 0.0.0.0  10.2.2.2, from 1.1.1.1,

O    10.1.2.0/24, metric 2 area 0.0.0.0  10.2.2.2, from 1.1.1.1,

O    10.1.20.0/24, metric 101 area 0.0.0.0
       10.19.20.20, from 1.1.1.1, via GigabitEthernet0/0/0/0.1920
O    10.19.20.0/24, metric 1 area 0.0.0.0
       10.19.20.19, directly connected, via GigabitEthernet0/0/0/0.1920
O    20.20.20.20/32, metric 2 area 0.0.0.0
       10.19.20.20, from 20.20.20.20, via GigabitEthernet0/0/0/0.1920
```

On IOS, the local OSPF RIB displays the Sham-Link interface as the outgoing interface for routes learned over the Sham-Link.

```
R2#show ip ospf 100 rib


            OSPF Router with ID (10.2.2.2) (Process ID 100)


                Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB

*>  1.1.1.1/32, Intra, cost 2, area 0
      via 10.1.2.1, GigabitEthernet1.12
*   10.1.2.0/24, Intra, cost 1, area 0, Connected
      via 10.1.2.2, GigabitEthernet1.12
*>  10.1.20.0/24, Intra, cost 101, area 0
      via 10.1.2.1, GigabitEthernet1.12
*>  10.19.20.0/24, Intra, cost 2, area 0 via 19.19.19.19, OSPF_SL0
*>  20.20.20.20/32, Intra, cost 3, area 0 via 19.19.19.19, OSPF_SL0
```

Although these routes are installed in the RIB via OSPF, they do not get redistributed back into BGP due to them resolving the next-hop/outgoing interface to the Sham-Link.

Proper labeling still takes place, as these routes end up recursing to their corresponding BGP next-hop once they are entered into the FIB. Notice that in IOS's case, the 1.1.1.1/32 prefix is considered a RIB-Failure due to this route being installed via OSPF.

```
R2#show bgp vpnv4 unicast all

 BGP table version is 23, local router ID is 2.2.2.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  r RIB-failure
, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
 RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight Path
 Route Distinguisher: 100:1 (default for vrf VPN_A)
  *>  1.1.1.1/32       10.1.2.1                 2         32768 ?
  *>  10.1.2.0/24      0.0.0.0                  0         32768 ?
  * i 10.1.20.0/24     19.19.19.19            101    100      0 ?
  *>                   10.1.2.1               101         32768 ?
  *>  10.2.2.2/32      0.0.0.0                  0         32768 i
  *>i 10.19.19.19/32   19.19.19.19              0    100      0 i
  r>i 10.19.20.0/24    19.19.19.19              0    100      0 ?
 r>i 20.20.20.20/32   19.19.19.19              2    100      0 ?

 R2#show ip cef vrf VPN_A 20.20.20.20/32 detail
 20.20.20.20/32
, epoch 0, flags [rib defined all labels]
   recursive via 19.19.19.19 label 16007 nexthop 20.2.3.3 GigabitEthernet1.23 label 37
  nexthop 20.2.4.4 GigabitEthernet1.24 label 28
 RP/0/0/CPU0:XR1#show bgp vpnv4 unicast
 advertised  attribute-key
 RP/0/0/CPU0:XR1#show bgp vpnv4 unicast
 Fri May  8 02:08:40.822 UTC
 BGP router identifier 19.19.19.19, local AS number 100
 BGP generic scan interval 60 secs
 BGP table state: Active
 Table ID: 0x0   RD version: 0
 BGP main routing table version 36
 BGP scan interval 60 secs

 Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
*>i1.1.1.1/32         2.2.2.2                  2    100      0 ?
*>i10.1.2.0/24        2.2.2.2                  0    100      0 ?
*> 10.1.20.0/24       10.19.20.20            101         32768 ?
* i                   2.2.2.2                101    100      0 ?
*>i10.2.2.2/32        2.2.2.2                  0    100      0 i
*> 10.19.19.19/32     0.0.0.0                  0         32768 i
*> 10.19.20.0/24      0.0.0.0                  0         32768 ?
*> 20.20.20.20/32     10.19.20.20              2         32768 ?

Processed 7 prefixes, 8 paths
RP/0/0/CPU0:XR1#show cef vrf VPN_A 1.1.1.1/32 detail

Fri May  8 02:08:54.331 UTC 1.1.1.1/32
, version 5, internal 0x14004001 0x0 (ptr 0xa0edc1f4) [1], 0x0 (0x0), 0x208 (0xa13f6280)
 Updated May  8 00:47:24.256
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
  gateway array (0xa0d30040) reference count 3, flags 0x4038, source rib (6), 0 backups
                [1 type 1 flags 0x48089 (0xa1410320) ext 0x0 (0x0)]
  LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0] via 2.2.2.2
, 3 dependencies, recursive [flags 0x6000]
    path-idx 0 NHID 0x0 [0xa145f5f4 0x0]
    next hop VRF - 'default', table - 0xe0000000
    next hop 2.2.2.2 via 16005/0/21 next hop 20.5.19.5/32 Gi0/0/0/0.519 labels imposed {28 21}
 next hop 20.6.19.6/32 Gi0/0/0/0.619 labels imposed {24 21}



    Load distribution: 0 (refcount 1)

    Hash  OK  Interface                 Address
    0     Y   Unknown                   16005/0
```

The final result is that all inter-site traffic goes over the MPLS L3VPN as opposed to the backdoor link.

```
R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.19.20.0/24 [110/3] via 10.1.2.2, 00:20:01, GigabitEthernet1.12
     20.0.0.0/32 is subnetted, 1 subnets
O        20.20.20.20 [110/4] via 10.1.2.2, 00:20:01, GigabitEthernet1.12
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 4 msec 1 msec 1 msec
  2 20.2.4.4 [MPLS: Labels 28/16007 Exp 0] 14 msec 11 msec 12 msec
  3 20.4.5.5 [MPLS: Labels 36/16007 Exp 0] 12 msec 8 msec 8 msec
  4 20.5.19.19 [MPLS: Label 16007 Exp 0] 20 msec 20 msec 20 msec
  5 10.19.20.20 20 msec *  11 msec
  5  10.19.20.20 136 msec * 0 msec
RP/0/0/CPU0:XR2#show route ospf
Fri May  8 01:28:51.456 UTC
O    1.1.1.1/32 [110/4] via 10.19.20.19, 00:22:22, GigabitEthernet0/0/0/0.1920
O    10.1.2.0/24 [110/3] via 10.19.20.19, 00:22:22, GigabitEthernet0/0/0/0.1920
RP/0/0/CPU0:XR2#traceroute 1.1.1.1

Fri May  8 01:29:09.305 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 9 msec  0 msec  0 msec
 2  20.5.19.5 [MPLS: Labels 28/21 Exp 0] 9 msec  0 msec  0 msec
 3  20.4.5.4 [MPLS: Labels 27/21 Exp 0] 0 msec  0 msec  0 msec
 4  10.1.2.2 [MPLS: Label 21 Exp 0] 0 msec  0 msec  0 msec
 5  10.1.2.1 0 msec  *  9 msec
```

If a connection to the MPLS network is lost, traffic will reroute over the backdoor link. Note that this path has a higher OSPF cost than the previous one.

```
RP/0/0/CPU0:XR2#configure

Fri May  8 01:31:38.134 UTCRP/0/0/CPU0:XR2(config)#interface GigabitEthernet0/0/0/0.1920
RP/0/0/CPU0:XR2(config-subif)#shutdown
```

```
RP/0/0/CPU0:XR2(config-subif)#commit
Fri May  8 01:31:48.724 UTC
RP/0/0/CPU0:May  8 01:31:48.754 : ospf[1015]: %ROUTING-OSPF-5-ADJCHG : Process 100,
Nbr 19.19.19.19 on GigabitEthernet0/0/0/0.1920 in area 0 from FULL to DOWN, Neighbor Down: interface down or detache
, vrf default vrfid 0x60000000
RP/0/0/CPU0:May  8 01:31:48.974 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR2(config-subif)#end
RP/0/0/CPU0:May  8 01:31:55.573 : config[65710]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin

RP/0/0/CPU0:XR2#show route ospf
Fri May  8 01:31:59.703 UTC
O    1.1.1.1/32 [110/101] via 10.1.20.1, 00:00:10, GigabitEthernet0/0/0/0.120
O    10.1.2.0/24 [110/101] via 10.1.20.1, 00:00:10, GigabitEthernet0/0/0/0.120

RP/0/0/CPU0:XR2#traceroute 1.1.1.1
Fri May  8 01:32:05.223 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1
 1  10.1.20.1 0 msec  *  0 msec
RP/0/0/CPU0:XR2#

R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.19.20.0/24 [110/3] via 10.1.2.2, 00:01:28, GigabitEthernet1.12
      20.0.0.0/32 is subnetted, 1 subnets
O        20.20.20.20 [110/101] via 10.1.20.20, 00:02:07, GigabitEthernet1.120
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
```

```
1 10.1.20.20 24 msec * 0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3 VPN and OSPF Domain-ID

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **L3VPN Backdoor Links**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **L3VPN Backdoor Links Diagram** in order to complete this task.

- Create a new Loopback1 interface on R1 with the IP address 10.1.1.1/32.
- Create a new Loopback1 interface on XR2 with the IP address 10.20.20.20/32.
- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2 respectively.
- Configure OSPF routing for the VRF as follows:
  - Use Process-ID 100.
  - Enable OSPF Area 0 between R1 & R2.
  - Enable OSPF Area 0 between XR1 & XR2.
  - Enable OSPF Area 120 between R1 & XR2.
  - Advertise the Loopback0 network of R1 into OSPF Area 1.
  - Advertise the Loopback0 network of XR2 into OSPF Area 20.
  - Redistribute the Loopback1 networks of R1 and XR2 into OSPF.
  - Modify the link between R1 and XR2 to have an OSPF cost of 100.
  - Configure the OSPF Domain-ID on R2 and XR1 for the VRF aware process as type 0005 with value 0x000000640200.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 Address Family.
  - Use their Loopback0 interfaces as the source of the BGP session.
  - Redistribute between BGP and the VRF aware OSPF process.

- Once complete, the following reachability should be achieved:
  - R1 and XR2 should have reachability to all of each other’s networks.
  - Traffic between the Loopback0 networks of R1 and XR2 should prefer to use the MPLS network.
  - Traffic between the Loopback1 networks of R1 and XR2 should prefer to use the backdoor link.
  - If either R1 or XR2 lose connectivity to the MPLS cloud or the backdoor link, traffic should be automatically be rerouted accordingly.

Configuration

```
R1:
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet1.120
 ip ospf cost 100
!
ip prefix-list LOOPBACK1 seq 5 permit 10.1.1.1/32
!
route-map CONNECTED_TO_OSPF permit 10
 match ip address prefix-list LOOPBACK1
!
router ospf 100
 redistribute connected subnets route-map CONNECTED_TO_OSPF
 network 1.1.1.1 0.0.0.0 area 1
 network 10.1.2.1 0.0.0.0 area 0
 network 10.1.20.1 0.0.0.0 area 120

R2:
vrf definition VPN_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 !
 address-family ipv4
 exit-address-family
!
interface GigabitEthernet1.12
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
router ospf 100 vrf VPN_A
```

```
 redistribute bgp 100 subnets
 network 10.1.2.2 0.0.0.0 area 0
 domain-id type 0005 value 000000640200
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
!
address-family ipv4 vrf VPN_A
  redistribute ospf 100 vrf VPN_A match internal external 1 external 2
 exit-address-family
!

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target 100:1
 !
  export route-target
   100:1
  !
 !
!
interface GigabitEthernet0/0/0/0.1920
 vrf VPN_A
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
vrf VPN_A
 rd 100:1
```

```
 address-family ipv4 unicast
   redistribute ospf 100
  !
 !
!
router ospf 100
 vrf VPN_A
  domain-id type 0005 value 000000640200
  redistribute bgp 100
  area 0
   interface GigabitEthernet0/0/0/0.1920
   !
  !
 !
!

XR2:
interface Loopback1
 ipv4 address 10.20.20.20 255.255.255.255
!
route-policy CONNECTED_TO_OSPF
 if destination in (10.20.20.20/32) then
    pass
 endif
end-policy
!
router ospf 100
 redistribute connected route-policy CONNECTED_TO_OSPF
  area 0
 interface GigabitEthernet0/0/0/0.1920
 !
!
area 20
 interface Loopback0
 !
!
area 120
 interface GigabitEthernet0/0/0/0.120
   cost 100
  !
 !
!
```

Verification

As previously discussed, the OSPF Domain-ID is encoded as a BGP Extended Community when redistribution of OSPF and VPNv4 BGP occurs. Once redistribution of OSPF and VPNv4 BGP is complete, and VPNv4 routes are exchanged between PE routers, the OSPF Domain-ID of the received BGP routes is compared against the OSPF Domain-ID of the local OSPF process. If these values match, the MPLS network can be treated as the OSPF "Superbackbone", which is considered a hierarchy above Area 0. This allows the PE routers to be treated as ABRs instead of ASBRs, and encode routes that are being redistributed from VPNv4 BGP into OSPF as Network Summary LSAs (LSA Type 3) as opposed to External LSAs (LSA Type 5). Note that this behavior only takes place if the route in question was not already an External route to begin with.

The details about the specific values that are encoded in the OSPF Route Type, OSPF Domain ID, and OSPF Router ID fields of the VPNv4 BGP Extended Communities can be found in RFC 4577: [OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)]().

In regular IOS, the Domain-ID is automatically inherited from the OSPF Process-ID number. In this example a Process-ID of decimal 100 equals a Domain-ID of hexadecimal 0x64. In IOS XR, the Domain-ID is not automatically set, which is why the command domain-id is needed. The actual encoding of the BGP extended community can be seen as follows.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
BGP routing table entry for 100:1:1.1.1.1/32, version 2
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, sourced, best
Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
 OSPF RT:0.0.0.0:3:0 OSPF ROUTER ID:10.1.2.2:0
      mpls labels in/out 32/nolabel
      rx pathid: 0, tx pathid: 0x0
R2#show bgp vpnv4 unicast all 20.20.20.20/32
BGP routing table entry for 100:1:20.20.20.20/32, version 14
Paths: (1 available, best #1, table VPN_A)
  Not advertised to any peer
  Refresh Epoch 1
  Local
```

```
    19.19.19.19 (metric 4) (via default) from 19.19.19.19 (19.19.19.19)
      Origin incomplete, metric 2, localpref 100, valid, internal, best
Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
OSPF RT:0.0.0.0:3:0 OSPF ROUTER ID:19.19.19.19:0
      mpls labels in/out nolabel/16007
      rx pathid: 0, tx pathid: 0x0
```

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32

```
Mon May 11 01:11:36.580 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  9           9
Last Modified: May 11 01:08:08.451 for 00:03:28
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
      Received Label 32
      Origin incomplete, metric 2, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 9
Extended community: OSPF domain-id:0x5:0x000000640200 OSPF route-type:0:3:0x0 OSPF router-id:10.1.2.2 RT:100:1

      Source VRF: VPN_A, Source Route Distinguisher: 100:1
```

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 20.20.20.20/32

```
Mon May 11 01:11:58.998 UTC
BGP routing table entry for 20.20.20.20/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 14          14
    Local Label: 16007
Last Modified: May 11 01:08:36.451 for 00:03:22
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    2.2.2.2
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    2.2.2.2
  Local
    10.19.20.20 from 0.0.0.0 (19.19.19.19)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, redistributed, best, group-best, import-candi
      Received Path ID 0, Local Path ID 1, version 14
```

```
Extended community: OSPF domain-id:0x5:0x000000640200 OSPF route-type:0:3:0x0 OSPF router-id:19.19.19.19 RT:100:1
```

Since the OSPF Domain-ID matches between the local OSPF process and the VPNv4 BGP route, and the OSPF Route Type is 3 (meaning the routes were Inter-Area to begin with), when VPNv4 BGP to OSPF redistribution occurs these routes should be encoded in the database as Network Summary LSAs (LSA Type 3). In other words, the PE routers will be seen as ABRs that are advertising Inter-Area routes.

```
R1#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA     10.19.20.0/24 [110/2] via 10.1.2.2, 00:04:48, GigabitEthernet1.12
O E2     10.20.20.20/32
          [110/20] via 10.1.20.20, 00:04:21, GigabitEthernet1.120
     20.0.0.0/32 is subnetted, 1 subnets
O IA     20.20.20.20 [110/3] via 10.1.2.2, 00:04:20, GigabitEthernet1.12

R1#show ip ospf database

            OSPF Router with ID (10.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        401         0x80000002 0x00F601 1
10.1.2.2        10.1.2.2        402         0x80000002 0x00E210 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.2        10.1.2.2        402         0x80000001 0x00748B
```

```
                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
1.1.1.1         10.1.1.1        462         0x80000001 0x00F535
10.1.20.0       10.1.1.1        462         0x80000001 0x009A12
10.19.20.0      10.1.2.2        320         0x80000001 0x004B30
20.20.20.20     10.1.2.2        292         0x80000001 0x00FD5D

                Summary ASB Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
20.20.20.20     10.1.1.1        292         0x80000001 0x005C1E
<snip>
```
RP/0/0/CPU0:XR2#show route ospf

```
Mon May 11 01:14:13.050 UTC
O IA 1.1.1.1/32 [110/3] via 10.19.20.19, 00:05:36, GigabitEthernet0/0/0/0.1920
O E2 10.1.1.1/32 [110/20] via 10.1.20.1, 00:05:36, GigabitEthernet0/0/0/0.120
O IA 10.1.2.0/24 [110/2] via 10.19.20.19, 00:05:36, GigabitEthernet0/0/0/0.1920
```
RP/0/0/CPU0:XR2#show ospf database

```
Mon May 11 01:14:42.108 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
19.19.19.19     19.19.19.19     366         0x80000002 0x00fe0f 1
20.20.20.20     20.20.20.20     365         0x80000003 0x00be45 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.19.20.19     19.19.19.19     366         0x80000001 0x00d438

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
1.1.1.1         19.19.19.19     393         0x80000001 0x00abbe

10.1.2.0        19.19.19.19     393         0x80000001 0x002b37
10.1.20.0       20.20.20.20     369         0x80000003 0x00abbb
20.20.20.20     20.20.20.20     375         0x80000001 0x009dfd

                Summary ASB Link States (Area 0)
```

```
Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        20.20.20.20     369         0x80000001 0x006911

<snip>
```

When R1 and XR2 make their path selection decision, they now see two possible paths to each other's Loopback0 networks, one via the MPLS L3VPN PE and one via the backdoor link.

```
R1#show ip ospf database summary 20.20.20.20

        OSPF Router with ID (10.1.1.1) (Process ID 100)

            Summary Net Link States (Area 0)

LS age: 441
Options: (No TOS-capability, DC, Downward)
LS Type: Summary Links(Network)
Link State ID: 20.20.20.20 (summary Network Number) Advertising Router: 10.1.2.2
LS Seq Number: 80000001
Checksum: 0xFD5D
Length: 28
Network Mask: /32
    MTID: 0         Metric: 2


            Summary Net Link States (Area 1)

LS age: 440
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 20.20.20.20 (summary Network Number)
Advertising Router: 10.1.1.1
LS Seq Number: 80000001
Checksum: 0x9C40
Length: 28
Network Mask: /32
    MTID: 0         Metric: 3


            Summary Net Link States (Area 120)

LS age: 440
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
```

```
Link State ID: 20.20.20.20 (summary Network Number)
Advertising Router: 10.1.1.1
LS Seq Number: 80000001
Checksum: 0x9C40
Length: 28
Network Mask: /32
    MTID: 0         Metric: 3

LS age: 450
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 20.20.20.20 (summary Network Number) Advertising Router: 20.20.20.20
LS Seq Number: 80000001
Checksum: 0x9DFD
Length: 28
Network Mask: /32
    MTID: 0         Metric: 1
```

```
RP/0/0/CPU0:XR2#show ospf database summary 1.1.1.1
Mon May 11 01:18:36.162 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100)

                Summary Net Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 627
  Options: (No TOS-capability, DC, DN)
  LS Type: Summary Links (Network)
  Link State ID: 1.1.1.1 (Summary Network Number) Advertising Router: 19.19.19.19
  LS Seq Number: 80000001
  Checksum: 0xabbe
  Length: 28
  Network Mask: /32
        TOS: 0  Metric: 2


                Summary Net Link States (Area 20)

  LS age: 599
  Options: (No TOS-capability, DC)
  LS Type: Summary Links (Network)
  Link State ID: 1.1.1.1 (Summary Network Number)
```

```
    Advertising Router: 20.20.20.20
    LS Seq Number: 80000001
    Checksum: 0x1fc6
    Length: 28
    Network Mask: /32
          TOS: 0  Metric: 3


                Summary Net Link States (Area 120)

    LS age: 770
    Options: (No TOS-capability, DC)
    LS Type: Summary Links (Network)
    Link State ID: 1.1.1.1 (Summary Network Number)  Advertising Router: 10.1.1.1

    LS Seq Number: 80000001
    Checksum: 0xf535
    Length: 28
    Network Mask: /32
          TOS: 0  Metric: 1

    LS age: 599
    Options: (No TOS-capability, DC)
    LS Type: Summary Links (Network)
    Link State ID: 1.1.1.1 (Summary Network Number)
    Advertising Router: 20.20.20.20
    LS Seq Number: 80000001
    Checksum: 0x1fc6
    Length: 28
    Network Mask: /32
          TOS: 0  Metric: 3
```

Since these routes are now both the same type (i.e. Type 3 LSA vs. Type 3 LSA) the OSPF cost is the tie breaker. On R1 the shortest path to the ABR 10.1.2.2 (R2) is closer than the shortest path to the ABR 20.20.20.20 (XR2) because the cost of the link to XR2 was increased to 100. Likewise XR2 prefers to route via the ABR 19.19.19.19 (XR1) due to the lower cost. The final result is that traffic between these links follows the MPLS L3VPN path.

```
R1#show ip ospf border-routers


            OSPF Router with ID (10.1.1.1) (Process ID 100)
```

```
                 Base Topology (MTID 0)

Internal Router Routing Table
Codes: i - Intra-area route, I - Inter-area route
 i 20.20.20.20 [100
] via 10.1.20.20, GigabitEthernet1.120, ABR/ASBR, Area 120, SPF 2 i 10.1.2.2 [1
] via 10.1.2.2, GigabitEthernet1.12, ABR/ASBR, Area 0, SPF 3

RP/0/0/CPU0:XR2#show ospf border-routers


Mon May 11 01:19:44.477 UTC


OSPF 100 Internal Routing Table


Codes: i - Intra-area route, I - Inter-area route
 i 10.1.1.1 [100
] via 10.1.20.1, GigabitEthernet0/0/0/0.120, ABR/ASBR , Area 120, SPF 6 i 19.19.19.19 [1
] via 10.19.20.19, GigabitEthernet0/0/0/0.1920, ABR/ASBR , Area 0, SPF 4

R1#traceroute 20.20.20.20 source 1.1.1.1
Type escape sequence to abort.
Tracing the route to 20.20.20.20
VRF info: (vrf in name/id, vrf out name/id) 1 10.1.2.2 4 msec 1 msec 1 msec
  2 20.2.4.4 [MPLS: Labels 21/16007 Exp 0] 14 msec 11 msec 12 msec
  3 20.4.6.6 [MPLS: Labels 22/16007 Exp 0] 12 msec 12 msec 20 msec
  4 20.6.19.19 [MPLS: Label 16007 Exp 0] 20 msec 20 msec 23 msec
  5 10.19.20.20 17 msec *  14 msec

RP/0/0/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
Mon May 11 01:22:30.166 UTC


Type escape sequence to abort.
Tracing the route to 1.1.1.1
 1  10.19.20.19 0 msec  0 msec  0 msec


 2  20.5.19.5 [MPLS: Labels 26/32 Exp 0] 9 msec  9 msec  9 msec
 3  20.4.5.4 [MPLS: Labels 19/32 Exp 0] 9 msec  9 msec  9 msec
 4  10.1.2.2 [MPLS: Label 32 Exp 0] 9 msec  9 msec  9 msec
 5  10.1.2.1 9 msec  *  19 msec
```

Both R1 and XR2 install the path to each other's Loopback0 with a cost of 2. 1 to reach the ABR (as seen in the border-router output), plus 2 as advertised by each ABR's Type-3 LSA.

Note that this conversion process with the OSPF Domain-ID only occurs when the route was first redistributed as an Intra-Area OSPF or Inter-Area OSPF route to being with. In this specific example when R2 redistributes OSPF into BGP, it is learning the route 1.1.1.1/32 as an OSPF Inter-Area route, but it's learning the route 10.1.1.1/32 as an OSPF External route.

```
R2#show ip route vrf VPN_A ospf

 Routing Table: VPN_A
 Codes: L - local, 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, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override

 Gateway of last resort is not set

       1.0.0.0/32 is subnetted, 1 subnets
 O IA     1.1.1.1 [110/2] via 10.1.2.1, 00:19:38, GigabitEthernet1.12
       10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
 O E2     10.1.1.1/32 [110/20] via 10.1.2.1, 00:19:38, GigabitEthernet1.12

 O IA     10.1.20.0/24 [110/101] via 10.1.2.1, 00:19:38, GigabitEthernet1.12
 O E2     10.20.20.20/32 [110/20] via 10.1.2.1, 00:17:48, GigabitEthernet1.12
```

This means that when OSPF to BGP redistribution occurs, R2 will encode the Inter-Area route 1.1.1.1/32 with an OSPF Route Type 3 (meaning the route was Inter-Area to start), but will encode the External route 10.1.1.1/32 with an OSPF Route Type 5 (meaning the route was External to start).

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
 BGP routing table entry for 100:1:1.1.1.1/32, version 2
 Paths: (1 available, best #1, table VPN_A)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   Local
     10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
       Origin incomplete, metric 2, localpref 100, weight 32768, valid, sourced, best
       Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200  OSPF RT:0.0.0.0:3:0
  OSPF ROUTER ID:10.1.2.2:0
       mpls labels in/out 32/nolabel
```

```
      rx pathid: 0, tx pathid: 0x0

R2#show bgp vpnv4 unicast all 10.1.1.1/32
BGP routing table entry for 100:1:10.1.1.1/32, version 3
Paths: (2 available, best #2, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    19.19.19.19 (metric 4) (via default) from 19.19.19.19 (19.19.19.19)
      Origin incomplete, metric 20, localpref 100, valid, internal
      Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200  OSPF RT:0.0.0.0:5:1
 OSPF ROUTER ID:19.19.19.19:0
      mpls labels in/out 24/16016
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  Local
    10.1.2.1 (via vrf VPN_A) from 0.0.0.0 (2.2.2.2)
      Origin incomplete, metric 20, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200  OSPF RT:0.0.0.0:5:1
 OSPF ROUTER ID:10.1.2.2:0
      mpls labels in/out 24/nolabel
      rx pathid: 0, tx pathid: 0x0
```

Notice the difference in the Route-Type Extended Community Attribute of both of these routes. R2 sees 1.1.1.1/32 as an Inter-Area route, and 10.1.1.1/32 as an external route, thus the routes are encoded with Route-Type 0.0.0.0:**3** and 0.0.0.0:**5** respectively. When the routes are learned by the remote PE (XR1) and redistributed from VPNv4 BGP back into OSPF, only the route with both the matching Domain ID and the Route Type of 3 can be advertised as a Network Summary LSA. The External route will remain an External route regardless of any other settings.

In this example this only becomes apparent when the backdoor link between R1 and XR2 is disabled, due to the fact that the PE routers will not re-originate a Type 5 LSA that someone else in their area is already originating.

Below we see that R1 and XR2 prefer to use the backdoor link to reach their Loopback1 networks, which are the External routes that came from **redistribute connected**.

```
R1#show ip route 10.20.20.20
Routing entry for 10.20.20.20/32
  Known via "ospf 100", distance 110, metric 20, type extern 2, forward metric 100
  Last update from 10.1.20.20 on GigabitEthernet1.120, 00:54:14 ago
  Routing Descriptor Blocks:  * 10.1.20.20, from 20.20.20.20, 00:54:14 ago, via GigabitEthernet1.120
```

```
      Route metric is 20, traffic share count is 1
R1#traceroute 10.20.20.20 source 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.20.20.20
 1 10.1.20.20
 4 msec *   0 msec
RP/0/0/CPU0:XR2#show route 10.1.1.1
Mon May 11 02:03:13.408 UTC

Routing entry for 10.1.1.1/32
  Known via "ospf 100", distance 110, metric 20, type extern 2
  Installed May 11 01:08:36.983 for 00:54:36
  Routing Descriptor Blocks 10.1.20.1, from 10.1.1.1, via GigabitEthernet0/0/0/0.120
      Route metric is 20
  No advertising protos.
RP/0/0/CPU0:XR2#traceroute 10.1.1.1 source 10.20.20.20
Fri Mar 16 16:09:35.648 UTC

Type escape sequence to abort.
Tracing the route to 10.1.1.1
 1 10.1.20.1
 5 msec    *   2 msec
```

Once the backdoor link is disabled, then the external route can transit over the MPLS L3VPN.

```
RP/0/0/CPU0:XR2#config
Mon May 11 02:03:59.535 UTCRP/0/0/CPU0:XR2(config)#interface GigabitEthernet0/0/0/0.120
RP/0/0/CPU0:XR2(config-subif)#shutdown

RP/0/0/CPU0:XR2(config-subif)#exit
RP/0/0/CPU0:XR2(config)#commit
Mon May 11 02:04:17.614 UTC
RP/0/0/CPU0:May 11 02:04:17.654 : ospf[1015]: %ROUTING-OSPF-5-ADJCHG : Process 100, Nbr 10.1.1.1 on GigabitEthernet0
RP/0/0/CPU0:May 11 02:04:17.914 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR2(config)#
RP/0/0/CPU0:XR2(config)#end
RP/0/0/CPU0:May 11 02:04:21.683 : config[65710]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin
RP/0/0/CPU0:XR2#
RP/0/0/CPU0:XR2#show route 10.1.1.1
Mon May 11 02:06:06.256 UTC

Routing entry for 10.1.1.1/32
  Known via "ospf 100", distance 110, metric 20
```

```
Tag 3489661028, type extern 2

  Installed May 11 02:04:18.114 for 00:01:48
  Routing Descriptor Blocks 10.19.20.19, from 19.19.19.19, via GigabitEthernet0/0/0/0.1920
      Route metric is 20
  No advertising protos.
RP/0/0/CPU0:XR2#traceroute 10.1.1.1 source 10.20.20.20
Mon May 11 02:06:43.404 UTC

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1  10.19.20.19 0 msec  0 msec  0 msec
 2  20.6.19.6 [MPLS: Labels 25/24 Exp 0] 9 msec  9 msec  0 msec
 3  20.3.6.3 [MPLS: Labels 20/24 Exp 0] 9 msec  0 msec  9 msec
 4  10.1.2.2 [MPLS: Label 24 Exp 0] 9 msec  9 msec  0 msec
 5  10.1.2.1 9 msec  *  9 msec
R1#show ip route 10.20.20.20
Routing entry for 10.20.20.20/32
 Known via "ospf 100", distance 110, metric 20
 Tag Complete, Path Length == 1, AS 100, , type extern 2, forward metric 1
 Last update from 10.1.2.2 on GigabitEthernet1.12, 00:02:04 ago
 Routing Descriptor Blocks: * 10.1.2.2, from 10.1.2.2, 00:02:04 ago, via GigabitEthernet1.12
     Route metric is 20, traffic share count is 1 Route tag 3489661028
R1#traceroute 10.20.20.20 source 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.20.20.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.2.2 5 msec 1 msec 1 msec
  2 20.2.3.3 [MPLS: Labels 24/16017 Exp 0] 11 msec 12 msec 12 msec
  3 20.3.6.6 [MPLS: Labels 22/16017 Exp 0] 12 msec 12 msec 12 msec
  4 20.6.19.19 [MPLS: Label 16017 Exp 0] 16 msec 20 msec 20 msec
  5 10.19.20.20 16 msec *  14 msec
```

Notice that the routes now have a Route-Tag value that was automatically generated. This is a 32 bit tag which is used for loop prevention, similar to the function provided by the OSPF Down Bit, however this tag is only present in External routes injected into the OSPF domain by redistribution from MP-BGP into OSPF by a PE router. When using 16 bit BGP ASNs, as such is the case in our example, the last 16 bits of the 32 bit tag are used to encode the BGP ASN.

XR1 receives a VPNv4 update for 10.1.1.1/32. The route has been advertised by R2, and the Route-Type Extended Community value has been encoded as External

(Type-5) by R2.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast rd 100:1 10.1.1.1/32

 Mon May 11 22:51:35.787 UTC
 BGP routing table entry for 10.1.1.1/32, Route Distinguisher: 100:1
 Versions:
   Process           bRIB/RIB  SendTblVer
   Speaker                 28          28
 Last Modified: May 11 02:27:54.451 for 20:23:41
 Paths: (1 available, best #1)
   Not advertised to any peer
   Path #1: Received by speaker 0
   Not advertised to any peer
   Local
     2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
       Received Label 44
       Origin incomplete, metric 20, localpref 100, valid, internal, best, group-best, import-candidate, imported
       Received Path ID 0, Local Path ID 1, version 28      Extended community:
 OSPF domain-id:0x5:0x000000640200 OSPF route-type:0:5:0x1 OSPF router-id:10.1.2.2 RT:100:1

       Source VRF: VPN_A, Source Route Distinguisher: 100:1
```

This route is then installed in VRF_A by XR1 as a BGP route, causing it to be redistributed into OSPF.

```
RP/0/0/CPU0:XR1#show route vrf VPN_A 10.1.1.1

 Mon May 11 22:51:44.876 UTC

 Routing entry for 10.1.1.1/32
   Known via "bgp 100", distance 200, metric 20, type internal
   Installed May 11 02:27:54.526 for 20:23:50
   Routing Descriptor Blocks
     2.2.2.2, from 2.2.2.2
       Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
       Route metric is 20
   No advertising protos.
```

Since this was an external route that originated from an OSPF domain, the route is tagged.

```
RP/0/0/CPU0:XR1#show ospf 100 vrf VPN_A database external 10.1.1.1
```

```
Mon May 11 23:00:14.191 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 100, VRF VPN_A)

                Type-5 AS External Link States

  LS age: 1502
  Options: (No TOS-capability, DC, DN)
  LS Type: AS External Link
  Link State ID: 10.1.1.1 (External Network Number) Advertising Router: 19.19.19.19
  LS Seq Number: 80000027
  Checksum: 0x7feb
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0 External Route Tag: 3489661028
```

If this OSPF route is then advertised over the backdoor link, the tag will prevent R2 from installing the route, much like the Down Bit.

```
> 3489661028 is the decimal representation of hex value 0xD0000064. The last 2 bytes (16 bits) of this hex value, 0x
```

More information about the tagging mechanism can be found on Section 4.2.5.2 of RFC 4577.

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

Multi-VRF CE (VRF Lite)

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Multi VRF CE**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Multi VRF CE Diagram** in order to complete this task.

- Configure a VRF on R1, R2, R4, XR1, and XR2 as follows:
  - VRF Name: VPN_A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the following links:
    - On both R1 and R2 on the link with the address 10.1.2.0/24
    - On both XR1 and XR2 on the link with the address 10.19.20.0/24
    - On R1's link to R3
    - On R4's link to R7
    - On XR2's link to R6
- Configure a VRF on R1, R2, R5, XR1, and XR2 as follows:
  - VRF Name: VPN_B
  - Route Distinguisher: 100:2
  - Route Target Import: 100:2
  - Route Target Export: 100:2
  - Assign the VRF to the following links:
    - On both R1 and R2 on the link with the address 30.1.2.0/24
    - On both XR1 and XR2 on the link with the address 30.19.20.0/24
    - On R1's link to R9
    - On R5's link to R8
    - On XR2's link to R9
- Configure OSPF routing for VRF VPN_A as follows:
  - R3, R6, and R7 are preconfigured with OSPF.

    - Configure OSPF Process-ID 100 on R1, R2, R4, XR1, and XR2.
    - Enable this OSPF process on all links in VRF VPN_A.
    - Configure the OSPF Domain-ID on XR1 as type 0005 with value 0x000000640200.
    - Configure the VRF aware OSPF process of R1 and XR2 to ignore the OSPF Down Bit in Type 3 LSAs.
- Configure RIP routing for VRF VPN_B as follows:
    - R8 and R9 are preconfigured with RIP.
    - Configure RIPv2 on R1, R2, R5, XR1, and XR2.
    - Enable this RIP process on all links in VRF VPN_B.
- Configure BGP on R2, R4, R5, and XR1 as follows:
    - Use BGP AS 100.
    - Configure a full mesh of iBGP VPNv4 peerings between the PE routers.
    - Use their Loopback0 interfaces as the source of the BGP sessions.
    - Redistribute between the VRF aware OSPF process and VPNv4 BGP.
    - Redistribute between the VRF aware RIP process and VPNv4 BGP.
- Once complete, the following reachability should be achieved:
    - R3, R6, and R7 should have full reachability to all networks in VRF VPN_A.
    - R8 and R9 should have full reachability to all networks in VRF VPN_B.

Configuration

```
R1:
vrf definition VPN_A
 rd 100:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition VPN_B
 rd 100:2
 !
 address-family ipv4
exit-address-family
!
interface GigabitEthernet1.13
 vrf forwarding VPN_A
 ip address 10.1.3.1 255.255.255.0
!
interface GigabitEthernet1.112
 vrf forwarding VPN_A
```

```
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet1.120
 vrf forwarding VPN_B
 ip address 30.1.20.1 255.255.255.0
!
interface GigabitEthernet1.212
 vrf forwarding VPN_B
 ip address 30.1.2.1 255.255.255.0
!
router ospf 100 vrf VPN_A
capability vrf-lite
network 0.0.0.0 255.255.255.255 area 0
!
router rip
 !
address-family ipv4 vrf VPN_B
 network 30.0.0.0
 no auto-summary
 version 2
exit-address-family
!

R2:
vrf definition VPN_A
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
vrf definition VPN_B
 rd 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
!
interface GigabitEthernet1.112
 vrf forwarding VPN_A
 ip address 10.1.2.2 255.255.255.0
!
interface GigabitEthernet1.212
 vrf forwarding VPN_B
```

```
 ip address 30.1.2.2 255.255.255.0
!
router ospf 100 vrf VPN_A
 redistribute bgp 100 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router rip
 !
address-family ipv4 vrf VPN_B
 redistribute bgp 100 metric 5
 network 30.0.0.0
 no auto-summary
 version 2
exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 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 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 redistribute ospf 100 vrf VPN_A
exit-address-family
!
address-family ipv4 vrf VPN_B
redistribute rip
exit-address-family
!

R4:
vrf definition VPN_A
 rd 100:1
 !
```

```
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
interface GigabitEthernet1.47
 vrf forwarding VPN_A
 ip address 10.4.7.4 255.255.255.0
!
router ospf 100 vrf VPN_A
 redistribute bgp 100 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 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 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 no synchronization
 redistribute ospf 100 vrf VPN_A match internal external 1 external 2
exit-address-family

R5:
vrf definition VPN_B
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
```

```
!
interface GigabitEthernet1.58
 vrf forwarding VPN_B
 ip address 30.5.8.5 255.255.255.0
!
router rip
 !
 address-family ipv4 vrf VPN_B
  redistribute bgp 100 metric 5
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 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 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 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
!
 address-family ipv4 vrf VPN_B
  no synchronization
  redistribute rip
 exit-address-family
!

XR1:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
```

```
  !
 !
!
vrf VPN_B
 address-family ipv4 unicast
  import route-target
   100:2
  !
  export route-target
   100:2
  !
 !
!
interface GigabitEthernet0/0/0/0.11920
 vrf VPN_A
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0
!
interface GigabitEthernet0/0/0/0.21920
 vrf VPN_B
 no ipv4 address
 ipv4 address 30.19.20.19 255.255.255.0
!
route-policy BGP_TO_RIP
 set rip-metric 5
end-policy
!
router ospf 100
 vrf VPN_A
  domain-id type 0005 value 000000640200
  redistribute bgp 100
  area 0
   interface GigabitEthernet0/0/0/0.11920
   !
  !
 !
!
router bgp 100
 address-family vpnv4 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
```

```
 neighbor 4.4.4.4
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
neighbor 5.5.5.5
 remote-as 100
 update-source Loopback0
 address-family vpnv4 unicast
 !
!
vrf VPN_A
 rd 100:1
 address-family ipv4 unicast
   redistribute ospf 100
!
!
vrf VPN_B
 rd 100:2
 address-family ipv4 unicast
   redistribute rip
  !
 !
!
router rip
 vrf VPN_B
  interface GigabitEthernet0/0/0/0.21920
  !
  redistribute bgp 100 route-policy BGP_TO_RIP
 !
!

XR2:
vrf VPN_A
 address-family ipv4 unicast
 !
!
vrf VPN_B
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/0.120
 vrf VPN_B
 no ipv4 address
 ipv4 address 30.1.20.20 255.255.255.0
```

```
!
interface GigabitEthernet0/0/0/0.620
 vrf VPN_A
 no ipv4 address
 ipv4 address 10.6.20.20 255.255.255.0
!
interface GigabitEthernet0/0/0/0.11920
 vrf VPN_A
 no ipv4 address
 ipv4 address 10.19.20.20 255.255.255.0
!
interface GigabitEthernet0/0/0/0.21920
 vrf VPN_B
 no ipv4 address
 ipv4 address 30.19.20.20 255.255.255.0
!
router ospf 100
 vrf VPN_A
 disable-dn-bit-check
 area 0
   interface GigabitEthernet0/0/0/0.620
   !
   interface GigabitEthernet0/0/0/0.11920
   !
  !
 !
!
router rip
 vrf VPN_B
  interface GigabitEthernet0/0/0/0.120
  !
  interface GigabitEthernet0/0/0/0.21920
  !
  redistribute bgp 100
 !
!
```

Verification

The Multi VRF CE feature, or what is more commonly referred to as “VRF Lite”, simply means that the router has been configured with multiple Virtual Routing and Forwarding instances (VRFs), but does not have MPLS or VPNv4 BGP configured. Typically this configuration is used to separate a single router or switch into multiple logical devices, as interfaces assigned to different VRF tables are then independent of each other. A common practical application of this feature is for managed CE devices that connect to multiple customers. For example a service provider may service multiple customers in the same office building, with their connections from the PE to CE aggregated by the managed CE.

Configuration of this feature is identical to the other L3VPN configs that have been done up to this point, with the exception that the BGP and MPLS portions are left out. As we see below on R1 and XR2, there are two separate VRFs configured to service VPN_A and VPN_B. Note that no Route Target import or export policies are configured on R1 or XR2, nor is the Route Distinguisher value set on XR2. These values can be configured, but are not needed, since they are only relevant within the scope of VPNv4 BGP.

```
R1#show ip vrf detail
VRF VPN_A (VRF Id = 1); default RD 100:1; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces:
    Gi1.13                   Gi1.112
Address family ipv4 unicast (Table ID = 0x1):
  Flags: 0x0 No Export VPN route-target communities
 No Import VPN route-target communities
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

VRF VPN_B (VRF Id = 2); default RD 100:2; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces:
    Gi1.120                  Gi1.212
Address family ipv4 unicast (Table ID = 0x2):
  Flags: 0x0 No Export VPN route-target communities
 No Import VPN route-target communities
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
RP/0/0/CPU0:XR2#show vrf all detail
Tue May 12 00:04:13.658 UTC

VRF **nVSatellite; RD not set; VPN ID not set
```

```
VRF mode: Regular
Description not set
Interfaces:
  nV-Loopback0
Address family IPV4 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy

VRF VPN_A; RD not set; VPN ID not set
VRF mode: Regular
Description not set
Interfaces:
  GigabitEthernet0/0/0/0.620
  GigabitEthernet0/0/0/0.11920
Address family IPV4 Unicast No import VPN route-target communities
 No export VPN route-target communities
  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy

VRF VPN_B; RD not set; VPN ID not set
VRF mode: Regular
Description not set
Interfaces:
  GigabitEthernet0/0/0/0.120
  GigabitEthernet0/0/0/0.21920
Address family IPV4 Unicast No import VPN route-target communities
 No export VPN route-target communities

  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
```

```
No export route policy
```

One of the potential design problems with this configuration (VRFs without MPLS/BGP) specifically relates to how the OSPF loop prevention process changes when a VRF aware OSPF process is used as opposed to a process in the global routing table.

Per RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs), loop prevention of VRF aware OSPF is enhanced by adding a new bit in the LSA Options field known as the “Down Bit” or the DN Bit, and by adding an automatically derived route tag. The Down Bit is set in OSPF when a PE router redistributes VPNv4 BGP into OSPF and originates a Type 3 Network Summary LSA (an Inter-Area route). For Type 5 External LSAs (an E1 or E2 route) a VPN Route Tag value is used in place of the Down Bit, but essentially serves the same purpose. The goal of the addition of the Down Bit is to use it determine if an OSPF route was originated from the local customer site or a remote customer site. Note that on current version of IOS and IOS-XR, such as the versions used during these labs, the DN bit is set in both Type-3 and Type-5 LSA - more closely following the RFC. The DN bit was only set on Type-3 LSAs in previous versions.

Since the Down Bit is set when a Type-3 or Type-5 LSA is generated during VPNv4 BGP to OSPF redistribution, and only routes originated by a remote customer site would have been redistributed from VPNv4 BGP into OSPF, the Down Bit can then be used to figure out if the route is from the local site or a remote site. Feedback loops can then be prevented for routes being redistributed from VPNv4 BGP to OSPF, then from OSPF back to VPNv4 BGP, then from VPNv4 BGP back to OSPF, etc. by using the Down Bit as an indicator if the route should be candidate for redistribution or not. From an implementation point of view the Down Bit is specifically used to control whether a route in the OSPF database can be installed in the routing table.

If the local router is running the VRF aware OSPF process, it is assumed that this router is a PE that is doing OSPF to VPNv4 BGP redistribution, as this is normally the default design logic of VRFs since they are used for MPLS L3VPN applications. In this case, it is advantageous to prevent received routes with the Down Bit set to be installed in the routing table, mitigating the possibility of redistributing the route into another protocol. The problem with this default logic though is that in the application of VRF Lite (i.e. Multi VRF CE), the router is not performing OSPF to VPNv4 BGP redistribution, and hence this native loop prevention mechanism is not needed.

In this example, the Down Bit loop prevention must be disabled on the Multi VRF CEs of R1 and XR2, otherwise they will not install Type 3 or Type 5 LSAs that are advertised by PE routers R2 and XR1. All of the Type-3 and Type-5 LSAs currently advertised by R2 and XR1 have the DN bit set, as they are routes that originated from another OSPF domain. This is what the commands **capability vrf-lite** and **disable-dn-bit-check** do under the VRF aware OSPF processes of IOS and IOS XR respectively. In the below output we see the final result of this configuration, where the VRF VPN_A and VPN_B tables are fully populated everywhere.

```
R3#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      6.0.0.0/32 is subnetted, 1 subnets
O IA     6.6.6.6 [110/5] via 10.1.3.1, 00:01:14, GigabitEthernet1.13
      7.0.0.0/32 is subnetted, 1 subnets
O E2     7.7.7.7 [110/20] via 10.1.3.1, 00:03:35, GigabitEthernet1.13
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O        10.1.2.0/24 [110/2] via 10.1.3.1, 00:45:54, GigabitEthernet1.13
O IA     10.4.7.0/24 [110/3] via 10.1.3.1, 00:03:35, GigabitEthernet1.13
O IA     10.6.20.0/24 [110/4] via 10.1.3.1, 00:01:14, GigabitEthernet1.13
O IA     10.7.7.7/32 [110/4] via 10.1.3.1, 00:03:35, GigabitEthernet1.13
O IA     10.19.20.0/24 [110/3] via 10.1.3.1, 00:01:14, GigabitEthernet1.13
R6#show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/5] via 10.6.20.20, 00:01:34, GigabitEthernet1.620
      7.0.0.0/32 is subnetted, 1 subnets
```

```
O E2     7.7.7.7 [110/20] via 10.6.20.20, 00:23:00, GigabitEthernet1.620
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA     10.1.2.0/24 [110/3] via 10.6.20.20, 00:01:34, GigabitEthernet1.620
O IA     10.1.3.0/24 [110/4] via 10.6.20.20, 00:01:34, GigabitEthernet1.620
O IA     10.4.7.0/24 [110/3] via 10.6.20.20, 00:01:34, GigabitEthernet1.620
O IA     10.7.7.7/32 [110/4] via 10.6.20.20, 00:01:34, GigabitEthernet1.620
O        10.19.20.0/24 [110/2] via 10.6.20.20, 00:41:44, GigabitEthernet1.620
R7#show ip route ospf

Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/4] via 10.4.7.4, 00:04:15, GigabitEthernet1.47
      6.0.0.0/32 is subnetted, 1 subnets
O IA     6.6.6.6 [110/4] via 10.4.7.4, 00:01:54, GigabitEthernet1.47
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA     10.1.2.0/24 [110/2] via 10.4.7.4, 00:04:20, GigabitEthernet1.47
O IA     10.1.3.0/24 [110/3] via 10.4.7.4, 00:04:15, GigabitEthernet1.47
O IA     10.6.20.0/24 [110/3] via 10.4.7.4, 00:01:54, GigabitEthernet1.47
O IA     10.19.20.0/24 [110/2] via 10.4.7.4, 00:01:54, GigabitEthernet1.47
```

The key prefixes to check reachability are networks 7.7.7.7/32 and 10.7.7.7/32, both of which are being originated by R7.

```
R3#show ip route 7.7.7.7
Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20  Tag Complete, Path Length == 1, AS 100, , type extern 2
, forward metric 2
  Last update from 10.1.3.1 on GigabitEthernet1.13, 00:05:01 ago
  Routing Descriptor Blocks:
  * 10.1.3.1, from 10.1.2.2, 00:05:01 ago, via GigabitEthernet1.13
      Route metric is 20, traffic share count is 1 Route tag 3489661028
R3#show ip route 10.7.7.7
Routing entry for 10.7.7.7/32  Known via "ospf 100", distance 110, metric 4, type inter area
```

```
  Last update from 10.1.3.1 on GigabitEthernet1.13, 00:05:31 ago
  Routing Descriptor Blocks:
  * 10.1.3.1, from 10.1.2.2, 00:05:31 ago, via GigabitEthernet1.13
      Route metric is 4, traffic share count is 1
R3#ping 7.7.7.7 source 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 3.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/25 ms
R3#ping 10.7.7.7 source 3.3.3.3


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 3.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/19 ms
```

The first prefix, 7.7.7.7/32, is a Type 5 External LSA that is being originated by R7.

```
R7#show ip ospf database external 7.7.7.7

            OSPF Router with ID (10.7.7.7) (Process ID 100)

                Type-5 AS External Link States

  LS age: 1636
  Options: (No TOS-capability, DC, Upward)
  LS Type: AS External Link
  Link State ID: 7.7.7.7 (External Network Number ) Advertising Router: 10.7.7.7

  LS Seq Number: 80000002
  Checksum: 0xB4AF
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

R7’s PE (R4) takes this OSPF route and redistributes it into VPNv4 BGP. Since the route is external to start, it is encoded with the OSPF Route Type of 5 for external.

```
R4#show bgp vpnv4 unicast all 7.7.7.7/32
BGP routing table entry for 100:1:7.7.7.7/32, version 2
Paths: (1 available, best #1, table VPN_A)
 Advertised to update-groups:
    1
 Refresh Epoch 1
 Local
   10.4.7.7 (via vrf VPN_A) from 0.0.0.0 (4.4.4.4)
     Origin incomplete, metric 20, localpref 100, weight 32768, valid, sourced, best
     Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
OSPF RT:0.0.0.0:5:1 OSPF ROUTER ID:10.4.7.4:0

     mpls labels in/out 36/nolabel
     rx pathid: 0, tx pathid: 0x0
```

When the remote PEs of R2 and XR1 redistribute VPNv4 BGP back into OSPF, they originate this route into the database as a Type 5 External LSA, and set both the DN Bit and VPN Route Tag. On previous versions of IOS, only the VPN Route Tag would have been set on this LSA.

```
R2#show ip ospf 100 database external 7.7.7.7

            OSPF Router with ID (10.1.2.2) (Process ID 100)
 Type-5 AS External Link States

  LS age: 574  Options: (No TOS-capability, DC, Downward
)
  LS Type: AS External Link
  Link State ID: 7.7.7.7 (External Network Number )
  Advertising Router: 10.1.2.2
  LS Seq Number: 80000004
  Checksum: 0xE5D6
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 0.0.0.0 External Route Tag: 3489661028
RP/0/0/CPU0:XR1#show ospf vrf VPN_A database external 7.7.7.7
Tue May 12 00:43:39.206 UTC


            OSPF Router with ID (19.19.19.19) (Process ID 100, VRF VPN_A)
```

```
 Type-5 AS External Link States

  LS age: 462  Options: (No TOS-capability, DC, DN
)
  LS Type: AS External Link
  Link State ID: 7.7.7.7 (External Network Number)
  Advertising Router: 19.19.19.19
  LS Seq Number: 80000003
  Checksum: 0x2858
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0 External Route Tag: 3489661028
```

This value 3489661028 is where the BGP AS number of the PE router is encoded. Converted to hexadecimal this number is 0xD0000064. The last two bytes, 0x0064, is the BGP AS number of the PE router, which is specifically AS 100 in this case. This value is then used for loop prevention where the OSPF route will not be redistributed back into VPNv4 BGP if the destination BGP AS number is 100. However, since the Multi VRF CEs of R1 and XR2 are not doing OSPF to VPNv4 BGP redistribution, this value is not examined, and the prefix can be installed without any issues. This can be seen below as both routers have the route installed and can reach it.

```
R1#show ip route vrf VPN_A 7.7.7.7

 Routing Table: VPN_A
 Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20
  Tag Complete, Path Length == 1, AS 100, , type extern 2, forward metric 1
  Last update from 10.1.2.2 on GigabitEthernet1.112, 00:11:27 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 00:11:27 ago, via GigabitEthernet1.112
      Route metric is 20, traffic share count is 1 Route tag 3489661028
 R1#ping vrf VPN_A 7.7.7.7

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
 !!!!! Success rate is 100 percent
  (5/5), round-trip min/avg/max = 1/6/19 ms
 RP/0/0/CPU0:XR2#show route vrf VPN_A 7.7.7.7/32
```

```
Tue May 12 00:45:31.959 UTC

Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20 Tag 3489661028
, type extern 2
  Installed May 12 00:14:30.716 for 00:31:01
  Routing Descriptor Blocks
    10.19.20.19, from 19.19.19.19, via GigabitEthernet0/0/0/0.11920
      Route metric is 20
  No advertising protos.
RP/0/0/CPU0:XR2#ping vrf VPN_A 7.7.7.7
Fri Mar 16 21:13:23.650 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
!!!!! Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/11/29 ms
```

The second prefix that is generated by R7, 10.7.7.7/32, is advertised as a normal internal OSPF route in Area 0.

```
R7#show ip ospf database router 10.7.7.7

            OSPF Router with ID (10.7.7.7) (Process ID 100)

                Router Link States (Area 0)

  LS age: 1264
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.7.7.7
  Advertising Router: 10.7.7.7
  LS Seq Number: 80000005
  Checksum: 0x284
  Length: 48
  AS Boundary Router
  Number of Links: 2

    Link connected to: a Stub Network (Link ID) Network/subnet number: 10.7.7.7
 (Link Data) Network Mask: 255.255.255.255

      Number of MTID metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.4.7.7
```

```
      (Link Data) Router Interface address: 10.4.7.7
       Number of MTID metrics: 0
        TOS 0 Metrics: 1
```

This means that when R7's PE router, R4, redistributes OSPF into BGP, the OSPF Route Type is set to 2, as this route is learned via the Type 2 LSA that the DR on the Ethernet link between R4 and R7 is generating.

```
R4#show bgp vpnv4 unicast all 10.7.7.7/32
BGP routing table entry for 100:1:10.7.7.7/32, version 4
Paths: (1 available, best #1, table VPN_A)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    10.4.7.7 (via vrf VPN_A) from 0.0.0.0 (4.4.4.4)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.4.7.4:0

      mpls labels in/out 34/nolabel
      rx pathid: 0, tx pathid: 0x0
```

When the remote PEs R2 and XR1 receive this VPNv4 route, they have to decide if they are going to encode it as a Type 3 LSA (Inter-Area route) or a Type 5 LSA (External route). As previously discussed, the route can be encoded as Type 3 if it was an Intra-Area or Inter-Area route to begin with, which the OSPF Route Type field tells us, and if the OSPF Domain-ID of the VPNv4 route matches the local OSPF process. In the case of R2 and XR1 both of these checks pass, and the route is then redistributed as a Type 3 LSA (Inter Area route). Note that when this origination occurs, the OSPF Down Bit is set in the LSA Options field.

```
R2#show bgp vpnv4 unicast all 10.7.7.7/32
BGP routing table entry for 100:1:10.7.7.7/32, version 13
Paths: (1 available, best #1, table VPN_A)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    4.4.4.4 (metric 2) (via default) from 4.4.4.4 (4.4.4.4)
      Origin incomplete, metric 2, localpref 100, valid, internal, best
      Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x000000640200
OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.4.7.4:0
      mpls labels in/out nolabel/34
      rx pathid: 0, tx pathid: 0x0
```

```
R2#show ip ospf 100 database summary 10.7.7.7



            OSPF Router with ID (10.1.2.2) (Process ID 100)
 Summary Net Link States (Area 0)


  LS age: 944  Options: (No TOS-capability, DC, Downward
)
  LS Type: Summary Links(Network)
  Link State ID: 10.7.7.7 (summary Network Number)
  Advertising Router: 10.1.2.2
  LS Seq Number: 80000004
  Checksum: 0x2960
  Length: 28
  Network Mask: /32
        MTID: 0         Metric: 2
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 10.7.7.7/32
Tue May 12 00:49:45.511 UTC
BGP routing table entry for 10.7.7.7/32, Route Distinguisher: 100:1
Versions:
 Process           bRIB/RIB  SendTblVer
 Speaker                 37          37
Last Modified: May 12 00:14:30.451 for 00:35:15
Paths: (1 available, best #1)
 Not advertised to any peer
 Path #1: Received by speaker 0
 Not advertised to any peer
 Local
   4.4.4.4 (metric 3) from 4.4.4.4 (4.4.4.4)
     Received Label 34
     Origin incomplete, metric 2, localpref 100, valid, internal, best, group-best, import-candidate, imported
     Received Path ID 0, Local Path ID 1, version 37
 Extended community: OSPF domain-id:0x5:0x000000640200 OSPF route-type:0:2:0x0 OSPF router-id:10.4.7.4 RT:100:1


     Source VRF: VPN_A, Source Route Distinguisher: 100:1



RP/0/0/CPU0:XR1#show ospf 100 vrf VPN_A database summary 10.7.7.7
Tue May 12 00:50:41.917 UTC



            OSPF Router with ID (19.19.19.19) (Process ID 100, VRF VPN_A)
 Summary Net Link States (Area 0)


  LS age: 885 Options: (No TOS-capability, DC, DN
)
```

```
  LS Type: Summary Links (Network)
  Link State ID: 10.7.7.7 (Summary Network Number)
  Advertising Router: 19.19.19.19
  LS Seq Number: 80000001
  Checksum: 0x6fdf
  Length: 28
  Network Mask: /32
        TOS: 0  Metric: 2
```

The Multi VRF CE routers R1 and XR2 now learn these Type 3 LSAs. Since the Down Bit is manually being ignored, the routes *can* be installed in the routing table.

```
R1#show ip route vrf VPN_A 10.7.7.7

Routing Table: VPN_A
Routing entry for 10.7.7.7/32  Known via "ospf 100", distance 110, metric 3, type inter area
  Last update from 10.1.2.2 on GigabitEthernet1.112, 00:17:43 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 00:17:43 ago, via GigabitEthernet1.112
      Route metric is 3, traffic share count is 1

R1#show ip ospf 100 database summary 10.7.7.7

            OSPF Router with ID (10.1.3.1) (Process ID 100)
 Summary Net Link States (Area 0)

  LS age: 1079 Options : (No TOS-capability, DC, Downward
)
  LS Type: Summary Links(Network)
  Link State ID: 10.7.7.7 (summary Network Number)
  Advertising Router: 10.1.2.2
  LS Seq Number: 80000004
  Checksum: 0x2960
  Length: 28
  Network Mask: /32
        MTID: 0        Metric: 2

R1#ping vrf VPN_A 10.7.7.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!! Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/5/19 ms
RP/0/0/CPU0:XR2#show route vrf VPN_A 10.7.7.7/32
```

```
Tue May 12 00:52:19.581 UTC

Routing entry for 10.7.7.7/32  Known via "ospf 100", distance 110, metric 3, type inter area
  Installed May 12 00:35:56.178 for 00:16:23
  Routing Descriptor Blocks
    10.19.20.19, from 19.19.19.19, via GigabitEthernet0/0/0/0.11920
      Route metric is 3
  No advertising protos.
RP/0/0/CPU0:XR2#show ospf vrf VPN_A database summary 10.7.7.7
Tue May 12 00:52:41.529 UTC


            OSPF Router with ID (20.20.20.20) (Process ID 100, VRF VPN_A)
 Summary Net Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 1006 Options: (No TOS-capability, DC, DN
)
  LS Type: Summary Links (Network)
  Link State ID: 10.7.7.7 (Summary Network Number)
  Advertising Router: 19.19.19.19
  LS Seq Number: 80000001
  Checksum: 0x6fdf
  Length: 28
  Network Mask: /32
        TOS: 0  Metric: 2

RP/0/0/CPU0:XR2#ping vrf VPN_A 10.7.7.7
Tue May 12 00:54:13.963 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!! Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/5/9 ms
```

If we were to revert back to the default behavior of using the Down Bit for filtering, these prefixes would still be advertised on to the C routers R3 and R6, but they would not actually be able to reach them, as the Multi VRF CE routers R1 and XR2 would not install them in the routing table. This can be demonstrated as follows.

Note that currently both Inter-Area and External (Type-3 and Type-5) are installed in the RIB. Both of these routes have the DN bit set as previously shown.

```
R1#show ip route vrf VPN_A 10.7.7.7

Routing Table: VPN_A
Routing entry for 10.7.7.7/32
```

```
  Known via "ospf 100", distance 110, metric 3, type inter area

  Last update from 10.1.2.2 on GigabitEthernet1.112, 00:22:57 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 00:22:57 ago, via GigabitEthernet1.112
      Route metric is 3, traffic share count is 1
R1#show ip route vrf VPN_A 7.7.7.7



Routing Table: VPN_A
Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20  Tag Complete, Path Length == 1, AS 100, , type extern 2
, forward metric 1
  Last update from 10.1.2.2 on GigabitEthernet1.112, 00:23:04 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 00:23:04 ago, via GigabitEthernet1.112
      Route metric is 20, traffic share count is 1
      Route tag 3489661028




R1#config t
Enter configuration commands, one per line. End with CNTL/Z.R1(config)#router ospf 100 vrf VPN_A
R1(config-router)#no capability vrf-lite
R1(config-router)#end
R1#
%OSPF-5-ADJCHG: Process 100, Nbr 10.1.2.2 on GigabitEthernet1.112 from FULL to DOWN, Neighbor Down: Interface down o
%OSPF-5-ADJCHG: Process 100, Nbr 3.3.3.3 on GigabitEthernet1.13 from FULL to DOWN, Neighbor Down: Interface down or
%OSPF-5-ADJCHG: Process 100, Nbr 10.1.2.2 on GigabitEthernet1.112 from LOADING to FULL, Loading Done
%OSPF-5-ADJCHG: Process 100, Nbr 3.3.3.3 on GigabitEthernet1.13 from LOADING to FULL, Loading Done
R1#R1#show ip route vrf VPN_A 10.7.7.7

Routing Table: VPN_A
% Subnet not in table
R1#show ip route vrf VPN_A 7.7.7.7

Routing Table: VPN_A
% Subnet not in table
R3#show ip route 10.7.7.7
Routing entry for 10.7.7.7/32  Known via "ospf 100", distance 110, metric 4, type inter area
  Last update from 10.1.3.1 on GigabitEthernet1.13, 00:26:24 ago
  Routing Descriptor Blocks:  * 10.1.3.1, from 10.1.2.2, 00:26:24 ago, via GigabitEthernet1.13
      Route metric is 4, traffic share count is 1
R3#show ip route 7.7.7.7
Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20
```

```
  Tag Complete, Path Length == 1, AS 100, , type extern 2
, forward metric 2
  Last update from 10.1.3.1 on GigabitEthernet1.13, 00:26:29 ago
  Routing Descriptor Blocks:  * 10.1.3.1, from 10.1.2.2, 00:26:29 ago, via GigabitEthernet1.13

      Route metric is 20, traffic share count is 1
      Route tag 3489661028
```

R3 is still learning the routes, as the LSAs are flooded throughout the area, but R1 doesn't have them installed in the routing table. The result is that R3 forwards packets which are dropped by R1, causing a traffic black-hole.

```
R3#debug ip icmp
ICMP packet debugging is onR3#ping 10.7.7.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
U ICMP: dst (10.1.3.3) host unreachable rcv from 10.1.3.1.U
ICMP: dst (10.1.3.3) host unreachable rcv from 10.1.3.1.U Success rate is 0 percent
 (0/5)
R3#
ICMP: dst (10.1.3.3) host unreachable rcv from 10.1.3.1
```

Likewise, the same would occur on R6 if XR2 reverted back to its default behavior of checking the Down Bit. This can be seen as follows.

```
RP/0/0/CPU0:XR2#show route vrf VPN_A 10.7.7.7
Tue May 12 01:02:55.237 UTC

Routing entry for 10.7.7.7/32  Known via "ospf 100", distance 110, metric 3, type inter area
  Installed May 12 00:35:56.178 for 00:26:59
  Routing Descriptor Blocks
    10.19.20.19, from 19.19.19.19, via GigabitEthernet0/0/0/0.11920
      Route metric is 3
  No advertising protos.
RP/0/0/CPU0:XR2#show route vrf VPN_A 7.7.7.7

Tue May 12 01:02:59.867 UTC

Routing entry for 7.7.7.7/32
  Known via "ospf 100", distance 110, metric 20  Tag 3489661028, type extern 2
  Installed May 12 00:14:30.716 for 00:48:29
  Routing Descriptor Blocks
    10.19.20.19, from 19.19.19.19, via GigabitEthernet0/0/0/0.11920
      Route metric is 20
```

```
  No advertising protos.

RP/0/0/CPU0:XR2#config t
Tue May 12 01:04:19.321 UTCRP/0/0/CPU0:XR2(config)#router ospf 100
RP/0/0/CPU0:XR2(config-ospf)#vrf VPN_A
RP/0/0/CPU0:XR2(config-ospf-vrf)#no disable-dn-bit-check
RP/0/0/CPU0:XR2(config-ospf-vrf)#commit
Tue May 12 01:04:22.321 UTC
RP/0/0/CPU0:May 12 01:04:22.681 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR2#show route vrf VPN_A 10.7.7.7
Tue May 12 01:04:50.689 UTC
% Network not in table
RP/0/0/CPU0:XR2#show route vrf VPN_A 7.7.7.7
Tue May 12 01:04:55.049 UTC
% Network not in table
```

Now that XR2 no longer installs the routes in the routing table, traffic is blackholed as it transits this router.

```
R6#debug ip icmp
ICMP packet debugging is onR6#ping 10.7.7.7



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
U ICMP: dst (10.6.20.6) net unreachable rcv from 10.6.20.20
.U
ICMP: dst (10.6.20.6) net unreachable rcv from 10.6.20.20.U Success rate is 0 percent
 (0/5)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3VPN Inter-AS Option A - Back-to-Back VRF Exchange

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Inter AS L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Inter AS L3VPN Diagram** in order to complete this task.

- Configure IGP routing and LDP in the first AS, which consists of R1, R2, and R3 as follows:
  - Enable OSPF Area 0 on the links between R1 & R3 and R2 & R3.
  - Enable OSPF Area 0 on the Loopback0 interfaces of R1, R2, & R3 as passive interfaces.
  - Enable LDP on the links between R1 & R3 and R2 & R3.
- Configure IGP routing and LDP in the second AS, which consists of R4, XR1, and XR2 as follows:
  - Use the following IS-IS NET addressing:
    - R4 – 49.0001.0000.0000.0004.00
    - XR1 – 49.0001.0000.0000.0019.00
    - XR1 – 49.0001.0000.0000.0020.00
  - Enable IS-IS Level 2 on the links between XR1 & R4 and R4 & XR2.
  - Advertise the Loopback0 interfaces of R4, XR1, and XR2 into IS-IS Level 2 as passive interfaces.
  - Enable LDP on the links between XR1 & R4 and R4 & XR2.
- Configure VPNv4 BGP peerings as follows:
  - R1 and R2 should peer in AS 100 using each other's Loopback0 interfaces.
  - XR1 and XR2 should peer in AS 200 using each other's Loopback0 interfaces.
- Configure the following VRFs on PE routers R1 and R2 in AS 100 as follows:
  - VRF VPN_A:
    - Route Distinguisher: 100:1
    - Route Target Import: 100:1

        - Route Target Export: 100:1
        - Assign this VRF on the links in the 30.0.0.0 network on R1 and R2.
    - VRF VPN_B:
        - Route Distinguisher: 100:2
        - Route Target Import: 100:2
        - Route Target Export: 100:2
        - Assign this VRF on the links in the 40.0.0.0 network on R1 and R2.
- Configure the following VRFs on PE routers XR1 and XR2 in AS 200 as follows:
    - VRF VPN_A:
        - Route Distinguisher: 200:1
        - Route Target Import: 200:1
        - Route Target Export: 200:1
        - Assign this VRF on the links in the 30.0.0.0 network on XR1 and XR2.
    - VRF VPN_B:
        - Route Distinguisher: 200:2
        - Route Target Import: 200:2
        - Route Target Export: 200:2
        - Assign this VRF on the links in the 40.0.0.0 network on XR1 and XR2.
- Configure RIPv2 routing for VRF VPN_A as follows:
    - Enable RIP between R9 & R2.
    - Enable RIP between R10 & XR2.
    - Advertise the Loopback0 networks of R9 & R10 into RIP.
- Configure EIGRP routing for VRF VPN_B as follows:
    - Use EIGRP Autonomous System 1.
    - Enable EIGRP between R7 & R2.
    - Enable EIGRP between R8 & XR2.
    - Advertise the Loopback0 networks of R7 & R8 into EIGRP.
- Redistribute between VPNv4 BGP and the VRF aware IGP processes on the PE routers R1, R2, XR1, and XR2.

- Once complete the following reachability should be achieved:
  - Customer routers R9 and R10 should have full IP reachability to each other’s networks.
  - Customer routers R7 and R8 should have full IP reachability to each other’s networks.
  - Traceroutes between these networks should indicate that separate Label Switch Paths are used within AS 100 and AS 200.

Configuration

```
R1:
vrf definition VPN_A
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
vrf definition VPN_B
  rd 100:2
  !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
!
interface Loopback0
  ip ospf 1 area 0
!
interface GigabitEthernet1.13
  ip ospf 1 area 0
  mpls ip
!
interface GigabitEthernet1.30
  vrf forwarding VPN_A
  ip address 30.1.19.1 255.255.255.0
!
interface GigabitEthernet1.40
  vrf forwarding VPN_B
  ip address 40.1.19.1 255.255.255.0
!
router eigrp 65535
```

```
  !
  address-family ipv4 vrf VPN_B
   redistribute bgp 100
  network 40.0.0.0
  autonomous-system 1
 exit-address-family
!
router ospf 1
  passive-interface Loopback0
!
router rip
  !
  address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
  exit-address-family
 !
 router bgp 100
  no bgp default ipv4-unicast
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 update-source Loopback0
  !
  address-family vpnv4
   neighbor 2.2.2.2 activate
   neighbor 2.2.2.2 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf VPN_A
   redistribute rip
  exit-address-family
  !
  address-family ipv4 vrf VPN_B
   redistribute eigrp 1
 exit-address-family
!
mpls ldp router-id Loopback0

R2:
vrf definition VPN_A
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
```

```
 exit-address-family
!
vrf definition VPN_B
 rd 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
!
interface Loopback0
 ip ospf 1 area 0
!
interface GigabitEthernet1.23
 ip ospf 1 area 0
 mpls ip
!
interface GigabitEthernet1.27
  vrf forwarding VPN_B
  ip address 40.2.7.2 255.255.255.0
 !
interface GigabitEthernet1.29
  vrf forwarding VPN_A
  ip address 30.2.9.2 255.255.255.0
 !
 router eigrp 65535
  !
  address-family ipv4 vrf VPN_B
   redistribute bgp 100
   network 40.0.0.0
   autonomous-system 1
 exit-address-family
!
router ospf 1
  passive-interface Loopback0
!
router rip
 !
 address-family ipv4 vrf VPN_A
   redistribute bgp 100 metric 1
   network 30.0.0.0
   no auto-summary
   version 2
 exit-address-family
!
router bgp 100
```

```
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family
 !
 address-family ipv4 vrf VPN_B
  redistribute eigrp 1
 exit-address-family
!
mpls ldp router-id Loopback0

R3:
!
interface Loopback0
  ip ospf 1 area 0
!
interface GigabitEthernet1.13
  ip ospf 1 area 0
  mpls ip
!
interface GigabitEthernet1.23
  ip ospf 1 area 0
  mpls ip
!
router ospf 1
  passive-interface Loopback0
!
mpls ldp router-id Loopback0

R4:
interface GigabitEthernet1.419
  ip router isis
  mpls ip
!
interface GigabitEthernet1.420
  ip router isis
  mpls ip
!
```

```
router isis
  net 49.0001.0000.0000.0004.00
  is-type level-2-only
  passive-interface Loopback0
!
mpls ldp router-id Loopback0

R7:
router eigrp 1
  network 0.0.0.0
  no auto-summary

R8:
router eigrp 1
  network 0.0.0.0
  no auto-summary

R9:
router rip
  version 2
  network 9.0.0.0
  network 30.0.0.0
  no auto-summary

R10:
router rip
  version 2
  network 10.0.0.0
  network 30.0.0.0
  no auto-summary

XR1:
vrf VPN_A
  address-family ipv4 unicast
   import route-target
    200:1
   !
   export route-target
    200:1
  !
 !
!
vrf VPN_B
  address-family ipv4 unicast
   import route-target
    200:2
```

```
    !
    export route-target
     200:2
   !
  !
 !
interface GigabitEthernet0/0/0/0.30
  vrf VPN_A
  no ipv4 address
  ipv4 address 30.1.19.19 255.255.255.0
!
interface GigabitEthernet0/0/0/0.40
  vrf VPN_B
  no ipv4 address
  ipv4 address 40.1.19.19 255.255.255.0
!
route-policy BGP_TO_RIP
  set rip-metric 1
end-policy
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 interface Loopback0
  passive
  address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/0.419
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family vpnv4 unicast
 !
 neighbor 20.20.20.20
  remote-as 200
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
vrf VPN_A
 rd 200:1
 address-family ipv4 unicast
  redistribute rip
```

```
 !
!
vrf VPN_B
 rd 200:2
 address-family ipv4 unicast
  redistribute eigrp 1
  !
 !
!
mpls ldp
 router-id 19.19.19.19
 interface GigabitEthernet0/0/0/0.419
 !
!
router eigrp 65535
 vrf VPN_B
  address-family ipv4
   autonomous-system 1
   redistribute bgp 200
   interface GigabitEthernet0/0/0/0.40
   !
  !
 !
!
router rip
 vrf VPN_A
interface GigabitEthernet0/0/0/0.30
!
redistribute bgp 200 route-policy BGP_TO_RIP
!
!
end

XR2:
vrf VPN_A
  address-family ipv4 unicast
   import route-target
    200:1
   !
   export route-target
    200:1
  !
 !
!
vrf VPN_B
 address-family ipv4 unicast
```

```
  import route-target
   200:2
  !
  export route-target
   200:2
  !
 !
!
interface GigabitEthernet0/0/0/0.820
 vrf VPN_B
 no ipv4 address
 ipv4 address 40.8.20.20 255.255.255.0
!
interface GigabitEthernet0/0/0/0.1020
 vrf VPN_A
 no ipv4 address
 ipv4 address 30.10.20.20 255.255.255.0
!
route-policy BGP_TO_RIP
 set rip-metric 1
end-policy
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 interface Loopback0
  passive
  address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/0.420
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family vpnv4 unicast
 !
 neighbor 19.19.19.19
  remote-as 200
  update-source Loopback0
  address-family vpnv4 unicast
  !
!
vrf VPN_A
 rd 200:1
```

```
 address-family ipv4 unicast
  redistribute rip
 !
!
vrf VPN_B
 rd 200:2
 address-family ipv4 unicast
  redistribute eigrp 1
  !
 !
!
mpls ldp
 router-id 20.20.20.20
 interface GigabitEthernet0/0/0/0.420
 !
!
router eigrp 65535
 vrf VPN_B
  address-family ipv4
   autonomous-system 1
   redistribute bgp 200
   interface GigabitEthernet0/0/0/0.820
   !
  !
 !
!
router rip
 vrf VPN_A
  interface GigabitEthernet0/0/0/0.1020
  !
  redistribute bgp 200 route-policy BGP_TO_RIP
 !
!
```

Verification

This example demonstrates one of the ways that a Service Provider can extend a customer’s Layer 3 MPLS VPN through another Service Provider, giving the customer transparent transport between their sites. This specific design is known as MPLS L3VPN Inter-AS Option A, or sometimes called Back-to-Back VRF Exchange. This is the simplest of all of the Inter-AS designs, because the different Service Providers essentially treat each other as just another customer site.

In this example the Inter-AS link between R1 and XR1 has one subinterfaces per-

VRF that the Service Providers wants to exchange. Each of them treat these links as if they are CE facing links, with normal VRF membership, VRF aware routing configuration, and redistribution of learned routes into VPNv4 BGP and back. The disadvantage of using this design is that scalability becomes an issue as the number of VRFs that the Service Providers want to exchange increase. This scaling problem is solved with the later options B and C, and in the hybrid option AB.

Verification of this design works just like any other MPLS L3VPN design covered up to this point. The PE routers R1 and R2 learn routes from the CE routers XR1, R7, and R9 and redistribute them into VPNv4 BGP. R1 and R2 agree on a Route Target Import and Export policy that will allow them to accept each other's routes for VRF VPN_A and VRF VPN_B.

```
R2#show ip route vrf VPN_A

Routing Table: VPN_A
Codes: L - local, 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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is not set

     9.0.0.0/32 is subnetted, 1 subnets
R        9.9.9.9 [120/1] via 30.2.9.9, 00:00:13, GigabitEthernet1.29
     10.0.0.0/32 is subnetted, 1 subnets
B        10.10.10.10 [200/1] via 1.1.1.1, 00:00:23
     30.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B        30.1.19.0/24 [200/0] via 1.1.1.1, 00:00:23
C        30.2.9.0/24 is directly connected, GigabitEthernet1.29
L        30.2.9.2/32 is directly connected, GigabitEthernet1.29
B        30.10.20.0/24 [200/1] via 1.1.1.1, 00:00:23
R1#show ip route vrf VPN_A

Routing Table: VPN_A
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      9.0.0.0/32 is subnetted, 1 subnets
B        9.9.9.9 [200/1] via 2.2.2.2, 00:00:53
      10.0.0.0/32 is subnetted, 1 subnets
R        10.10.10.10 [120/1] via 30.1.19.19, 00:00:25, GigabitEthernet1.30
      30.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        30.1.19.0/24 is directly connected, GigabitEthernet1.30
L        30.1.19.1/32 is directly connected, GigabitEthernet1.30
B        30.2.9.0/24 [200/0] via 2.2.2.2, 00:00:53
R        30.10.20.0/24 [120/1] via 30.1.19.19, 00:00:25, GigabitEthernet1.30
R2#show bgp vpnv4 unicast vrf VPN_A
BGP table version is 21, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
             r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
             x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
*>  9.9.9.9/32       30.2.9.9                 1         32768 ?
*>i 10.10.10.10/32   1.1.1.1                  1    100      0 ?
*>i 30.1.19.0/24     1.1.1.1                  0    100      0 ?
*>  30.2.9.0/24      0.0.0.0                  0         32768 ?
*>i 30.10.20.0/24    1.1.1.1                  1    100      0 ?
R1#show bgp vpnv4  unicast vrf VPN_A

BGP table version is 15, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
 *>i 9.9.9.9/32       2.2.2.2                  1    100      0 ?
 *>  10.10.10.10/32   30.1.19.19               1         32768 ?
 *>  30.1.19.0/24     0.0.0.0                  0         32768 ?
 *>i 30.2.9.0/24      2.2.2.2                  0    100      0 ?
```

```
 *>  30.10.20.0/24    30.1.19.19               1         32768 ?
```

When the routes are advertised to the other Service Provider, AS 200 in this case, they treat AS 100 just like any other customer site.

```
RP/0/0/CPU0:XR2#show route vrf VPN_A
Tue May 12 23:59:52.338 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route, (!) - FRR Backup path

Gateway of last resort is not set

B    9.9.9.9/32 [200/1] via 19.19.19.19 (nexthop in vrf default), 00:02:56
R    10.10.10.10/32 [120/1] via 30.10.20.10, 00:09:25, GigabitEthernet0/0/0/0.1020
B    30.1.19.0/24 [200/0] via 19.19.19.19 (nexthop in vrf default), 00:08:07
B    30.2.9.0/24 [200/1] via 19.19.19.19 (nexthop in vrf default), 00:02:56
C    30.10.20.0/24 is directly connected, 00:10:09, GigabitEthernet0/0/0/0.1020
L    30.10.20.20/32 is directly connected, 00:10:09, GigabitEthernet0/0/0/0.1020

RP/0/0/CPU0:XR1#show route vrf VPN_A
Wed May 13 00:00:05.186 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route, (!) - FRR Backup path

Gateway of last resort is not set

R    9.9.9.9/32 [120/1] via 30.1.19.1, 00:03:09, GigabitEthernet0/0/0/0.30
B    10.10.10.10/32 [200/1] via 20.20.20.20 (nexthop in vrf default), 00:08:20
C    30.1.19.0/24 is directly connected, 00:09:55, GigabitEthernet0/0/0/0.30
L    30.1.19.19/32 is directly connected, 00:09:55, GigabitEthernet0/0/0/0.30
R    30.2.9.0/24 [120/1] via 30.1.19.1, 00:03:09, GigabitEthernet0/0/0/0.30
```

```
B    30.10.20.0/24 [200/0] via 20.20.20.20 (nexthop in vrf default), 00:08:20
RP/0/0/CPU0:XR2#show bgp vpnv4 unicast vrf VPN_A
Wed May 13 00:00:18.366 UTC
BGP router identifier 20.20.20.20, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 17
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:1 (default for vrf VPN_A)
*>i9.9.9.9/32         19.19.19.19              1    100      0 ?
*> 10.10.10.10/32     30.10.20.10              1         32768 ?
*>i30.1.19.0/24       19.19.19.19              0    100      0 ?
*>i30.2.9.0/24        19.19.19.19              1    100      0 ?
*> 30.10.20.0/24      0.0.0.0                  0         32768 ?

Processed 5 prefixes, 5 paths

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A

Wed May 13 00:00:34.384 UTC
BGP router identifier 19.19.19.19, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 18
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:1 (default for vrf VPN_A)
*> 9.9.9.9/32         30.1.19.1                1         32768 ?
*>i10.10.10.10/32     20.20.20.20              1    100      0 ?
*> 30.1.19.0/24       0.0.0.0                  0         32768 ?
*> 30.2.9.0/24        30.1.19.1                1         32768 ?
*>i30.10.20.0/24      20.20.20.20              0    100      0 ?
```

```
Processed 5 prefixes, 5 paths
```

The final result of this is that although the customer sites do have end-to-end reachability to each other, they do not use the same MPLS Label Switch Path to exchange their traffic. Instead there is one LSP from PEs R1 to R2, and second LSP from PEs XR1 to XR2, and vice versa. The Inter-AS traffic exchanged on the R1 to XR1 link is sent as normal *unlabeled* IPv4 traffic, resulting in a path that is not end to end MPLS encapsulated. Verification of this can be seen through a traceroute.

```
R7#traceroute 8.8.8.8 source loopback 0
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
 1 40.2.7.2 2 msec 1 msec 1 msec
 2 10.2.3.3 [MPLS: Labels 17/23 Exp 0] 3 msec 2 msec 10 msec
 3 40.1.19.1 [MPLS: Label 23 Exp 0] 19 msec 18 msec 19 msec
 4 40.1.19.19 19 msec 14 msec 14 msec
 5 20.4.19.4 [MPLS: Labels 17/16005 Exp 0] 31 msec 23 msec 20 msec
 6 20.4.20.20 [MPLS: Label 16005 Exp 0] 24 msec 24 msec 20 msec
 7 40.8.20.8 20 msec *  25 msec
R10#traceroute 9.9.9.9 source loopback 0

Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
  1 30.10.20.20 1 msec 2 msec 1 msec
  2 20.4.20.4 [MPLS: Labels 16/16009 Exp 0] 26 msec 19 msec 19 msec
  3 20.4.19.19 [MPLS: Label 16009 Exp 0] 20 msec 20 msec 20 msec
  4 30.1.19.1 20 msec 20 msec 20 msec
  5 10.1.3.3 [MPLS: Labels 16/16 Exp 0] 20 msec 20 msec 20 msec
  6 30.2.9.2 [MPLS: Label 16 Exp 0] 25 msec 23 msec 20 msec
  7 30.2.9.9 20 msec *  28 msec
```

The above output indicates that when traffic from R7’s site in VPN_B goes to 8.8.8.8 – the Loopback0 of R8 – it uses the VPN label 23 to reach R1, traffic is unlabeled IPv4 traffic between R1 and XR1, then XR1 uses the VPN label 16005 to reach XR2, where the traffic is sent towards the final customer site. However, from the customer’s point of view, end-to-end IP transport is provided, and they have no way of knowing that their traffic is transiting more than one service provider.

This Inter-AS Layer 3 VPNs design is documented under Section 10.a in RFC 4364

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

MPLS L3VPN Inter-AS Option B - VPNv4 EBGP Exchange

> **A Note On Section Initial Configuration Files**: You must load the initial configuration files for the section, named **Inter AS L3VPN**, which can be found in CCIE SPv4 Topology Diagrams & Initial Configurations. Reference the **Inter AS L3VPN Diagram** in order to complete this task.

- Disable the VLAN 40 subinterface of both R1 and XR1.
- Configure IGP routing and LDP in the first AS, which consists of R1, R2, and R3 as follows:
  - Enable OSPF Area 0 on the links between R1 & R3 and R2 & R3.
  - Enable OSPF Area 0 on the Loopback0 interfaces of R1, R2, & R3 as passive interfaces.
  - Enable LDP on the links between R1 & R3 and R2 & R3.
- Configure IGP routing and LDP in the second AS, which consists of R4, XR1, and XR2 as follows:
  - Use the following IS-IS NET addressing:
    - R4 – 49.0001.0000.0000.0004.00
    - XR1 – 49.0001.0000.0000.0019.00
    - XR2 – 49.0001.0000.0000.0020.00
  - Enable IS-IS Level 2 on the links between XR1 & R4 and R4 & XR2.
  - Advertise the Loopback0 interfaces of R4, XR1, and XR2 into IS-IS Level 2 as passive interfaces.
  - Enable LDP on the links between XR1 & R4 and R4 & XR2.
- Configure the following VRFs on PE routers R2 and XR2 follows:
  - VRF VPN_A:
    - Route Distinguisher: 101:201
    - Route Target Import: 101:201
    - Route Target Export: 101:201
    - Assign this VRF on the links in the 30.0.0.0 network on R2 and XR2.
  - VRF VPN_B:

        - Route Distinguisher: 102:202
        - Route Target Import: 102:202
        - Route Target Export: 102:202
        - Assign this VRF on the links in the 40.0.0.0 network on R2 and XR2.
- Configure RIPv2 routing for VRF VPN_A as follows:
    - Enable RIP between R9 & R2.
    - Enable RIP between R10 & XR2.
    - Advertise the Loopback0 networks of R9 & R10 into RIP.
- Configure EIGRP routing for VRF VPN_B as follows:
    - Use EIGRP Autonomous System 1. o
    - Enable EIGRP between R7 & R2.
    - Enable EIGRP between R8 & XR2.
    - Advertise the Loopback0 networks of R7 & R8 into RIP.
- Configure VPNv4 BGP peerings as follows:
    - R1 and R2 should peer in AS 100 using each other's Loopback0 interfaces.
    - XR1 and XR2 should peer in AS 200 using each other's Loopback0 interfaces.
    - R1 and XR1 should peer EBGP.
- Redistribute between VPNv4 BGP and the VRF aware IGP processes on R2 and XR2.
- Once complete the following reachability should be achieved:
    - Customer routers R9 and R10 should have full IP reachability to each other's networks.
    - Customer routers R7 and R8 should have full IP reachability to each other's networks.
    - Traceroutes between these networks should indicate that separate Label Switch Paths are used within AS 100 and AS 200.

Configuration

```
R1:
interface Loopback0
 ip ospf 1 area 0
!
interface GigabitEthernet1.13
 ip ospf 1 area 0
 mpls ip
!
interface GigabitEthernet1.30
 mpls bgp forwarding
```

```
!
router bgp 100
 no bgp default ipv4-unicast
 no bgp default route-target filter
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 30.1.19.19 remote-as 200
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 next-hop-self
  neighbor 30.1.19.19 activate
  neighbor 30.1.19.19 send-community extended
 exit-address-family
!
mpls ldp router-id Loopback0

R2:
vrf definition VPN_A
 rd 101:201
 !
 address-family ipv4
 route-target export 101:201
 route-target import 101:201
 exit-address-family
!
vrf definition VPN_B
 rd 102:202
 !
 address-family ipv4
 route-target export 102:202
 route-target import 102:202
 exit-address-family
!
interface Loopback0
 ip ospf 1 area 0
!
interface GigabitEthernet1.23
 ip ospf 1 area 0
 mpls ip
!
interface GigabitEthernet1.27
 vrf forwarding VPN_B
 ip address 40.2.7.2 255.255.255.0
!
```

```
interface GigabitEthernet1.29
 vrf forwarding VPN_A
 ip address 30.2.9.2 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
  redistribute bgp 100
  network 40.0.0.0
  autonomous-system 1
 exit-address-family
!
router ospf 1
 passive-interface Loopback0
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family
 !
address-family ipv4 vrf VPN_B
  redistribute eigrp 1
 exit-address-family
!
mpls ldp router-id Loopback0

R3:
!
```

```
interface Loopback0
 ip ospf 1 area 0
!
interface GigabitEthernet1.13
 ip ospf 1 area 0
 mpls ip
!
interface GigabitEthernet1.23
 ip ospf 1 area 0
 mpls ip
!
router ospf 1
 passive-interface Loopback0
!
mpls ldp router-id Loopback0

R4:
interface GigabitEthernet1.419
 ip router isis
 mpls ip
!
interface GigabitEthernet1.420
 ip router isis
 mpls ip
!
router isis
 net 49.0001.0000.0000.0004.00
 is-type level-2-only
 passive-interface Loopback0
!
mpls ldp router-id Loopback0

R7:
router eigrp 1
 network 0.0.0.0
 no auto-summary

R8:
router eigrp 1
 network 0.0.0.0
 no auto-summary

R9:
router rip
 version 2
 network 9.0.0.0
```

```
 network 30.0.0.0
 no auto-summary

R10:
 router rip
  version 2
  network 10.0.0.0
  network 30.0.0.0
  no auto-summary

XR1:
route-policy PASS
  pass
end-policy
!
router static
 address-family ipv4 unicast
  30.1.19.1/32 GigabitEthernet0/0/0/0.30
 !
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.419
  address-family ipv4 unicast
  !
 !
!
router bgp 200
  address-family vpnv4 unicast
   retain route-target all
  !
  neighbor 20.20.20.20
   remote-as 200
   update-source Loopback0
   address-family vpnv4 unicast
    next-hop-self
   !
  !
  neighbor 30.1.19.1
   remote-as 100
```

```
   address-family vpnv4 unicast
    route-policy PASS in
    route-policy PASS out
   !
  !
!
mpls ldp
 router-id 19.19.19.19
 interface GigabitEthernet0/0/0/0.419
 !
!

XR2:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   101:201
  !
  export route-target
   101:201
  !
 !
!
vrf VPN_B
 address-family ipv4 unicast
  import route-target
   102:202
  !
  export route-target
   102:202
  !
 !
!
interface GigabitEthernet0/0/0/0.820
 vrf VPN_B
 no ipv4 address
 ipv4 address 40.8.20.20 255.255.255.0
!
interface GigabitEthernet0/0/0/0.1020
 vrf VPN_A
 no ipv4 address
 ipv4 address 30.10.20.20 255.255.255.0
!
route-policy BGP_TO_RIP
  set rip-metric 1
end-policy
```

```
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0.420
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family vpnv4 unicast
 !
 neighbor 19.19.19.19
  remote-as 200
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf VPN_A
  rd 101:201
  address-family ipv4 unicast
   redistribute rip
  !
 !
 vrf VPN_B
  rd 102:202
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
mpls ldp
 router-id 20.20.20.20
 interface GigabitEthernet0/0/0/0.420
 !
!
router eigrp 65535
 vrf VPN_B
  address-family ipv4
   autonomous-system 1
   redistribute bgp 200
```

```
   interface GigabitEthernet0/0/0/0.820
   !
  !
 !
!
router rip
 vrf VPN_A
  interface GigabitEthernet0/0/0/0.1020
  !
  redistribute bgp 200 route-policy BGP_TO_RIP
 !
!
```

Verification

MPLS L3VPN Inter-AS Option B, sometimes also called MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, is similar to the previous Option A example with the exception that the Inter-AS link runs a single VPNv4 EBGP peering instead of multiple VRF aware IGP or BGP instances. Unlike the Option A example in which the providers did not run VPNv4 BGP with each other, Option B's VPNv4 EBGP peering between the providers means that the VPNv4 Route Distinguisher and Route Target fields have global significance between the MPLS Service Providers. This is evident based on the fact that the customer attached PE routers R2 and XR2, who do not have VPNv4 BGP peerings with each other, must agree on a standard RD and RT policy in order for routing exchange to be complete.

The final verification of this design, like any other L3VPN configuration, would be to test end- to-end connectivity between the customer sites. Once again just like in Option A the customer networks are oblivious to the fact that their traffic is transiting multiple providers. As long as the SP is able to provide end-to-end IP connectivity this is what the customer is most concerned with.

```
R9#show ip route rip
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
      10.0.0.0/32 is subnetted, 1 subnets
R        10.10.10.10 [120/1] via 30.2.9.2, 00:00:15, GigabitEthernet1.29
      30.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        30.10.20.0/24 [120/1] via 30.2.9.2, 00:00:15, GigabitEthernet1.29
R9#ping 10.10.10.10 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/32 ms
R9#traceroute 10.10.10.10 source loopback0

Type escape sequence to abort.
Tracing the route to 10.10.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 30.2.9.2 1 msec 1 msec 1 msec
  2 10.2.3.3 [MPLS: Labels 17/24 Exp 0] 26 msec 89 msec 31 msec
  3 10.1.3.1 [MPLS: Label 24 Exp 0] 32 msec 28 msec 32 msec
  4 30.1.19.19 [MPLS: Label 16015 Exp 0] 30 msec 30 msec 32 msec
  5 20.4.19.4 [MPLS: Labels 17/16003 Exp 0] 30 msec 30 msec 31 msec
  6 20.4.20.20 [MPLS: Label 16003 Exp 0] 23 msec 24 msec 24 msec
  7 30.10.20.10 20 msec *  23 msec
```

From inside the Service Provider network though, it begins to become clear that the design is now more complicated than the Service Providers simply treating each other as customer sites. Instead, the Service Providers now treat each other as VPNv4 EBGP peers, which means the design is more similar to normal IPv4 Unicast EBGP for regular unlabeled IPv4 transport over the Internet.

In the below output we see that the final PE routers R2 and XR2 learn the VPNv4 BGP routes via their Inter-AS PEs R1 and XR1, however transitive attributes such as the AS-Path, the VPNv4 Route Distinguisher, and the VPNv4 Route Target values remain.

```
R2#show bgp vpnv4 unicast all
BGP table version is 21, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
```

```
 *>  9.9.9.9/32       30.2.9.9                 1         32768 ?
*>i 10.10.10.10/32    1.1.1.1                 0     100       0 200 ?
 *>  30.2.9.0/24      0.0.0.0                  0         32768 ?
*>i 30.10.20.0/24     1.1.1.1                 0     100       0 200 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
 *>  7.7.7.7/32       40.2.7.7            130816         32768 ?
*>i 8.8.8.8/32        1.1.1.1                 0     100       0 200 ?
 *>  40.2.7.0/24      0.0.0.0                  0         32768 ?
*>i 40.8.20.0/24      1.1.1.1                 0     100       0 200 ?
```

R2#show bgp vpnv4 unicast all 8.8.8.8

```
             BGP routing table entry for 102:202:8.8.8.8/32
, version 19
Paths: (1 available, best #1, table VPN_B)
  Not advertised to any peer
  Refresh Epoch 1
  200
    1.1.1.1 (metric 3) (via default) from 1.1.1.1 (1.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:102:202 0x8800:32768:0 0x8801:1:128256
 0x8802:65281:2560 0x8803:1:1500
      mpls labels in/out nolabel/26
      rx pathid: 0, tx pathid: 0x0
```

RP/0/0/CPU0:XR2#show bgp vpnv4 unicast

```
Wed May 13 01:24:16.081 UTC
BGP router identifier 20.20.20.20, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 19
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
*>i9.9.9.9/32         19.19.19.19                  100      0 100 ?
*> 10.10.10.10/32     30.10.20.10              1         32768 ?
*>i30.2.9.0/24        19.19.19.19                  100      0 100 ?
*> 30.10.20.0/24      0.0.0.0                  0         32768 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
*>i7.7.7.7/32         19.19.19.19                  100      0 100 ?
*> 8.8.8.8/32         40.8.20.8          2570240         32768 ?
*>i40.2.7.0/24        19.19.19.19                  100      0 100 ?
```

```
*> 40.8.20.0/24       0.0.0.0                  0         32768 ?

Processed 8 prefixes, 8 paths
RP/0/0/CPU0:XR2#show bgp vpnv4 unicast vrf VPN_A 9.9.9.9
Wed May 13 01:25:22.566 UTC BGP routing table entry for 9.9.9.9/32, Route Distinguisher: 101:201
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 14          14
Last Modified: May 13 01:18:17.625 for 00:07:05
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  100
    19.19.19.19 (metric 20) from 19.19.19.19 (19.19.19.19) Received Label 16011
Origin incomplete
, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 14 Extended community: RT:101:201

      Source VRF: VPN_A, Source Route Distinguisher: 101:201
```

Since the PE routers R2 and XR2 do not have an IGP route to the transit link between R1 and XR1, these edge routers are changing the next-hop value to their own local Loopback.

Changing the BGP next-hop value of a VPNv4 route has an additional special significance, because the next-hop value is what's used to determine which LDP derived Transport Label to use when encapsulating MPLS traffic towards the destination. In this specific design, the VPNv4 next-hop value is changing three times for every route that is originated by the customer facing PEs.

When R2 originates the VPNv4 route 7.7.7.7/32 towards R1, it sets the next-hop value to its own local Loopback. This means that R1 will use the transport label towards 2.2.2.2 in order to label switch traffic towards 7.7.7.7/32. Notice that an "In" label has been allocated locally by R1, and is what will be advertised towards XR1.

```
R1#show bgp vpnv4 unicast all 7.7.7.7/32
BGP routing table entry for 102:202:7.7.7.7/32
, version 4
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  Local
    2.2.2.2 (metric 3) (via default) from 2.2.2.2 (2.2.2.2)
      Origin incomplete, metric 130816, localpref 100, valid, internal, best
```

```
      Extended Community: RT:102:202
 Cost:pre-bestpath:128:130816
        0x8800:32768:0 0x8801:1:128256 0x8802:65281:2560 0x8803:65281:1500
        0x8806:0:117901063 mpls labels in/out 22/21

      rx pathid: 0, tx pathid: 0x0
```

When a VPNv4 router without local VRFs inserts itself in the forwarding path by changing the next-hop to self, LFIB state is created for such paths. This forwarding state is what is then used for packet forwarding in hardware. Not only does R1 have LFIB entries for the LDP derived labels, but additional entries have been created for all VPN routes for which R1 set itself as a next-hop. Notice that local label 22 has an entry, the VPN "in" label which is advertised to XR1 for 102:202:7.7.7.7/32. The "out" label from the VPN route, 21, is the label that R2 originated for the route.

```
R1#show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  3.3.3.3/32       0             Gi1.13     10.1.3.3
17         Pop Label  10.2.3.0/24      0             Gi1.13     10.1.3.3
18         16         2.2.2.2/32       0             Gi1.13     10.1.3.3
19         Pop Label  30.1.19.19/32    0             Gi1.30     30.1.19.19
20         19         101:201:9.9.9.9/32   \
                                       3728          Gi1.13     10.1.3.3
21         20         101:201:30.2.9.0/24   \
                                       0             Gi1.13     10.1.3.3
22         21         102:202:7.7.7.7/32
   \
                                       0             Gi1.13     10.1.3.3
23         22         102:202:40.2.7.0/24   \
                                       0             Gi1.13     10.1.3.3
24         16015      101:201:10.10.10.10/32   \
                                       1912          Gi1.30     30.1.19.19
25         16016      101:201:30.10.20.0/24   \
                                       0             Gi1.30     30.1.19.19
26         16017      102:202:8.8.8.8/32   \
                                       0             Gi1.30     30.1.19.19
27         16018      102:202:40.8.20.0/24   \
                                       0             Gi1.30     30.1.19.19
```

When R1 sends the route to its VPNv4 EBGP neighbor, XR1, the next-hop value is changed to the local peering address. Specifically this is the address 30.1.19.1, as seen below. Also notice that the VPNv4 MPLS Label is changing every time the next-hop value changes.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast rd 102:202 7.7.7.7/32
Wed May 13 02:01:35.687 UTC BGP routing table entry for 7.7.7.7/32, Route Distinguisher: 102:202
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  4           4 Local Label: 16013
Last Modified: May 13 01:16:26.451 for 00:45:09
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    20.20.20.20
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    20.20.20.20
  100
    30.1.19.1 from 30.1.19.1 (1.1.1.1) Received Label 22
      Origin incomplete, localpref 100, valid, external, best, group-best, import-candidate, not-in-vrf
      Received Path ID 0, Local Path ID 1, version 4
      Extended community: EIGRP route-info:0x8000:0 EIGRP AD:1:128256 EIGRP RHB:255:1:2560 EIGRP LM:0xff:1:1500 0x88
RT:102:202
```

XR1 also creates LFIB state for all the VPN routes for which it is setting itself as the next-hop. Notice that the "out" or "received" label for 102:202:7.7.7.7/32 is 22.

```
RP/0/0/CPU0:XR1#show mpls forwarding

Wed May 13 02:19:08.005 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  17          20.20.20.20/32     Gi0/0/0/0.419 20.4.19.4       9851
16001  Pop         20.4.20.0/24       Gi0/0/0/0.419 20.4.19.4       0
16003  Pop         4.4.4.4/32         Gi0/0/0/0.419 20.4.19.4       7272
16007  Pop         30.1.19.1/32       Gi0/0/0/0.30 30.1.19.1       10574
16011  20          101:201:9.9.9.9/32 Gi0/0/0/0.30 30.1.19.1       3244
16012  21          101:201:30.2.9.0/24   \
                                      Gi0/0/0/0.30 30.1.19.1       0
16013  22          102:202:7.7.7.7/32 Gi0/0/0/0.30 30.1.19.1       0

16014  23          102:202:40.2.7.0/24   \
                                      Gi0/0/0/0.30 30.1.19.1       0
16015  16003       101:201:10.10.10.10/32   \
                                                   20.20.20.20     2584
```

```
16016  16008       101:201:30.10.20.0/24   \
                                                            20.20.20.20     0
16017  16005       102:202:8.8.8.8/32              20.20.20.20     0
16018  16009       102:202:40.8.20.0/24   \
                                                            20.20.20.20     0
```

A very important point about this design is that IOS XR cannot label switch traffic towards a next-hop that is not learned via a /32 host route. This means that in order for XR1 to label switch traffic towards the connected link to R1, it must have a /32 host route to the address 30.1.19.1. This is the reason that XR1 has a static route locally configured in its routing table, as seen below.

```
RP/0/0/CPU0:XR1#show run router static
Wed May 13 02:04:01.147 UTC
router static
 address-family ipv4 unicast
  30.1.19.1/32 GigabitEthernet0/0/0/0.30
 !
!
RP/0/0/CPU0:XR1#show route static

Wed May 13 02:04:15.376 UTC

S   30.1.19.1/32 is directly connected, 00:49:57, GigabitEthernet0/0/0/0.30
```

Note that IOS does this automatically when the 'mpls bgp forwarding' command is enabled, as it is on R1's interface towards XR1. This command is automatically generated when an EBGP VPNv4 session is established.

```
R1#show run int Gi1.30
Building configuration...

Current configuration : 118 bytes
!
interface GigabitEthernet1.30
 encapsulation dot1Q 30
 ip address 30.1.19.1 255.255.255.0 mpls bgp forwarding
end
R1#show ip route connected | include GigabitEthernet1.30
C        30.1.19.0/24 is directly connected, GigabitEthernet1.30
L        30.1.19.1/32 is directly connected, GigabitEthernet1.30
C        30.1.19.19/32 is directly connected, GigabitEthernet1.30
R1#show ip route 30.1.19.19
```

```
Routing entry for 30.1.19.19/32
  Known via "connected", distance 0, metric 0 (connected, via interface
)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet1.30
      Route metric is 0, traffic share count is 1
```

XR1 continues to advertise the route on to XR2, again updating the next-hop value of the VPNv4 route, which is due to the **next-hop-self** command under the VPNv4 BGP process. Note again that since the next-hop value changed, so did the MPLS Label.

```
RP/0/0/CPU0:XR2#show bgp vpnv4 unicast rd 102:202 7.7.7.7/32

Wed May 13 02:07:55.391 UTC BGP routing table entry for 7.7.7.7/32, Route Distinguisher: 102:202
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 16          16
Last Modified: May 13 01:18:17.625 for 00:49:37
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  100
    19.19.19.19 (metric 20) from 19.19.19.19 (19.19.19.19) Received Label 16013
      Origin incomplete, localpref 100, valid, internal, best, group-best, import-candidate, imported
      Received Path ID 0, Local Path ID 1, version 16
      Extended community: EIGRP route-info:0x8000:0 EIGRP AD:1:128256 EIGRP RHB:255:1:2560 EIGRP LM:0xff:1:1500 0x88
RT:102:202

      Source VRF: VPN_B, Source Route Distinguisher: 102:202
```

The end result of this is that when a traceroute is sent between the customer sites it can be seen that the VPN Label changes three times during transit. The LFIB state created on R1 and XR1 allows for the "stitching" of the LSPs to occur.

```
R8#traceroute 7.7.7.7 source loopback 0
Type escape sequence to abort.
Tracing the route to 7.7.7.7
VRF info: (vrf in name/id, vrf out name/id)
  1 40.8.20.20 2 msec 1 msec 1 msec  2 20.4.20.4 [MPLS: Labels 16/16013
 Exp 0] 24 msec 20 msec 20 msec  3 20.4.19.19 [MPLS: Label 16013
 Exp 0] 20 msec 20 msec 27 msec  4 30.1.19.1 [MPLS: Label 22
 Exp 0] 43 msec 21 msec 28 msec
```

```
  5 10.1.3.3 [MPLS: Labels 16/21
 Exp 0] 32 msec 32 msec 28 msec   6 40.2.7.2 [MPLS: Label 21
 Exp 0] 24 msec 20 msec 20 msec
  7 40.2.7.7 20 msec *  24 msec
```

From R8 to R7 the VPN label 16013 terminates at XR1, a second LSP via VPN label 22 terminates at R1, and a third LSP via VPN label 21 terminates at R2. This can likewise be seen on the reverse path, with label value 26 from R2 to R1, label value 16017 from R1 to XR1, and label value 16005 from XR1 to XR2.

```
R7#traceroute 8.8.8.8 source loopback 0
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 40.2.7.2 4 msec 1 msec 1 msec  2 10.2.3.3 [MPLS: Labels 17/26
 Exp 0] 27 msec 25 msec 24 msec  3 10.1.3.1 [MPLS: Label 26
 Exp 0] 23 msec 24 msec 28 msec  4 30.1.19.19 [MPLS: Label 16017
 Exp 0] 19 msec 24 msec 20 msec  5 20.4.19.4 [MPLS: Labels 17/16005
 Exp 0] 28 msec 32 msec 31 msec  6 20.4.20.20 [MPLS: Label 16005
 Exp 0] 28 msec 20 msec 24 msec
  7 40.8.20.8 20 msec *  24 msec
```

Keep in mind that this also means that the traffic on the Inter-AS link between R1 and XR1 is now MPLS Labeled, where in the previous Inter-AS Option A example the traffic was native IPv4. This can have a potential impact when trying to implement features such as QoS, which require different configuration to classify packets as MPLS vs. native IPv4 packets.

Another caveat of this configuration is the need for the command **no bgp default route-target filter** in regular IOS on R1 and **retain route-target all** in IOS XR on XR1. These are needed because the VPNv4 peers do not have the VRFs VPN_A and VPN_B configured locally, which means that they will discard the VPNv4 routes when received from their peers because they do not have a matching Route Target Import Policy. The potential problem of this can be seen below with the default behavior of the route target filter.

```
R1#debug bgp vpnv4 unicast update
BGP updates debugging is on for address family: VPNv4 Unicast
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.R1(config)#router bgp 100
R1(config-router)#bgp default route-target filter
R1(config-router)#endR1#clear bgp vpnv4 unicast * in
BGP: nbr_topo global 2.2.2.2 VPNv4 Unicast:base (0x7FF7B88F7BE0:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 2.2.2.2 VPNv4 Unicast:base (0x7FF7B88F7BE0:1) refresh_epoch is 2
```

```
BGP(4): 2.2.2.2 rcvd UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 130816, extended community RT:
BGP(4): 2.2.2.2 rcvd 102:202:7.7.7.7/32, label 21 --DENIED due to:  extended community not supported;
BGP(4): no valid path for 102:202:7.7.7.7/32
BGP(4): 2.2.2.2 rcvd UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 0, extended community RT:102:2
BGP(4): 2.2.2.2 rcvd 102:202:40.2.7.0/24, label 22 --DENIED due to:  extended community not supported;
BGP(4): no valid path for 102:202:40.2.7.0/24
BGP(4): 2.2.2.2 rcvd UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 0, extended community RT:101:2
BGP(4): 2.2.2.2 rcvd 101:201:30.2.9.0/24, label 20 --DENIED due to:  extended community not supported;
BGP(4): no valid path for 101:201:30.2.9.0/24
BGP(4): 2.2.2.2 rcvd UPDATE w/ attr: nexthop 2.2.2.2, origin ?, localpref 100, metric 1, extended community RT:101:2
BGP(4): 2.2.2.2 rcvd 101:201:9.9.9.9/32, label 19 --DENIED due to:  extended community not supported;

BGP(4): no valid path for 101:201:9.9.9.9/32
BGP: nbr_topo global 2.2.2.2 VPNv4 Unicast:base (0x7FF7B88F7BE0:1) rcvd Refresh End-of-RIB
```

Since R1 now drops inbound advertisements from its VPNv4 peers R2 and XR1, the end-to- end control plane is now broken.

```
R7#show ip route eigrp

R7#
R9#show ip route rip

R9#
R2#show bgp vpnv4 unicast all
BGP table version is 27, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
 *>  9.9.9.9/32       30.2.9.9                 1         32768 ?
 *>  30.2.9.0/24      0.0.0.0                  0         32768 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
 *>  7.7.7.7/32       40.2.7.7            130816         32768 ?
 *>  40.2.7.0/24      0.0.0.0                  0         32768 ?
RP/0/0/CPU0:XR2#show bgp vpnv4 unicast

Wed May 13 02:30:18.139 UTC
BGP router identifier 20.20.20.20, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
```

```
Table ID: 0x0   RD version: 0
BGP main routing table version 23
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
*> 10.10.10.10/32     30.10.20.10              1         32768 ?
*> 30.10.20.0/24      0.0.0.0                  0         32768 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
*> 8.8.8.8/32         40.8.20.8          2570240         32768 ?
*> 40.8.20.0/24       0.0.0.0                  0         32768 ?

Processed 4 prefixes, 4 paths
```

From the above output we see that the final PE routers of R2 and XR2 only know about VPNv4 routes that they are locally originating. All Inter-AS exchanged VPNv4 routes are no longer learned. The same would be true if XR1 reverted back to its default filtering behavior.

```
RP/0/0/CPU0:XR1#debug bgp update vpnv4 unicast in
RP/0/0/CPU0:XR1(config)#no router bgp 100
RP/0/0/CPU0:XR1(config)#router bgp 200
RP/0/0/CPU0:XR1(config-bgp)#address-family vpnv4 unicast
RP/0/0/CPU0:XR1(config-bgp-af)#no retain route-target all

RP/0/0/CPU0:XR1(config-bgp-af)#commit
Wed May 13 02:32:31.570 UTC
RP/0/0/CPU0:XR1#clear bgp vpnv4 unicast * soft in
RP/0/0/CPU0:XR1#RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: UPDATE from 20.20.20.20 contains nh 20.2
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=20.20.20.20/32, len=12, nlriafi
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=20.20.20.20:: msg=0x10
as_prepended=0, attr_wdr_flags 0x00000000, myascount=0:: rcvdata=0x1002fe27/0, errptr=0x1002fe1c/11
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 20.20.20.20 with attributes
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): nexthop 20.20.20.20/32, origin ?, localpref 100,
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:101:201:30.10.20.0/24 (path
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:101:201:30.10.20.0/24 (path ID: none
DENIED RT extended community is not imported locally
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: UPDATE from 20.20.20.20 contains nh 20.20.20.20/32, gw_a
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=20.20.20.20/32, len=12, nlriafi
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=20.20.20.20:: msg=0x10
as_prepended=0, attr_wdr_flags 0x00000000, myascount=0:: rcvdata=0x1002fbc0/0, errptr=0x1002fbb5/11
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 20.20.20.20 with attributes
```

```
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): nexthop 20.20.20.20/32, origin ?, localpref 100,
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:101:201:10.10.10.10/32 (pat
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:101:201:10.10.10.10/32 (path ID: non
DENIED RT extended community is not imported locally
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: UPDATE from 20.20.20.20 contains nh 20.20.20.20/32, gw_a
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=20.20.20.20/32, len=12, nlriafi
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=20.20.20.20:: msg=0x10
al_as_prepended=0, attr_wdr_flags 0x00000000, myascount=0:: rcvdata=0x10037d33/0, errptr=0x10037d00/51
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 20.20.20.20 with attributes
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): nexthop 20.20.20.20/32, origin ?, localpref 100,
2
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:102:202:40.8.20.0/24 (path
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:102:202:40.8.20.0/24 (path ID: none)
DENIED RT extended community is not imported locally
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: UPDATE from 20.20.20.20 contains nh 20.20.20.20/32, gw_a
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: NH-Validate-Create: addr=20.20.20.20/32, len=12, nlriafi
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr]: --bgp4_rcv_attributes--: END: nbr=20.20.20.20:: msg=0x10
al_as_prepended=0, attr_wdr_flags 0x00000000, myascount=0:: rcvdata=0x10037ecc/0, errptr=0x10037e99/51
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received UPDATE from 20.20.20.20 with attributes
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): nexthop 20.20.20.20/32, origin ?, localpref 100,
0 RT:102:202
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Received prefix 2ASN:102:202:8.8.8.8/32 (path ID
RP/0/0/CPU0:May 13 02:35:09.209 : bgp[1047]: [default-rtr] (vpn4u): Prefix 2ASN:102:202:8.8.8.8/32 (path ID: none) r
DENIED RT extended community is not imported locally
```

An alternate solution to this problem would be to locally configure the VRFs on the edge routers R1 and XR1, or to configure them as VPNv4 Route Reflectors, as Route Reflectors do not filter prefixes based on the Route Target extended community. These possible solutions can be seen below.

```
R1#show bgp vpnv4 unicast all

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.R1(config)#vrf definition VPN_A
R1(config-vrf)# rd 101:201
R1(config-vrf)# !
R1(config-vrf)# address-family ipv4
R1(config-vrf-af)# route-target export 101:201
R1(config-vrf-af)# route-target import 101:201
 R1(config-vrf-af)# exit-address-family R1(config-
vrf)#!
R1(config-vrf)#vrf definition VPN_B
 R1(config-vrf)# rd 102:202
R1(config-vrf)# !
R1(config-vrf)# address-family ipv4
R1(config-vrf-af)# route-target export 102:202
```

```
R1(config-vrf-af)#end
R1#

RP/0/0/CPU0:XR1#conf t
Wed May 13 02:37:57.637 UTCRP/0/0/CPU0:XR1(config)#router bgp 200
RP/0/0/CPU0:XR1(config-bgp)#neighbor 20.20.20.20
RP/0/0/CPU0:XR1(config-bgp-nbr)#address-family vpnv4 unicast
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#route-reflector-client
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#commit
Wed May 13 02:38:20.896 UTC
RP/0/0/CPU0:May 13 02:38:21.306 : config[65729]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'.
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#RP/0/0/CPU0:May 13 02:38:22.956 : bgp[1047]: %ROUTING-BGP-5-ADJCHANGE : neighbor
RP/0/0/CPU0:May 13 02:38:25.625 : bgp[1047]: %ROUTING-BGP-5-ADJCHANGE : neighbor 20.20.20.20 Up (VRF: default) (AS:
R1#show bgp vpnv4 unicast all

BGP table version is 33, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
 *>i 9.9.9.9/32       2.2.2.2                  1    100      0 ?
 *>  10.10.10.10/32   30.1.19.19                             0 200 ?
 *>i 30.2.9.0/24      2.2.2.2                  0    100      0 ?
 *>  30.10.20.0/24    30.1.19.19                             0 200 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
 *>i 7.7.7.7/32       2.2.2.2             130816    100      0 ?
 *>  8.8.8.8/32       30.1.19.19                             0 200 ?
 *>i 40.2.7.0/24      2.2.2.2                  0    100      0 ?
 *>  40.8.20.0/24     30.1.19.19                             0 200 ?
```

Notice that now the LFIB state on R1 now shows an "V" - this is referencing the fact that the routes are in a VRF. The downside to this technique is that additional resources are consumed because R1 now has to install all of the routes in each VRF's RIB - even though they will never be used. With the previous solution, only LFIB state was created, and no routes were installed (there were no VRFs to install the routes into).

```
R1#show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
```

```
16          Pop Label  3.3.3.3/32       0              Gi1.13     10.1.3.3
17          Pop Label  10.2.3.0/24      0              Gi1.13     10.1.3.3
18          16         2.2.2.2/32       0              Gi1.13     10.1.3.3
19          Pop Label  30.1.19.19/32    0              Gi1.30     30.1.19.19
20          20         30.2.9.0/24[V
]   0            Gi1.13     10.1.3.3    21          21         7.7.7.7/32[V
]    3098          Gi1.13     10.1.3.3    22          19         9.9.9.9/32[V
]    1824          Gi1.13     10.1.3.3    23          22         40.2.7.0/24[V
]   0            Gi1.13     10.1.3.3    24          16016      30.10.20.0/24[V
] 0            Gi1.30     30.1.19.19   25          16017      8.8.8.8/32[V
]    1302          Gi1.30     30.1.19.19   26          16015      10.10.10.10/32[V
]   \
                                       3030           Gi1.30     30.1.19.19
27          16018      40.8.20.0/24[V
]  0            Gi1.30     30.1.19.19
R1#show mpls forwarding-table vrf VPN_B 7.7.7.7 detail

Local       Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label       Label      or Tunnel Id     Switched      interface
21          21         7.7.7.7/32[V
]    3098          Gi1.13     10.1.3.3          MAC/Encaps=18/26, MRU=1496, Label Stack{16 21}
        0050569E6E6A0050569E59138100000D8847 0001000000015000 VPN route: VPN_B
        No output feature configured
R1#show ip route vrf VPN_B 7.7.7.7

Routing Table: VPN_B Routing entry for 7.7.7.7/32
  Known via "bgp 100", distance 200, metric 130816, type internal
  Last update from 2.2.2.2 00:11:37 ago
  Routing Descriptor Blocks:
  * 2.2.2.2 (default), from 2.2.2.2, 00:11:37 ago
      Route metric is 130816, traffic share count is 1
      AS Hops 0 MPLS label: 21
 MPLS Flags: MPLS Required

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast
Wed May 13 02:39:33.381 UTC
BGP router identifier 19.19.19.19, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 25
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201*> 9.9.9.9/32         30.1.19.1                                  0 100 ?
*>i10.10.10.10/32     20.20.20.20              1    100      0 ?
*> 30.2.9.0/24        30.1.19.1                              0 100 ?
*>i30.10.20.0/24      20.20.20.20              0    100      0 ?
Route Distinguisher: 102:202*> 7.7.7.7/32         30.1.19.1                                  0 100 ?
*>i8.8.8.8/32         20.20.20.20        2570240    100      0 ?
*> 40.2.7.0/24        30.1.19.1                              0 100 ?
*>i40.8.20.0/24       20.20.20.20              0    100      0 ?

Processed 8 prefixes, 8 paths
```

R2#show bgp vpnv4 unicast all

```
BGP table version is 35, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
 *>  9.9.9.9/32       30.2.9.9                 1         32768 ?
*>i 10.10.10.10/32   1.1.1.1                  0    100      0 200 ?
 *>  30.2.9.0/24      0.0.0.0                  0         32768 ?
*>i 30.10.20.0/24    1.1.1.1                  0    100      0 200 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
 *>  7.7.7.7/32       40.2.7.7            130816         32768 ?
*>i 8.8.8.8/32       1.1.1.1                  0    100      0 200 ?
 *>  40.2.7.0/24      0.0.0.0                  0         32768 ?
*>i 40.8.20.0/24     1.1.1.1                  0    100      0 200 ?
```

RP/0/0/CPU0:XR2#show bgp vpnv4 unicast

```
Wed May 13 02:40:20.188 UTC
BGP router identifier 20.20.20.20, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 43
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
*>i9.9.9.9/32         19.19.19.19                   100      0 100 ?
```

```
*> 10.10.10.10/32     30.10.20.10              1         32768 ?
*>i30.2.9.0/24        19.19.19.19                   100       0 100 ?

*> 30.10.20.0/24      0.0.0.0                  0         32768 ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
*>i7.7.7.7/32         19.19.19.19                   100       0 100 ?
*> 8.8.8.8/32         40.8.20.8          2570240         32768 ?
*>i40.2.7.0/24        19.19.19.19                   100       0 100 ?
*> 40.8.20.0/24       0.0.0.0                  0         32768 ?

Processed 8 prefixes, 8 paths
```

R9#show ip route rip

```
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 1 subnets
R        10.10.10.10 [120/1] via 30.2.9.2, 00:00:10, GigabitEthernet1.29
      30.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        30.10.20.0/24 [120/1] via 30.2.9.2, 00:00:10, GigabitEthernet1.29
```

R10#traceroute 9.9.9.9 source loopback 0

```
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
  1 30.10.20.20 4 msec 2 msec 0 msec
  2 20.4.20.4 [MPLS: Labels 16/16011 Exp 0] 27 msec 26 msec 24 msec
  3 20.4.19.19 [MPLS: Label 16011 Exp 0] 24 msec 21 msec 23 msec
  4 30.1.19.1 [MPLS: Label 22 Exp 0] 24 msec 32 msec 29 msec
  5 10.1.3.3 [MPLS: Labels 16/19 Exp 0] 27 msec 28 msec 29 msec
  6 30.2.9.2 [MPLS: Label 19 Exp 0] 22 msec 24 msec 24 msec
  7 30.2.9.9 24 msec *  26 msec
```

R7#traceroute 8.8.8.8 source loopback 0

```
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 40.2.7.2 3 msec 1 msec 0 msec
```

```
2 10.2.3.3 [MPLS: Labels 17/25 Exp 0] 26 msec 23 msec 24 msec
3 10.1.3.1 [MPLS: Label 25 Exp 0] 28 msec 24 msec 24 msec
4 30.1.19.19 [MPLS: Label 16017 Exp 0] 24 msec 24 msec 24 msec
5 20.4.19.4 [MPLS: Labels 17/16005 Exp 0] 30 msec 29 msec 31 msec
6 20.4.20.20 [MPLS: Label 16005 Exp 0] 28 msec 23 msec 24 msec
7 40.8.20.8 24 msec *  26 msec
```

This Inter-AS Layer 3 VPNs design is documented under [Section 10.b in RFC 4364]

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.16 MPLS L3VPN Inter-AS Option C - Multihop VPNv4 EBGP Exchange (pending update)

- Configure IGP routing and LDP in the first AS, which consists of R1, R2, R3, and R5 as follows:
  - Enable OSPF Area 0 on the links between R1 & R3, R1 & R5, R2 & R3, and R3 & R5.
  - Enable OSPF Area 0 on the Loopback0 interfaces of R1, R2, R3, and R5 as passive interfaces.
  - Enable LDP on the links between R1 & R3, R1 & R5, R2 & R3, and R3 & R5.
- Configure IGP routing and LDP in the second AS, which consists of R4, R6, XR1, and XR2 as follows:
  - Use the following IS-IS NET addressing:
    - R4 – 49.0001.0000.0000.0004.00
    - R6 – 49.0001.0000.0000.0006.00
    - XR1 – 49.0001.0000.0000.0019.00
    - XR1 – 49.0001.0000.0000.0020.00
  - Enable IS-IS Level 2 on the links between R4 & R6, R4 & XR1, R4 & XR2, and XR1 & XR2.
  - Advertise the Loopback0 interfaces of R4, R6, XR1, and XR2 into IS-IS Level 2 as passive interfaces.
  - Enable LDP on the links between R4 & R6, R4 & XR1, R4 & XR2, and XR1 & XR2.
- Configure the following VRFs on PE routers R2 and R6 follows:
  - VRF VPN_A:
    - Route Distinguisher: 101:201
    - Route Target Import: 101:201
    - Route Target Export: 101:201
    - Assign this VRF on the links in the 30.0.0.0 network on R2 and R6.
  - VRF VPN_B:
    - Route Distinguisher: 102:202
    - Route Target Import: 102:202

        - Route Target Export: 102:202
        - Assign this VRF on the links in the 40.0.0.0 network on R2 and R6.
- Configure RIPv2 routing for VRF VPN_A as follows:
    - Enable RIP between SW1 and R2.
    - Enable RIP between SW2 and R6.
    - Advertise the Loopback0 networks of SW1 and SW2 into RIP.
- Configure EIGRP routing for VRF VPN_B as follows:
    - Use EIGRP Autonomous System 1.
    - Enable EIGRP between R7 and R2.
    - Enable EIGRP between R8 and R6.
    - Advertise the Loopback0 networks of R7 & R8 into RIP.
- Configure IPv4 Labeled Unicast BGP peerings as follows:
    - R1 is in AS 100, and XR1 is in AS 200.
    - R1 and XR1 should be IPv4 Unicast EBGP peers.
    - Advertise the Loopback0 networks of R2 and R5 into BGP on R1.
    - Advertise the Loopback0 networks of R6 and XR2 into BGP on XR1.
    - Include BGP MPLS Labels advertisements with all four of these networks.
- Redistribute IPv4 Unicast BGP into IGP as follows:
    - R1 should redistribute the Loopback0 networks of R6 and XR2 into OSPF that were learned from XR1.
    - XR1 should redistribute the Loopback0 networks of R2 and R5 into IS-IS that were learned from R1.
- Configure VPNv4 BGP peerings as follows:
    - R2 and R5 should peer in AS 100 using each other’s Loopback0 interfaces.
    - R5 should be a VPNv4 Route Reflector for R2.
    - R6 and XR2 should peer in AS 200 using each other’s Loopback0 interfaces.
    - XR2 should be a VPNv4 Route Reflector for R6.
    - R5 and XR2 should peer multihop EBGP with each other’s Loopback0 interfaces.
    - Do not change the next-hop value of VPNv4 routes advertised from R5 to XR2 and vice versa.
- Redistribute between VPNv4 BGP and the VRF aware IGP processes on R2 and R6.
- When complete, the following reachability should be achieved:
    - Customer routers SW1 and SW2 should have full IP reachability to each other’s networks.
    - Customer routers R7 and R8 should have full IP reachability to each other’s networks.
    - Traceroutes between these networks should indicate that a single end-to-

end Label Switch Path is used.
  - Traceroutes should also indicate that traffic between VPN_A and VPN_B sites does not transit through the VPNv4 Route Reflectors R5 and XR2.

Configuration

```
R1:
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.119
 mpls bgp forwarding
!
router ospf 1
 redistribute bgp 100 subnets
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router bgp 100
 network 2.2.2.2 mask 255.255.255.255
 network 5.5.5.5 mask 255.255.255.255
 neighbor 12.1.19.19 remote-as 200
 neighbor 12.1.19.19 send-label
!
mpls ldp router-id Loopback0

R2:
vrf definition VPN_A
 rd 101:201
 !
 address-family ipv4
 route-target export 101:201
 route-target import 101:201
 exit-address-family
!
vrf definition VPN_B
 rd 102:202
 !
 address-family ipv4
 route-target export 102:202
 route-target import 102:202
 exit-address-family
!
```

```
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.27
 vrf forwarding VPN_B
 ip address 40.2.7.2 255.255.255.0
!
interface FastEthernet0/0.29
 vrf forwarding VPN_A
 ip address 30.2.9.2 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
  redistribute bgp 100
  network 40.0.0.0
  autonomous-system 1
  exit-address-family
!
router ospf 1
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 5.5.5.5 remote-as 100
 neighbor 5.5.5.5 update-source Loopback0
 !
 address-family vpnv4
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended exit-address-
 family
 !
address-family ipv4 vrf VPN_A
no synchronization
redistribute rip exit-address-family
```

```
!
address-family ipv4 vrf VPN_B
 no synchronization
 redistribute eigrp 1 exit-
address-family
!
mpls ldp router-id Loopback0


R3:
interface Loopback0
 ip ospf 1 area 0
!
router ospf 1
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
mpls ldp router-id Loopback0


R4:
interface FastEthernet0/0.46
 ip router isis
!
interface FastEthernet0/0.419
 ip router isis
!
interface FastEthernet0/0.420
 ip router isis
!
router isis
  net 49.0001.0000.0000.0004.00
is-type level-2-only
 passive-interface Loopback0
 mpls ldp autoconfig
!
mpls ldp router-id Loopback0


R5:
interface Loopback0
 ip ospf 1 area 0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

```
 mpls ldp autoconfig area 0
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 20.20.20.20 remote-as 200
 neighbor 20.20.20.20 ebgp-multihop 255
 neighbor 20.20.20.20 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 20.20.20.20 activate
 neighbor 20.20.20.20 send-community extended
 neighbor 20.20.20.20 next-hop-unchanged
exit-address-family
!
mpls ldp router-id Loopback0


R6:
vrf definition VPN_A
 rd 101:201
 !
 address-family ipv4
 route-target export 101:201
 route-target import 101:201
 exit-address-family
!
vrf definition VPN_B
 rd 102:202
 !
 address-family ipv4
 route-target export 102:202
 route-target import 102:202
 exit-address-family
!
interface FastEthernet0/0.46
 ip router isis
!
interface FastEthernet0/0.68
 vrf forwarding VPN_B
 ip address 40.6.8.6 255.255.255.0
!
```

```
interface FastEthernet0/0.610
 vrf forwarding VPN_A
 ip address 30.6.10.6 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
  redistribute bgp 200
  network 40.0.0.0
  autonomous-system 1 exit-
 address-family
!
router isis
 net 49.0001.0000.0000.0006.00
 is-type level-2-only passive-
 interface Loopback0 mpls ldp
 autoconfig
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 200 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 no bgp default ipv4-unicast
 neighbor 20.20.20.20 remote-as 200
 neighbor 20.20.20.20 update-source Loopback0
 !
 address-family vpnv4
  neighbor 20.20.20.20 activate
  neighbor 20.20.20.20 send-community extended
 exit-address-family
 !
address-family ipv4 vrf VPN_A
  redistribute rip
exit-address-family
!
address-family ipv4 vrf VPN_B
  redistribute eigrp 1
exit-address-family
!
mpls ldp router-id Loopback0
```

```
R7:
router eigrp 1
 network 0.0.0.0
 no auto-summary

R8:
router eigrp 1
 network 0.0.0.0
 no auto-summary

SW1:
router rip
 version 2
 network 9.0.0.0
 network 30.0.0.0
 no auto-summary

SW2:
router rip
 version 2
 network 10.0.0.0
 network 30.0.0.0
 no auto-summary

XR1:
route-policy PASS
  pass
end-policy
!
router static
 address-family ipv4 unicast
  12.1.19.1/32 GigabitEthernet0/1/0/0.119
 !
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 address-family ipv4 unicast
  redistribute bgp 200
 mpls ldp auto-config
!
interface Loopback0
 passive
 address-family ipv4 unicast
 !
```

```
!
interface GigabitEthernet0/1/0/0.419
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/1/0/0.1920
  address-family ipv4 unicast
  !
 !
!
router bgp 200
address-family ipv4 unicast
 network 6.6.6.6/32
 network 20.20.20.20/32
 allocate-label all
!
neighbor 12.1.19.1
 remote-as 100
 address-family ipv4 labeled-unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
!
mpls ldp
 router-id Loopback0


XR2:
route-policy PASS
 pass
end-policy
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 address-family ipv4 unicast
  mpls ldp auto-config
 !
interface Loopback0
 passive
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/4/0/0.420
 address-family ipv4 unicast
```

```
 !
!
interface GigabitEthernet0/4/0/0.1920
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family vpnv4 unicast
 !
 neighbor 5.5.5.5
  remote-as 100
  ebgp-multihop 255
 update-source Loopback0
 address-family vpnv4 unicast
  route-policy PASS in
  route-policy PASS out
  next-hop-unchanged
 !
!
neighbor 6.6.6.6
 remote-as 200
 update-source Loopback0
 address-family vpnv4 unicast
   route-reflector-client
  !
 !
!
mpls ldp
 router-id Loopback0
```

Verification

Like previous L3VPN designs, the final verification is always the end-to-end reachability between the final customer sites. In this case, customers in VPN_A and VPN_B have full reachability to their remote sites.

```
SW1#show ip route rip
    10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10 [120/1] via 30.2.9.2, 00:00:21, Vlan29
    30.0.0.0/24 is subnetted, 2 subnets
R       30.6.10.0 [120/1] via 30.2.9.2, 00:00:21, Vlan29
SW1#ping 10.10.10.10 source 9.9.9.9
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
Packet sent with a source address of 9.9.9.9
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
R7#show ip route eigrp
    8.0.0.0/32 is subnetted, 1 subnets
D       8.8.8.8 [90/158720] via 40.2.7.2, 01:06:11, FastEthernet0/0
    40.0.0.0/24 is subnetted, 2 subnets
D       40.6.8.0 [90/30720] via 40.2.7.2, 01:06:11, FastEthernet0/0
R7#ping 8.8.8.8 source 7.7.7.7


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The difference between this design and the previous ones, though, is that a single Label Switched Path (LSP) is used between the multiple Autonomous Systems that are doing Inter-AS exchange. This can be seen from the VPN Label number in the traceroute between the customer sites.

```
R2#traceroute vrf VPN_A 10.10.10.10

Type escape sequence to abort.
Tracing the route to 10.10.10.10
   1    10.2.3.3 [MPLS: Labels 21/24
 Exp 0] 0 msec 4 msec 0 msec    2    10.1.3.1 [MPLS: Labels 22/24
 Exp 0] 0 msec 4 msec 0 msec    3    12.1.19.19 [MPLS: Labels 16001/24
 Exp 0] 4 msec 4 msec 4 msec    4    20.4.19.4 [MPLS: Labels 16/24
 Exp 0] 0 msec 4 msec 0 msec    5    30.6.10.6 [MPLS: Label 24
 Exp 0] 4 msec 0 msec 4 msec
   6    30.6.10.10 0 msec * 0 msec


R2#traceroute vrf VPN_B 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8
   1    10.2.3.3 [MPLS: Labels 21/26
 Exp 0] 0 msec 4 msec 4 msec    2    10.1.3.1 [MPLS: Labels 22/26
 Exp 0] 0 msec 4 msec 0 msec
```

```
   3    12.1.19.19 [MPLS: Labels 16001/26
 Exp 0] 4 msec 4 msec 4 msec    4    20.4.19.4 [MPLS: Labels 16/26
 Exp 0] 0 msec 0 msec 4 msec    5    40.6.8.6 [MPLS: Label 26
 Exp 0] 0 msec 4 msec 0 msec
   6    40.6.8.8 4 msec *   0 msec
```

From the above output, we can see that when traffic comes from the VPN_A site attached to R2 and transits to the VPN_A site attached to R6, which are in separate Autonomous Systems, the VPN Label remains the same end-to-end. For VPN_A specifically, this VPN Label value is 24. For VPN_B the same occurs, maintaining VPN Label value 26.

The reason the LSP remains the same end-to-end is that the VPNv4 route information is also maintained end-to-end, without changes in the next-hop value. If we look at the origination of the prefix 10.10.10.10/32 in VRF VPN_A, first SW2 advertises this to its PE router via IGP. R6 then redistributes this PE-CE IGP learned route into VPNv4 BGP, which generates a local VPN Label value.

```
R6#show ip route vrf VPN_A 10.10.10.10

Routing Table: VPN_A
Routing entry for 10.10.10.10/32 Known via "rip",
 distance 120, metric 1
    Redistributing via rip, bgp 200
    Advertised by bgp 200    Last update from 30.6.10.10
 on FastEthernet0/0.610, 00:00:07 ago
    Routing Descriptor Blocks:
    * 30.6.10.10, from 30.6.10.10, 00:00:07 ago, via FastEthernet0/0.610
        Route metric is 1, traffic share count is 1
R6#show bgp vpnv4 unicast vrf VPN_A 10.10.10.10/32
BGP routing table entry for 101:201:10.10.10.10/32, version 2
Paths: (1 available, best #1, table VPN_A)
    Advertised to update-groups:
        1
    Local
      30.6.10.10 from 0.0.0.0 (6.6.6.6)
        Origin incomplete, metric 1, localpref 100, weight 32768, valid, sourced,
best
        Extended Community: RT:101:201  mpls labels in/out 24/nolabel
```

R6 now takes this VPNv4 route and advertises it to its VPNv4 BGP peer XR2. The next-hop value is set to R6's Loopback0 network 6.6.6.6, because this is the address that R6 and XR2 are peering with for the VPNv4 BGP session.

```
RP/0/3/CPU0:XR2#show bgp vpnv4 unicast rd 101:201 10.10.10.10/32
Wed Mar 21 17:05:53.900 UTC BGP routing table entry for 10.10.10.10/32, Route Distinguisher: 101:201
Versions:
    Process      bRIB/RIB     SendTblVer
    Speaker             2              2
Last Modified: Mar 21 15:50:01.819 for 01:15:52
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    5.5.5.5
  Path #1: Received by speaker 0    Local, (Received from a RR-client)
6.6.6.6
 (metric 20) from 6.6.6.6 (6.6.6.6) Received Label 24
      Origin incomplete, metric 1, localpref 100, valid, internal, best, import-
candidate, not-in-vrf      Extended community: RT:101:201
```

Specifically, the VPNv4 prefix is now 101:201:10.10.10.10/32 with a next-hop value of 6.6.6.6, a Route Target of 101:201, and a VPN Label of 24. XR2 is configured as a VPNv4 Route Reflector for R6, so there are no restrictions as to what type of peers this route can now be advertised to. In this case, XR2 only has one other VPNv4 BGP peer, the multihop EBGP peering to R5. In a practical design, the VPNv4 Route Reflector would then have other VPNv4 iBGP peers for this and other VRFs, but for this example having just one VPNv4 iBGP RR client illustrates the same concept. Specifically, this concept is that normally when a route is learned from an iBGP peer and then advertised to an EBGP peer, the next-hop value is updated to the local peering address.

For this example, this would normally mean that XR2 would set the next-hop of 101:201:10.10.10.10/32 to 20.20.20.20, its own local Loopback0 interface, when the route is advertised to R5. Recall that in VPNv4 routing the next-hop value has an extra significance, because this is where the Label Switch Path terminates. This means that if XR2 were to update the next-hop value to R5, the LSP would change, and a new VPN Label would need to be generated. However, in this case, XR2 and R5 have the command `next-hop-unchanged` on their VPNv4 EBGP peering. The result of this can be seen below, as the next-hop value of the prefix is not changed when advertised between the EBGP peers.

```
RP/0/3/CPU0:XR2#show bgp vpnv4 unicast neighbors 5.5.5.5 advertised-routes
Wed Mar 21 17:12:20.495 UTC
Network          Next Hop     From      AS Path
```

```
Route Distinguisher: 101:201 10.10.10.10/32 6.6.6.6       6.6.6.6     ?

30.6.10.0/24    6.6.6.6     6.6.6.6  ?
Route Distinguisher: 102:202
8.8.8.8/32      6.6.6.6     6.6.6.6  ?
40.6.8.0/24     6.6.6.6     6.6.6.6  ?
R5#show bgp vpnv4 unicast all 10.10.10.10/32
BGP routing table entry for 101:201:10.10.10.10/32
, version 7
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      2
   200 6.6.6.6
 (metric 1) from 20.20.20.20 (20.20.20.20)
      Origin incomplete, localpref 100, valid, external, best      Extended Community: RT:101:201
 mpls labels in/out nolabel/24
```

When R5 receives this route, the next-hop value is still 6.6.6.6, R6's Loopback0. Note that the VPN Label value has not changed. Instead it remains 24, which is what R6 originally allocated for this route. R5 now takes this prefix and advertises it to R2, its VPNv4 iBGP peer. Because already by default the next-hop value is not changed when advertising a route from EBGP peers to iBGP peers (that is, the `next-hop-self` command is not configured), R2 will receive the route with the same original next-hop value of 6.6.6.6.

```
R5#show bgp vpnv4 unicast all neighbors 2.2.2.2 advertised-routes
BGP table version is 9, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop        Metric LocPrf  Weight   Path
Route Distinguisher: 101:201        *> 10.10.10.10/32    6.6.6.6                             0  200 ?
*> 30.6.10.0/24     6.6.6.6                            0    200 ?
Route Distinguisher: 102:202
*> 8.8.8.8/32       6.6.6.6                            0    200 ?
*> 40.6.8.0/24      6.6.6.6                            0    200 ?
R2#show bgp vpnv4 unicast all 10.10.10.10/32

BGP routing table entry for 101:201:10.10.10.10/32, version 12
Paths: (1 available, best #1, table VPN_A)
  Not advertised to any peer
  200 6.6.6.6
 (metric 1) from 5.5.5.5 (5.5.5.5)
```

```
     Origin incomplete, metric 0, localpref 100, valid, internal, best      Extended Community:
 RT:101:201
 mpls labels in/out nolabel/24
```

Now R2 has the route in the local VPNv4 BGP table, and can redistribute it to the VRF aware IGP process of the PE-CE facing link. Nothing about this portion of the design changes as compared to previous L3VPN examples. As long as R2 has a VRF with a Route Target import policy of 101:201, the route can be imported to that VRF table. What is different, however, is that R2 must now form an end-to-end Label Switch Path to the final next-hop value of 6.6.6.6.

Recall that for MPLS L3VPN to work, there are two label values that must work hand in hand. The first is the VPN Label, which tells the final PE router which customer VRF table to do the routing lookup in. The VPN Label is originated by the VPNv4 BGP process. The second is the Transport Label, which tells the core of the MPLS network which exit PE to label switch the traffic toward. The Transport Label is normally originated by IGP+LDP, but it could be allocated via RSVP for MPLS TE or even BGP. Regardless of how this label is allocated, the concept stays the same, that the core of the network must have an end-to-end LSP for the Transport Label to get traffic from the ingress PE to the egress PE. This is where the second part of this design comes in, which is the BGP + Label exchange between the Inter-AS edge routers, or what is sometimes referred to as IPv4 Labeled Unicast BGP.

We know that because BGP does not provide its own transport protocol, normally an IGP like OSPF or IS-IS provides transport between non-connected peers so they can establish their TCP peering. For example, in AS 100 the iBGP peers R2 and R5 are not directly connected. This means that the IGP of OSPF is needed to give them IP reachability between their Loopback0 interfaces before the TCP session can establish. The same concept is true here for the Inter-AS multihop VPNv4 peering that is occurring between R5 and XR2.

For R5 to peer with XR2, it first must have a route to XR2, and vice versa. In this design, the route is learned through a normal IPv4 Unicast BGP peering between the Inter-AS edge routers R1 and XR1.

```
R1#show bgp ipv4 unicast
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop    Metric  LocPrf  Weight  Path
*>  2.2.2.2/32       10.1.3.3    3               32768   i
*>  5.5.5.5/32       10.1.5.5    2               32768   i
```

```
*>  6.6.6.6/32      12.1.19.19  20                  0   200 i
*>  20.20.20.20/32  12.1.19.19  10                  0   200 i


RP/0/0/CPU0:XR1#show bgp ipv4 unicast


Wed Mar 21 17:22:44.879 UTC
BGP router identifier 19.19.19.19, local AS number 200
BGP generic scan interval 60 secs BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 6
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network         Next Hop    Metric  LocPrf  Weight  Path
*>  2.2.2.2/32      12.1.19.1   3                   0   100 i
*>  5.5.5.5/32      12.1.19.1   2                   0   100 i
*>  6.6.6.6/32      20.4.19.4   20              32768   i
*>  20.20.20.20/32  20.19.20.20 10              32768   i

Processed 4 prefixes, 4 paths
```

As seen in the above output, R1 and XR1 are advertising the Loopback0 networks of R2/R5 and R6/XR2, respectively. This is just a normal IPv4 Unicast BGP design where the BGP routers learn their own internal routes via an IGP, and then inject them into the BGP topology with a `network` command under the BGP process. This is the same as how normal IPv4 Unicast BGP routing works for Internet transit. However, in this design there is an additional requirement that there must be an MPLS LSP between the Loopback0 networks of R2 and R6.

To provide this, R1 and XR1 advertise not only the IPv4 Unicast BGP routes to each other, but they also allocate MPLS Labels via IPv4 Unicast BGP. This is different from a VPNv4 BGP allocated label, because a VPNv4 BGP peer is allocating a *VPN Label*, whereas the IPv4 Unicast BGP peer is allocating a *Transport Label*. This is what the `send-label` command does in regular IOS and the `allocate-label-all` under the `address-family ipv4 labeled-unicast` of IOS XR. The specific label allocations can be verified as follows:

```
R1#show ip bgp labels
    Network         Next Hop    In label/Out label     2.2.2.2/32      10.1.3.320
/nolabel    5.5.5.5/32      10.1.5.519
/nolabel    6.6.6.6/32      12.1.19.19      nolabel/16001
```

```
    20.20.20.20/32  12.1.19.19      nolabel/ 16002

RP/0/0/CPU0:XR1#show bgp ipv4 unicast labels
Wed Mar 21 17:26:09.906 UTC
BGP router identifier 19.19.19.19, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 6
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network         Next Hop    Rcvd Label  Local Label*> 2.2.2.2/32       12.1.19.1 20
          16003 *> 5.5.5.5/32       12.1.19.1 19
          16004 *> 6.6.6.6/32       20.4.19.4   nolabel 16001
*> 20.20.20.20/32   20.19.20.20 nolabel 16002


Processed 4 prefixes, 4 paths
```

The above output shows that R1 is creating label value 20 for its BGP prefix 2.2.2.2/32 and label value 19 for prefix 5.5.5.5/32. Likewise, XR1 is allocating label value 16001 for prefix 6.6.6.6/32 and label value 16002 for prefix 20.20.20.20/32. This now means that the edge routers agree on a Label Switch Path to reach routes that would normally be internal to their own network. In other words, for Inter-AS Option C to work, the Service Providers have to leak their *internal* routing information to each other via IPv4 Labeled Unicast BGP.

The next step is to figure out how to form the LSP within the Autonomous Systems, because in this example the routers in the transit path, such as R2, R3, R4, R5, R6, and XR2, are not running IPv4 Unicast BGP. One option would be to turn regular BGP on everywhere and exchang the BGP + Label prefixes, but a simpler design is used in this example. Because for Intra-AS reachability the routers are already running IGP + LDP, we can simply redistribute the BGP + Label learned route into IGP and have LDP create a label for it. This allows everyone to label switch traffic to the Inter-AS edge routers, and then the Inter-AS edge routers (R1 and XR1 in this case) can use the BGP-derived labels to label switch traffic on the connected Inter-AS link. This LSP can be verified end-to-end as follows:

```
R2#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32 Known via "ospf 1",
 distance 110, metric 1
    Tag 200, type extern 2, forward metric 2
```

```
    Last update from 10.2.3.3 on FastEthernet0/0.23, 01:51:05 ago
    Routing Descriptor Blocks:    * 10.2.3.3
, from 1.1.1.1, 01:51:05 ago, via FastEthernet0/0.23
        Route metric is 1, traffic share count is 1
        Route tag 200
R2#show mpls forwarding-table 6.6.6.6
Local   Outgoing    Prefix           Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id     Switched    interface 23 21
        6.6.6.6/32      0            Fa0/0.23 10.2.3.3
```

R2 learns the route to R6's Loopback – 6.6.6.6/32 – via External OSPF, and via LDP with a Transport Label value of 21, which was allocated by R3.

```
R3#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32 Known via "ospf 1",
 distance 110, metric 1
    Tag 200, type extern 2, forward metric 1
    Last update from 10.1.3.1 on FastEthernet0/0.13, 01:51:41 ago
    Routing Descriptor Blocks:    * 10.1.3.1
, from 1.1.1.1, 01:51:41 ago, via FastEthernet0/0.13
        Route metric is 1, traffic share count is 1
        Route tag 200
R3#show mpls forwarding-table 6.6.6.6
Local   Outgoing    Prefix           Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id     Switched    interface 21 22
         6.6.6.6/32      251862      Fa0/0.13 10.1.3.1
```

R3 learns the route to R6's Loopback via External OSPF, and via LDP with a Transport Label value of 22, which was allocated by R1.

```
R1#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32 Known via "bgp 100",
 distance 20, metric 20
    Tag 200, type external Redistributing via ospf 1
    Advertised by ospf 1 subnets
    Last update from 12.1.19.19 01:59:43 ago
    Routing Descriptor Blocks:    * 12.1.19.19
, from 12.1.19.19, 01:59:43 ago
        Route metric is 20, traffic share count is 1
        AS Hops 1
        Route tag 200
        MPLS label: 16001
R1#show mpls forwarding-table 6.6.6.6
```

```
Local   Outgoing    Prefix          Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id    Switched    interface 22         16001
    6.6.6.6/32        253446      Fa0/0.119 12.1.19.19
R1#show ip bgp labels
    Network         Next Hop    In label/Out label
    2.2.2.2/32      10.1.3.3      20/nolabel
    5.5.5.5/32      10.1.5.5      19/nolabel    6.6.6.6/32      12.1.19.19    nolabel/16001

    20.20.20.20/32  12.1.19.19    nolabel/16002
```

R1 learns the route to R6's Loopback via External BGP. This means that if traffic toward the destination is going to be label switched, it has to use a label that was derived from BGP. This is essentially where R1 ties the BGP allocated label from XR1 together with its locally allocated label via LDP. Traffic on the LSP toward 6.6.6.6 will use the incoming LDP label of 22 and the outgoing BGP label of 16001.

```
RP/0/0/CPU0:XR1#show ip route 6.6.6.6
Wed Mar 21 17:36:56.377 UTC

Routing entry for 6.6.6.6/32 Known via "isis 1",
 distance 115, metric 20, type level-2
    Installed Mar 21 15:33:48.514 for 02:03:08
    Routing Descriptor Blocks 20.4.19.4,
 from 6.6.6.6, via GigabitEthernet0/1/0/0.419
        Route metric is 20
    No advertising protos.

RP/0/0/CPU0:XR1#show mpls forwarding prefix 6.6.6.6/32
Wed Mar 21 17:37:09.876 UTC
Local   Outgoing    Prefix              Outgoing        Next Hop        Bytes
Label   Label       or ID               Interface                       Switched
------  ----------- ------------------ ------------     --------------- ------------ 16001   16
          6.6.6.6/32          Gi0/1/0/0.419 20.4.19.4
  206296
RP/0/0/CPU0:XR1#show bgp ipv4 unicast labels
Wed Mar 21 17:37:28.722 UTC
BGP router identifier 19.19.19.19, local AS number 200
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 6
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop         Rcvd Label  Local Label
*> 2.2.2.2/32       12.1.19.1        20          16003
*> 5.5.5.5/32       12.1.19.1        19          16004
*> 6.6.6.6/32      20.4.19.4       nolabel     16001

*> 20.20.20.20/32   20.19.20.20      nolabel     16002

Processed 4 prefixes, 4 paths
```

XR1 learns the route to R6's Loopback via IS-IS. This means that if traffic toward the destination is going to be label switched, it has to use a label that was derived from LDP. This is where XR1 ties the BGP allocated label back to the LDP label allocated from the IGP route. Traffic on the LSP towards 6.6.6.6 will use the incoming BGP label of 16001 and the outgoing LDP label of 16.

The process then continues below on R4 who is the Penultimate (next to last) Hop for R6's Loopback0. This makes R4 pop the top label off the stack and forward the remaining payload towards R6.

```
R4#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32 Known via "isis",
 distance 115, metric 10, type level-2
    Redistributing via isis
    Last update from 20.4.6.6 on FastEthernet0/0.46, 02:17:46 ago
    Routing Descriptor Blocks:    * 20.4.6.6
, from 6.6.6.6, 02:17:46 ago, via FastEthernet0/0.46
        Route metric is 10, traffic share count is 1
R4#show mpls forwarding-table 6.6.6.6
Local    Outgoing    Prefix          Bytes Label Outgoing    Next Hop
Label    Label       or Tunnel Id    Switched    interface 16 Pop Label
   6.6.6.6/32      250037      Fa0/0.46    20.4.6.6
```

Another interesting point about this design is that even though the VPNv4 Route Reflectors are in the path of the control plane advertisements for the VPNv4 routes, they are not in the actual data forwarding plane. This can be seen from the traceroutes below; neither R5 nor XR2's IP addresses appear as hops in the path.

```
R6#traceroute vrf VPN_A 9.9.9.9

Type escape sequence to abort.
Tracing the route to 9.9.9.9

   1    20.4.6.4 [MPLS: Labels 20/28 Exp 0] 4 msec 0 msec 4 msec
   2    20.4.19.19 [MPLS: Labels 16003/28 Exp 0] 4 msec 0 msec 4 msec
```

```
   3    12.1.19.1 [MPLS: Labels 20/28 Exp 0] 4 msec 0 msec 0 msec
   4    10.1.3.3 [MPLS: Labels 19/28 Exp 0] 4 msec 0 msec 4 msec
   5    30.2.9.2 [MPLS: Label 28 Exp 0] 0 msec 4 msec 0 msec
   6    30.2.9.9 4 msec *   0 msec
R6#traceroute vrf VPN_B 7.7.7.7


Type escape sequence to abort.
Tracing the route to 7.7.7.7

   1    20.4.6.4 [MPLS: Labels 20/27 Exp 0] 0 msec 4 msec 0 msec
   2    20.4.19.19 [MPLS: Labels 16003/27 Exp 0] 8 msec 4 msec 0 msec
   3    12.1.19.1 [MPLS: Labels 20/27 Exp 0] 4 msec 0 msec 4 msec
   4    10.1.3.3 [MPLS: Labels 19/27 Exp 0] 0 msec 4 msec 0 msec
   5    40.2.7.2 [MPLS: Label 27 Exp 0] 4 msec 0 msec 0 msec
   6    40.2.7.7 4 msec *   0 msec
```

The reason this is occurring is because the original next-hop values are maintained end-to-end, the Transport Labels used on the LSP between R2 and R6 are for each other's Loopback0 interfaces, instead of the Loopback0 interfaces of the Route Reflectors. If we were to change this design so that R5 and XR2 were updating the next-hop values in their VPNv4 advertisements we would see that the Route Reflectors would then begin to collect all the traffic in the data plane. This fact can be demonstrated as follows:

```
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.R5(config)#router bgp 100
R5(config-router)#address-family vpnv4 unicast
R5(config-router-af)#no neighbor 20.20.20.20 next-hop-unchanged
R5(config-router-af)#end
R5#
%SYS-5-CONFIG_I: Configured from console by consoleR5#clear bgp vpnv4 unicast * out
R5#clear bgp vpnv4 unicast * in
R5#

RP/0/3/CPU0:XR2#config t
Wed Mar 21 17:45:49.067 UTCRP/0/3/CPU0:XR2(config)#router bgp 200
RP/0/3/CPU0:XR2(config-bgp)#neighbor 5.5.5.5
 RP/0/3/CPU0:XR2(config-bgp-nbr)# address-family vpnv4 unicast
 RP/0/3/CPU0:XR2(config-bgp-nbr-af)#no next-hop-unchanged
 RP/0/3/CPU0:XR2(config-bgp-nbr-af)#commit
RP/0/3/CPU0:Mar 21 17:46:08.885 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xr2'. Use 'show configuration commit changes
1000000092' to view the changes.
RP/0/3/CPU0:XR2(config-bgp-nbr-af)#end
```

```
RP/0/3/CPU0:Mar 21 17:46:08.927 : config[65734]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xr2RP/0/3/CPU0:XR2#clear bgp vpnv4 unicast * soft in
Wed Mar 21 17:46:16.218 UTCRP/0/3/CPU0:XR2#clear bgp vpnv4 unicast * soft out


Wed Mar 21 17:46:17.636 UTC
```

Now R2 will see the next-hop value of the remote VPN_A and VPN_B sites' routes as XR2, and R6 will see the next-hop as R5.

```
R2#show bgp vpnv4 unicast all

BGP table version is 19, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf    Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
*> 9.9.9.9/32       30.2.9.9                 1            32768  ?
*>i10.10.10.10/32   20.20.20.20              0 100            0  200   ?

*> 30.2.9.0/24      0.0.0.0                  0            32768  ?
*>i30.6.10.0/24     20.20.20.20              0 100            0  200   ?

Route Distinguisher: 102:202 (default for vrf VPN_B)
*> 7.7.7.7/32       40.2.7.7                  156160      32768  ?
*>i8.8.8.8/32       20.20.20.20              0 100            0  200   ?

*> 40.2.7.0/24      0.0.0.0                  0           32768   ?
*>i40.6.8.0/24      20.20.20.20              0 100            0  200   ?

R6#show bgp vpnv4 unicast all

BGP table version is 17, local router ID is 6.6.6.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop    Metric LocPrf     Weight Path
Route Distinguisher: 101:201 (default for vrf VPN_A)
*>i9.9.9.9/32       5.5.5.5                 100          0   100 ?

*> 10.10.10.10/32   30.6.10.10      1           32768   ?
*>i30.2.9.0/24       5.5.5.5                100          0   100 ?

*> 30.6.10.0/24     0.0.0.0         0           32768   ?
Route Distinguisher: 102:202 (default for vrf VPN_B)
*>i7.7.7.7/32       5.5.5.5                 100          0   100 ?

*> 8.8.8.8/32       40.6.8.8    156160          32768   ?
*>i40.2.7.0/24       5.5.5.5                100          0   100 ?
```

```
*> 40.6.8.0/24      0.0.0.0         0           32768   ?
```

This now means that R5 and XR2 will be in the data plane path for the traffic between the customer sites.

```
R2#traceroute vrf VPN_A 10.10.10.10

Type escape sequence to abort.
Tracing the route to 10.10.10.10

  1 10.2.3.3 [MPLS: Labels 20/16007 Exp 0] 4 msec 0 msec 4 msec
  2 10.1.3.1 [MPLS: Labels 23/16007 Exp 0] 4 msec 0 msec 4 msec
  3 12.1.19.19 [MPLS: Labels 16002/16007 Exp 0] 4 msec 4 msec 4 msec
4 20.19.20.20 [MPLS: Label 16007 Exp 0] 4 msec 4 msec 0 msec
  5 20.4.20.4 [MPLS: Labels 16/24 Exp 0] 0 msec 4 msec 0 msec
  6 30.6.10.6 [MPLS: Label 24 Exp 0] 4 msec 4 msec 0 msec
  7 30.6.10.10 4 msec * 0 msec
R6#traceroute vrf VPN_B 7.7.7.7

Type escape sequence to abort.
Tracing the route to 7.7.7.7

1   20.4.6.4 [MPLS: Labels 21/24 Exp 0] 0 msec 4 msec 0 msec
2   20.4.19.19 [MPLS: Labels 16004/24 Exp 0] 4 msec 4 msec 4 msec
3   12.1.19.1 [MPLS: Labels 19/24 Exp 0] 0 msec 4 msec 0 msec
4   10.1.5.5 [MPLS: Label 24 Exp 0] 0 msec 4 msec 0 msec

5   10.3.5.3 [MPLS: Labels 19/27 Exp 0] 4 msec 0 msec 4 msec
6   40.2.7.2 [MPLS: Label 27 Exp 0] 0 msec 4 msec 0 msec
7   40.2.7.7 0 msec *   0 msec
```

In a real-world design, this behavior is undesirable because not only is the route now suboptimal (R2 > R3 > R1 > XR1 > XR2 > R4 > R6 instead of R2 > R3 > R1 > XR1 > R4 > R6) but it means that the route reflectors who are potentially servicing hundreds or thousands of PEs now need to not only maintain the routing control plane for all of them, but actually perform the data forwarding. By using the `next-hop-unchanged` command, this removes the RR’s need to be in the data plane when there a more optimal path that avoids the RR is available.

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.17 MPLS L3VPN Inter-AS Option C with iBGP + Label (pending update)

- Configure IGP routing and LDP in the first AS, which consists of R1, R2, R3, and R5 as follows:
    - Enable OSPF Area 0 on the links between R1 & R3, R1 & R5, R2 & R3, and R3 & R5.
    - Enable OSPF Area 0 on the Loopback0 interfaces of R1, R2, R3, and R5 as passive interfaces.
    - Enable LDP on the links between R1 & R3, R1 & R5, R2 & R3, and R3 & R5.
- Configure IGP routing and LDP in the second AS, which consists of R4, R6, XR1, and XR2 as follows:
    - Use the following IS-IS NET addressing:
        - R4 – 49.0001.0000.0000.0004.00
        - R6 – 49.0001.0000.0000.0006.00
        - XR1 – 49.0001.0000.0000.0019.00
        - XR1 – 49.0001.0000.0000.0020.00
    - Enable IS-IS Level 2 on the links between R4 & R6, R4 & XR1, R4 & XR2, and XR1 & XR2.
    - Advertise the Loopback0 interfaces of R4, R6, XR1, and XR2 into IS-IS Level 2 as passive interfaces.
    - Enable LDP on the links between R4 & R6, R4 & XR1, R4 & XR2, and XR1 & XR2.
- Configure the following VRFs on PE routers R2 and R6 follows:
    - VRF VPN_A:
        - Route Distinguisher: 101:201
        - Route Target Import: 101:201
        - Route Target Export: 101:201
        - Assign this VRF on the links in the 30.0.0.0 network on R2 and R6.
    - VRF VPN_B:
        - Route Distinguisher: 102:202
        - Route Target Import: 102:202

    - Route Target Export: 102:202
    - Assign this VRF on the links in the 40.0.0.0 network on R2 and R6.
- Configure RIPv2 routing for VRF VPN_A as follows:
  - Enable RIP between SW1 and R2.
  - Enable RIP between SW2 and R6.
  - Advertise the Loopback0 networks of SW1 and SW2 into RIP.
- Configure EIGRP routing for VRF VPN_B as follows:
  - Use EIGRP Autonomous System 1.
  - Enable EIGRP between R7 and R2.
  - Enable EIGRP between R8 and R6.
  - Advertise the Loopback0 networks of R7 and R8 into EIGRP.
- Configure IPv4 Labeled Unicast BGP peerings as follows:
  - R1, R2, R3, and R5 are in AS 100.
  - R4, R6, XR1, and XR2 are in AS 200.
  - R1 should be an IPv4 Unicast iBGP Route Reflector for R2, R3, and R5.
  - XR1 should be an IPv4 Unicast iBGP Route Reflector for R4, R6, and XR2.
  - R1 and XR1 should be IPv4 Unicast EBGP peers.
  - Advertise the Loopback0 networks of R2 and R5 into BGP on R1.
  - Advertise the Loopback0 networks of R6 and XR2 into BGP on XR1.
  - Include BGP MPLS Labels advertisements everywhere for these networks.
- Configure VPNv4 BGP peerings as follows:
  - R2 and R5 should peer in AS 100 using each other’s Loopback0 interfaces.
  - R5 should be a VPNv4 Route Reflector for R2.
  - R6 and XR2 should peer in AS 200 using each other’s Loopback0 interfaces.
  - XR2 should be a VPNv4 Route Reflector for R6.
  - R5 and XR2 should peer multihop EBGP with each other’s Loopback0 interfaces.
  - Do not change the next-hop value of VPNv4 routes advertised from R5 to XR2 and vice versa.
- Redistribute between VPNv4 BGP and the VRF aware IGP processes on R2 and R6.
- When complete, the following reachability should be achieved:
  - Customer routers SW1 and SW2 should have full IP reachability to each other’s networks.
  - Customer routers R7 and R8 should have full IP reachability to each other’s networks.
  - Traceroutes between these networks should indicate that a single end-to-end Label Switch Path is used.
  - Traceroutes should also indicate that traffic between VPN_A and VPN_B

sites does not transit through the VPNv4 Route Reflectors R5 and XR2.

Configuration

```
R1:
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.119
 mpls bgp forwarding
!
router ospf 1
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router bgp 100
 network 2.2.2.2 mask 255.255.255.255
 network 5.5.5.5 mask 255.255.255.255
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 2.2.2.2 route-reflector-client
 neighbor 2.2.2.2 next-hop-self
 neighbor 2.2.2.2 send-label
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 3.3.3.3 route-reflector-client
 neighbor 3.3.3.3 next-hop-self
 neighbor 3.3.3.3 send-label
 neighbor 5.5.5.5 remote-as 100
 neighbor 5.5.5.5 update-source Loopback0
 neighbor 5.5.5.5 route-reflector-client
 neighbor 5.5.5.5 next-hop-self
 neighbor 5.5.5.5 send-label
 neighbor 12.1.19.19 remote-as 200
 neighbor 12.1.19.19 send-label
!
mpls ldp router-id Loopback0

R2:
vrf definition VPN_A
 rd 101:201
 !
 address-family ipv4
```

```
 route-target export 101:201
 route-target import 101:201
 exit-address-family
!
vrf definition VPN_B
 rd 102:202
 !
 address-family ipv4
 route-target export 102:202
 route-target import 102:202
 exit-address-family
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.27
 vrf forwarding VPN_B
 ip address 40.2.7.2 255.255.255.0
!
interface FastEthernet0/0.29
 vrf forwarding VPN_A
 ip address 30.2.9.2 255.255.255.0
!
router eigrp 65535
 !
address-family ipv4 vrf VPN_B
 redistribute bgp 100
 network 40.0.0.0
 autonomous-system 1 exit-
address-family
!
router ospf 1
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 100 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 100
```

```
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 5.5.5.5 remote-as 100
 neighbor 5.5.5.5 update-source Loopback0
!
address-family ipv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-label
exit-address-family
!
address-family vpnv4
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
exit-address-family
!
address-family ipv4 vrf VPN_A
 redistribute rip exit-
address-family
!
address-family ipv4 vrf VPN_B
 redistribute eigrp 1
exit-address-family
!
mpls ldp router-id Loopback0

R3:
interface Loopback0
 ip ospf 1 area 0
!
router ospf 1
 passive-interface Loopback0
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router bgp 100
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
!
address-family ipv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-label
 no auto-summary exit-address-family
!
mpls ldp router-id Loopback0
```

```
R4:
interface FastEthernet0/0.46
 ip router isis
!
interface FastEthernet0/0.419
 ip router isis
!
interface FastEthernet0/0.420
 ip router isis
!
router isis
 net 49.0001.0000.0000.0004.00
 is-type level-2-only
 passive-interface Loopback0
 mpls ldp autoconfig
!
router bgp 200
 neighbor 19.19.19.19 remote-as 200
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family ipv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-label
 exit-address-family
 !
 mpls ldp router-id Loopback0

R5:
interface Loopback0
 ip ospf 1 area 0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls ldp autoconfig area 0
!
router bgp 100
 no bgp default ipv4-unicast
 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
 neighbor 20.20.20.20 remote-as 200
 neighbor 20.20.20.20 ebgp-multihop 255
 neighbor 20.20.20.20 update-source Loopback0
 !
```

```
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-label
 exit-address-family
 !
 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 20.20.20.20 activate
  neighbor 20.20.20.20 send-community extended
  neighbor 20.20.20.20 next-hop-unchanged
 exit-address-family
!
mpls ldp router-id Loopback0

R6:
vrf definition VPN_A
 rd 101:201
 !
 address-family ipv4
 route-target export 101:201
 route-target import 101:201
 exit-address-family
!
vrf definition VPN_B
 rd 102:202
 !
 address-family ipv4
 route-target export 102:202
 route-target import 102:202
 exit-address-family
!
interface FastEthernet0/0.46
 ip router isis
!
interface FastEthernet0/0.68
 vrf forwarding VPN_B
 ip address 40.6.8.6 255.255.255.0
!
interface FastEthernet0/0.610
 vrf forwarding VPN_A
 ip address 30.6.10.6 255.255.255.0
!
router eigrp 65535
 !
 address-family ipv4 vrf VPN_B
```

```
  redistribute bgp 200
  network 40.0.0.0
  autonomous-system 1
 exit-address-family
!
router isis
 net 49.0001.0000.0000.0006.00
 is-type level-2-only
 passive-interface Loopback0
 mpls ldp autoconfig
!
router rip
 !
 address-family ipv4 vrf VPN_A
  redistribute bgp 200 metric 1
  network 30.0.0.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 200
 neighbor 19.19.19.19 update-source Loopback0
 neighbor 20.20.20.20 remote-as 200
 neighbor 20.20.20.20 update-source Loopback0
 !
 address-family ipv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-label exit-
 address-family
 !
 address-family vpnv4
  neighbor 20.20.20.20 activate
  neighbor 20.20.20.20 send-community extended exit-
 address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family
 !
 address-family ipv4 vrf VPN_B
  redistribute eigrp 1
 exit-address-family
!
mpls ldp router-id Loopback0
```

```
R7:
router eigrp 1
 network 0.0.0.0
 no auto-summary

R8:
router eigrp 1
 network 0.0.0.0
 no auto-summary

SW1:
router rip
 version 2
 network 9.0.0.0
 network 30.0.0.0
 no auto-summary

SW2:
router rip
 version 2
 network 10.0.0.0
 network 30.0.0.0
 no auto-summary

XR1:
route-policy PASS
  pass
end-policy
!
router static
 address-family ipv4 unicast
  12.1.19.1/32 GigabitEthernet0/1/0/0.119
 !
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 address-family ipv4 unicast
  redistribute bgp 200
 mpls ldp auto-config
!
interface Loopback0
 passive
 address-family ipv4 unicast
 !
```

```
!
interface GigabitEthernet0/1/0/0.419
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/1/0/0.1920
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family ipv4 unicast
  network 6.6.6.6/32
  network 20.20.20.20/32
  allocate-label all
 !
 neighbor 4.4.4.4
  remote-as 200
  update-source Loopback0
  address-family ipv4 labeled-unicast
   route-reflector-client next-
   hop-self
 !
!
neighbor 6.6.6.6
 remote-as 200
 update-source Loopback0
 address-family ipv4 labeled-unicast route-
  reflector-client
   next-hop-self
!
!
neighbor 12.1.19.1
 remote-as 100
 address-family ipv4 labeled-unicast
  route-policy PASS in
  route-policy PASS out
 !
!
neighbor 20.20.20.20
 remote-as 200
 update-source Loopback0
 address-family ipv4 labeled-unicast route-
   reflector-client
   next-hop-self
  !
```

```
 !
!
mpls ldp
 router-id Loopback0

XR2:
route-policy PASS
  pass
end-policy
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 address-family ipv4 unicast
  mpls ldp auto-config
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
 !
!
interface GigabitEthernet0/4/0/0.420
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/4/0/0.1920
  address-family ipv4 unicast
  !
 !
!
router bgp 200
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 5.5.5.5
  remote-as 100
  ebgp-multihop 255
  update-source Loopback0
  address-family vpnv4 unicast
   next-hop-unchanged route-
   policy PASS in route-
   policy PASS out
 !
!
neighbor 6.6.6.6
```

```
 remote-as 200
 update-source Loopback0
 address-family vpnv4 unicast
  route-reflector-client
 !
!
neighbor 19.19.19.19
  remote-as 200
  update-source Loopback0
  address-family ipv4 labeled-unicast
  !
 !
!
mpls ldp
 router-id Loopback0
```

Verification

This example is similar to the previous MPLS L3VPN Inter-AS Option C design, with the exception that now BGP + Label is used everywhere to build Transport Labels between the Autonomous Systems instead of redistributing BGP into IGP and using LDP derived labels. This design is also used to help dispel a common misconception about where you do or do not need to add the `send-label` command in regular IPv4 Unicast BGP. The key question to always ask yourself is, "How is the next-hop of the VPNv4 route being learned?" If the next-hop is being learned via IGP, you need to use an IGP based label (LDP or MPLS TE) to reach it, but if the next-hop is being learned via BGP, you need to use a BGP-based label.

In this case, all routers in AS 100 are peering IPv4 Unicast BGP with R1, and all routers in AS 200 are peering with XR1. R1 and XR1 are originating the Loopback0 networks of R2/R5 and R6/XR2 into BGP, respectively. No redistribution of regular IPv4 Unicast BGP is occurring, so everyone should be learning these routes through regular BGP, as seen below.

```
R1#show ip route bgp | begin ^Gateway
Gateway of last resort is not set

    6.0.0.0/32 is subnetted, 1 subnets
B       6.6.6.6 [20/20] via 12.1.19.19, 00:33:33
    20.0.0.0/32 is subnetted, 1 subnets
B       20.20.20.20 [20/10] via 12.1.19.19, 00:33:33
R2#show ip route bgp | begin ^Gateway
Gateway of last resort is not set
```

```
    6.0.0.0/32 is subnetted, 1 subnets
B       6.6.6.6 [200/20] via 1.1.1.1, 00:32:17
    20.0.0.0/32 is subnetted, 1 subnets
B       20.20.20.20 [200/10] via 1.1.1.1, 00:32:17
R3#show ip route bgp | begin ^Gateway
Gateway of last resort is not set

    6.0.0.0/32 is subnetted, 1 subnets
B       6.6.6.6 [200/20] via 1.1.1.1, 00:32:45
    20.0.0.0/32 is subnetted, 1 subnets
B       20.20.20.20 [200/10] via 1.1.1.1, 00:32:45
R4#show ip route bgp | begin ^Gateway
Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
B       2.2.2.2 [200/3] via 19.19.19.19, 00:28:19
    5.0.0.0/32 is subnetted, 1 subnets
B       5.5.5.5 [200/2] via 19.19.19.19, 00:28:19
R4#

R5#show ip route bgp | begin ^Gateway
Gateway of last resort is not set

    6.0.0.0/32 is subnetted, 1 subnets
B       6.6.6.6 [200/20] via 1.1.1.1, 00:32:17
    20.0.0.0/32 is subnetted, 1 subnets
B       20.20.20.20 [200/10] via 1.1.1.1, 00:32:17
R6#show ip route bgp | begin ^Gateway
Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
B       2.2.2.2 [200/3] via 19.19.19.19, 00:28:19
    5.0.0.0/32 is subnetted, 1 subnets
B       5.5.5.5 [200/2] via 19.19.19.19, 00:28:19
RP/0/0/CPU0:XR1#show route bgp
Wed Mar 21 19:08:48.316 UTC

B   2.2.2.2/32 [20/3] via 12.1.19.1, 00:34:13
B   5.5.5.5/32 [20/2] via 12.1.19.1, 00:34:13
RP/0/3/CPU0:XR2#show route bgp

Wed Mar 21 19:08:56.141 UTC

B   2.2.2.2/32 [200/3] via 19.19.19.19, 00:29:05
```

```
B   5.5.5.5/32 [200/2] via 19.19.19.19, 00:29:05
```

Note that in the routing tables only the BGP routes from the remote AS are installed, and not the BGP routes from the local AS. This is because the Loopbacks of R2, R5, R6, and XR2 are advertised into both IGP and iBGP, and IGP has a lower administrative distance than iBGP. The routes will still be in the BGP table, but won't be installed in the routing table. This is what the RIB Failure indicates in the `show ip bgp` output.

```
R3#show ip bgp

BGP table version is 8, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network            Next Hop    Metric LocPrf  Weight   Path
r>i2.2.2.2/32       1.1.1.1         3   100         0   i
r>i5.5.5.5/32       1.1.1.1         2   100         0   i
*>i6.6.6.6/32       1.1.1.1         20  100         0   200 i
*>i20.20.20.20/32   1.1.1.1         10  100         0   200 i
```

Now that we know at least that the routes to the remote AS are being learned via BGP, let's look at how this affects the Label Switch Path of traffic going between the VPN_A and VPN_B customer sites.

```
R2#traceroute vrf VPN_A 10.10.10.10

Type escape sequence to abort.
Tracing the route to 10.10.10.10
   1    10.2.3.3 [MPLS: Labels 16/22/24
 Exp 0] 0 msec 0 msec 4 msec   2    10.1.3.1 [MPLS: Labels 22/24
 Exp 0] 0 msec 4 msec 0 msec   3    12.1.19.19 [MPLS: Labels 16001/24
 Exp 0] 4 msec 4 msec 4 msec   4    20.4.19.4 [MPLS: Labels 16/24
 Exp 0] 0 msec 4 msec 4 msec   5    30.6.10.6 [MPLS: Label 24
 Exp 0] 0 msec 4 msec 0 msec
   6    30.6.10.10 4 msec * 0 msec
```

R2's traceroute from the local VPN_A site to the remote VPN_A site on R6 indicates that the traffic goes from R2 > R3 > R1 > XR1 > R4 > R6 > CE. This is as expected, because like in the last example, the VPNv4 Route Reflectors (R5 and XR2) are not updating the VPNv4 next-hop value. This means that although they are in the control plane for the VPNv4 route advertisement, they are not actually in the data plane.

What is different about the above traceroute in this example vs. the last one though is that when R2 sends traffic to the first hop of R3, a three-label stack of 16/22/24 is used instead of a normal two label stack commonly seen in L3VPN. To see why this is happening we need to look at the VPNv4 route recursion process in more detail for this destination.

```
R2#show bgp vpnv4 unicast vrf VPN_A 10.10.10.10/32
BGP routing table entry for 101:201:10.10.10.10/32, version 40
Paths: (1 available, best #1, table VPN_A)
    Not advertised to any peer
    200 6.6.6.6  (metric 3) from 5.5.5.5
 (5.5.5.5)
        Origin incomplete, metric 0, localpref 100, valid, internal, best
        Extended Community: RT:101:201 mpls labels in/out nolabel/24
```

The first step is to look at the VPNv4 route itself. Like in the last example, this route is being learned from the VPNv4 Route Reflector R5, but the next-hop value points at 6.6.6.6 (R6's Loopback0). We already know the VPN Label will be 24 from this output, but to find a transport label for 6.6.6.6 we next need to look in the global routing table.

```
R2#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32 Known via "bgp 100"
, distance 200, metric 20
    Tag 200, type internal
    Last update from 1.1.1.1 00:40:21 ago
    Routing Descriptor Blocks:     * 1.1.1.1
, from 1.1.1.1, 00:40:21 ago
        Route metric is 20, traffic share count is 1
        AS Hops 1
        Route tag 200  MPLS label: 22
```

R2 sees the next-hop value 6.6.6.6 learned via iBGP from R1. In the previous example, this next-hop was learned from OSPF due to the BGP to IGP redistribution on the Inter-AS edge routers. Because this is a BGP-learned route, it means that we have to use a BGP-derived label in the LSP. This is seen in the output above as label number 22. Again note that this is a *transport label* and not a *VPN label*. Even though we have found the label number, the route recursion process is not complete because we haven't found the outgoing interface. We must now do a lookup on the next-hop of 1.1.1.1 until route recursion eventually points at a physical interface.

```
R2#show ip route 1.1.1.1
Routing entry for 1.1.1.1/32 Known via "ospf 1"
, distance 110, metric 3, type intra area
    Last update from 10.2.3.3 on FastEthernet0/0.23, 03:37:41 ago
    Routing Descriptor Blocks:     * 10.2.3.3, from 1.1.1.1, 03:37:41 ago, via FastEthernet0/0.23

        Route metric is 3, traffic share count is 1
```

The next recursion is the last one needed, because the next-hop 1.1.1.1 is learned from the IGP peer 10.2.3.3 on the connected link Fa0/0.23. When R2 goes to actually encapsulate the packet, however, it means that two transport labels will be used in the stack. The topmost label will be for the last recursion of 1.1.1.1 toward R3, the next label will be for the BGP route recursion of 6.6.6.6 toward 1.1.1.1, and the bottom VPN label will be for the final destination. We can verify this from the outputs below:

```
R2#show mpls forwarding-table
Local   Outgoing     Prefix            Bytes Label      Outgoing    Next Hop
Label   Label        or Tunnel Id      Switched         interface
16      18           5.5.5.5/32        0                Fa0/0.23    10.2.3.3
17      Pop Label    3.3.3.3/32        0                Fa0/0.23    10.2.3.318  16               1.1.1.1/32
        0               Fa0/0.23    10.2.3.3
19      Pop Label    10.3.5.0/24       0                Fa0/0.23    10.2.3.3
20      17           10.1.5.0/24       0                Fa0/0.23    10.2.3.3
21      Pop Label    10.1.3.0/24       0                Fa0/0.23    10.2.3.3
24      No Label     30.2.9.0/24[V]    2998             aggregate/VPN_A
25      No Label     40.2.7.0/24[V]    0                aggregate/VPN_B
27      No Label     7.7.7.7/32[V]     228212           Fa0/0.27    40.2.7.7
28      No Label     9.9.9.9/32[V]     0                Fa0/0.29    30.2.9.9
R2#show ip bgp labels
    Network          Next Hop     In label/Out label
    2.2.2.2/32       1.1.1.1      nolabel/20
    5.5.5.5/32       1.1.1.1      nolabel/19 6.6.6.6/32      1.1.1.1     nolabel/ 22
    20.20.20.20/32   1.1.1.1      nolabel/23
R2#traceroute vrf VPN_A 10.10.10.10

Type escape sequence to abort.
Tracing the route to 10.10.10.10
   1    10.2.3.3 [MPLS: Labels 16/22
/24 Exp 0] 4 msec 4 msec 0 msec
   2    10.1.3.1 [MPLS: Labels 22/24 Exp 0] 4 msec 4 msec 0 msec
   3    12.1.19.19 [MPLS: Labels 16001/24 Exp 0] 4 msec 4 msec 4 msec
```

```
    4    20.4.19.4 [MPLS: Labels 16/24 Exp 0] 4 msec 0 msec 4 msec
    5    30.6.10.6 [MPLS: Label 24 Exp 0] 0 msec 0 msec 4 msec
    6    30.6.10.10 0 msec * 0 msec
```

As the number of recursive lookups increases, so would the depth of the label stack. It could then be argued that this design is less efficient from a data plane point of view, because there is one extra label of overhead in the traffic forwarding. Realistically, though, this small additional overhead should be negligible in the SP network.

The same would be true in the other Autonomous System on R6, where its route to the VPN_B remote customer site recurses as R7 via R2 via XR1 via R4. This means a VPN Label is needed for R7 via R2, a Transport Label is needed for R2 via XR1, and a second transport label is needed for XR1 via R4. This can be seen as follows:

```
R6#show ip cef vrf VPN_B 7.7.7.7/32 detail
7.7.7.7 /32, epoch 0, flags rib defined all labels  recursive via 2.2.2.2 label 27
 recursive via 19.19.19.19 label 16003
 nexthop 20.4.6.4 FastEthernet0/0.46 label 18
 R6#traceroute vrf VPN_B 7.7.7.7

Type escape sequence to abort.
Tracing the route to 7.7.7.7
    1    20.4.6.4 [MPLS: Labels 18/16003/27
 Exp 0] 4 msec 0 msec 4 msec
    2    20.4.19.19 [MPLS: Labels 16003/27 Exp 0] 4 msec 0 msec 4 msec
    3    12.1.19.1 [MPLS: Labels 20/27 Exp 0] 4 msec 0 msec 4 msec
    4    10.1.3.3 [MPLS: Labels 19/27 Exp 0] 0 msec 4 msec 0 msec
    5    40.2.7.2 [MPLS: Label 27 Exp 0] 4 msec 0 msec 4 msec
    6   40.2.7.7 0 msec *    0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.18 Carrier Supporting Carrier (pending update)

- This scenario consists of two carrier networks and four customer sites as follows:
  - The “Core Carrier”:
    - Consists of R1, R7, R8, and XR1.
    - Uses OSPF + LDP for internal label distribution
    - Uses BGP AS 17819
  - The “Customer Carrier”:
    - Consists of R2, R3, R4, R5, R6, and XR2.
    - Uses IS-IS + LDP for internal label distribution
    - Uses BGP AS 100
  - Customer Site VPN_A
    - Consists of SW1 and SW2’s 30.0.0.0 networks.
    - Preconfigured for VRF Lite RIPv2 routing.
  - Customer Site VPN_B
    - Consists of SW1 and SW2’s 40.0.0.0 networks.
    - Preconfigured for VRF Lite RIPv2 routing.
- Configure IGP routing and LDP in the Core Carrier network as follows:
  - Enable OSPF Area 0 on the links between R1 & R7, R7 & R8, and R8 & XR1.
  - Enable OSPF Area 0 on the Loopback0 interfaces of these routers as passive interfaces.
  - Enable LDP on the links between between R1 & R7, R7 & R8, and R8 & XR1.
- Configure IGP routing and LDP in the Customer Carrier network as follows:
  - Use IS-IS Process-ID 1 and NET addresses in the format 49.0001.0000.0000.000X.00 where X is the router number.
  - Enable IS-IS Level 2 on the links between R2 & R5, R5 & R3, R4 & R6, and R6 & XR2.
  - Advertise the Loopback0 interfaces of these routers into IS-IS Level 2 as passive interfaces.
  - Enable LDP on the links between R2 & R5, R5 & R3, R4 & R6, and R6 &

XR2.

- Configure the VRF CSC on the Core Carrier PE routers R1 and XR1 as follows:
  - VRF Name: CSC
  - Route Distinguisher: 17819:1 o Route Target Import: 17819:1 o Route Target Export: 17819:1
  - Assign the VRF to the links connecting to R3 and R4 respectively.
- Configure the following VRFs on the Customer Carrier PE routers R2 and XR2 follows:
  - VRF VPN_A:
    - Route Distinguisher: 100:1
    - Route Target Import: 100:1
    - Route Target Export: 100:1
    - Assign this VRF on the links in the 30.0.0.0 network on R2 and XR2.
    - Enable RIPv2 routing for the VRF on R2 and XR2.
  - VRF VPN_B:
    - Route Distinguisher: 100:2
    - Route Target Import: 100:2
    - Route Target Export: 100:2
    - Assign this VRF on the links in the 40.0.0.0 network on R2 and XR2.
    - Enable RIPv2 routing for the VRF on R2 and XR2.
- Configure IPv4 Labeled Unicast BGP peerings as follows:
  - R1 and XR1 are in AS 17819.
  - R3 and R4 are in AS 100.
  - R1 should form an IPv4 Unicast EBGP peering with R3.
  - XR1 should form an IPv4 Unicast EBGP peering with R4.
  - Advertise all links that are part of the Customer Carrier network into BGP on R3 and R4, including Loopbacks.
  - Include BGP MPLS Labels advertisements between R1 & R3 and R4 & XR1.
- Configure a VPNv4 iBGP peering between the Customer Carrier PE routers R2 and XR2.
- Redistribute between VPNv4 BGP and the VRF aware IGP processes on R2 and XR2.
- Once complete the following reachability should be achieved:
  - Customer routers SW1 and SW2 should have full IP reachability to each other’s 30.x.x.x networks in VRF VPN_A.
  - Customer routers SW1 and SW2 should have full IP reachability to each other’s 40.x.x.x networks in VRF VPN_B.
  - Traceroutes between these networks should indicate that an additional level

of labels is used in the LSP through the Core Carrier network.

Configuration

```
R1:
vrf definition CSC
 rd 17819:1
 !
 address-family ipv4
 route-target export 17819:1
 route-target import 17819:1
 exit-address-family
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.13
 vrf forwarding CSC
 ip address 20.1.3.1 255.255.255.0
 mpls bgp forwarding
!
interface FastEthernet0/0.17
 ip ospf 1 area 0
 mpls ip
!
router ospf 1
 passive-interface Loopback0
!
router bgp 17819
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 17819
 neighbor 19.19.19.19 update-source Loopback0
!
address-family vpnv4
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-community extended
exit-address-family
!
address-family ipv4 vrf CSC
 neighbor 20.1.3.3 remote-as 100
 neighbor 20.1.3.3 activate
 neighbor 20.1.3.3 as-override
 neighbor 20.1.3.3 send-label
exit-address-family
```

```
!

R2:
vrf definition VPN_A
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
vrf definition VPN_B
 rd 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
!
interface FastEthernet0/0.25
 ip router isis 1
 mpls ip
!
interface FastEthernet0/0.29
 vrf forwarding VPN_A
 ip address 30.2.9.2 255.255.255.0
!
interface FastEthernet0/0.210
 vrf forwarding VPN_B
 ip address 40.2.10.2 255.255.255.0
!
router isis 1
 net 49.0001.0000.0000.0002.00
 is-type level-2-only
 passive-interface Loopback0
!
router rip
 !
 address-family ipv4 vrf VPN_B
  redistribute bgp 100 metric 1
  network 40.0.0.0
  no auto-summary
  version 2
exit-address-family
!
address-family ipv4 vrf VPN_A
```

```
 redistribute bgp 100 metric 1
 network 30.0.0.0
 no auto-summary
 version 2
exit-address-family
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 20.20.20.20 remote-as 100
 neighbor 20.20.20.20 update-source Loopback0
 !
 address-family vpnv4
  neighbor 20.20.20.20 activate
  neighbor 20.20.20.20 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VPN_A
  redistribute rip
 exit-address-family
 !
 address-family ipv4 vrf VPN_B
  redistribute rip
 exit-address-family

R3:
interface FastEthernet0/0.13
 mpls bgp forwarding
!
interface FastEthernet0/0.35
 ip router isis 1
 mpls ip
!
router isis 1
 net 49.0001.0000.0000.0003.00
 is-type level-2-only
 redistribute bgp 100 passive-
 interface Loopback0
!
router bgp 100
 network 2.2.2.2 mask 255.255.255.255
 network 3.3.3.3 mask 255.255.255.255
 network 5.5.5.5 mask 255.255.255.255
 network 20.1.3.0 mask 255.255.255.0
 network 20.2.5.0 mask 255.255.255.0
 network 20.3.5.0 mask 255.255.255.0
 neighbor 20.1.3.1 remote-as 17819
```

```
 neighbor 20.1.3.1 send-label

R4:
interface FastEthernet0/0.46
 ip router isis 1
 mpls ip
!
interface FastEthernet0/0.419
 mpls bgp forwarding
!
router isis 1
 net 49.0001.0000.0000.0004.00
 is-type level-2-only
 redistribute bgp 100
 passive-interface Loopback0
!
router bgp 100
 network 4.4.4.4 mask 255.255.255.255
 network 6.6.6.6 mask 255.255.255.255
 network 20.4.6.0 mask 255.255.255.0
 network 20.4.19.0 mask 255.255.255.0
 network 20.6.20.0 mask 255.255.255.0
 network 20.20.20.20 mask 255.255.255.255
 neighbor 20.4.19.19 remote-as 17819
 neighbor 20.4.19.19 send-label

R5:
interface FastEthernet0/0.25
 ip router isis 1
 mpls ip
!
interface FastEthernet0/0.35
 ip router isis 1
 mpls ip
!
router isis 1
 net 49.0001.0000.0000.0005.00
 is-type level-2-only
 passive-interface Loopback0
!

R6:
interface FastEthernet0/0.46
 ip router isis 1
 mpls ip
!
```

```
interface FastEthernet0/0.620
 ip router isis 1
 mpls ip
!
router isis 1
 net 49.0001.0000.0000.0006.00
 is-type level-2-only
 passive-interface Loopback0



R7:
mpls label protocol ldp
!
interface FastEthernet0/0.17
 mpls ip
!
interface FastEthernet0/0.78
 mpls ip
!
router ospf 1
 passive-interface Loopback0
 network 7.7.7.7 0.0.0.0 area 0
 network 10.0.0.0 0.255.255.255 area 0

R8:
mpls label protocol ldp
!
interface FastEthernet0/0.78
 mpls ip
!
interface FastEthernet0/0.819
 mpls ip
!
router ospf 1
 passive-interface Loopback0
 network 8.8.8.8 0.0.0.0 area 0
 network 10.0.0.0 0.255.255.255 area 0



XR1:
vrf CSC
 address-family ipv4 unicast
  import route-target 17819:1
  !
 export route-target
  17819:1
```

```
!
interface GigabitEthernet0/1/0/0.419
 vrf CSC
 ipv4 address 20.4.19.19 255.255.255.0
!
route-policy PASS
 pass
end-policy
!
router static
 vrf CSC
  address-family ipv4 unicast
   20.4.19.4/32 GigabitEthernet0/1/0/0.419
!
router ospf 1
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/1/0/0.819
!
router bgp 17819
 address-family vpnv4 unicast
 !
 neighbor 1.1.1.1
  remote-as 17819
  update-source Loopback0
  address-family vpnv4 unicast
 !
!
vrf CSC
 rd 17819:1
 address-family ipv4 unicast
  allocate-label all
 !
 neighbor 20.4.19.4
  remote-as 100
  address-family ipv4 labeled-unicast
    route-policy PASS in
    route-policy PASS out
    as-override
   !
  !
 !
!
mpls ldp
 interface GigabitEthernet0/1/0/0.819
```

```
 !
!


XR2:
vrf VPN_A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
!
vrf VPN_B
 address-family ipv4 unicast
  import route-target
   100:2
  !
  export route-target
   100:2
!
interface GigabitEthernet0/4/0/0.920
 vrf VPN_B
 ipv4 address 40.9.20.20 255.255.255.0
!
interface GigabitEthernet0/4/0/0.1020
 vrf VPN_A
 ipv4 address 30.10.20.20 255.255.255.0
!
route-policy BGP_TO_RIP
  set rip-metric 1
end-policy
!
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0020.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
!
interface GigabitEthernet0/4/0/0.620
 address-family ipv4 unicast
!
router bgp 100
 address-family vpnv4 unicast
```

```
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
 !
!
vrf VPN_A
 rd 100:1
 address-family ipv4 unicast
  redistribute rip
 !
!
vrf VPN_B
 rd 100:2
 address-family ipv4 unicast
  redistribute rip
  !
 !
!
mpls ldp
 interface GigabitEthernet0/4/0/0.620
 !
!
router rip
 vrf VPN_A
  interface GigabitEthernet0/4/0/0.1020
  !
  redistribute bgp 100 route-policy BGP_TO_RIP
 !
 vrf VPN_B
  interface GigabitEthernet0/4/0/0.920
  !
  redistribute bgp 100 route-policy BGP_TO_RIP
 !
!
End
```

Verification

Carrier Supporting Carrier (CsC), or what is sometimes referred to as Hierarchical MPLS VPNs, is when a typically smaller Service Provider uses another larger Service Provider's MPLS network for transport between the smaller SP's sites, and ultimately between the sites of the smaller SP's customers. In this type of design the larger Service Provider is considered to be the "Core Carrier", while the smaller Service Provider is considered the "Customer Carrier".

This design is common in cases where a Service Provider has customers in geographically diverse areas, for example in London and Los Angeles, but does not own long haul transit links between these locations. With CsC the Customer Carrier can still transparently offer services to its customers in London and Los Angeles without them knowing that they are actually transiting through a third party to provide services.

From a configuration point of view a CsC design is similar to an Inter-AS MPLS L3VPN, with the exception that the Core Carrier to Customer Carrier link is MPLS enabled, as is treated like a normal L3VPN customer site from the Core Carrier's point of view. These links are then referred to as the CsC-PE to CsC-CE links, with the Core Carrier being the PE side and the Customer Carrier being the CE side.

One of the key points to keep in mind about this design is that since the Core Carrier does not have knowledge of the final customer prefixes, all traffic must follow an end-to-end LSP as it moves from the Customer Carrier through the Core Carrier network. In order to achieve this then the next-hop values that are used for the Customer Carrier's VPNv4 BGP peering sessions must have corresponding LSPs inside the Core Carrier.

In this specific configuration example the final customer networks are represented by the VPN_A and VPN_B networks on SW1 and SW2. Note that this portion of the configuration is unrelated to the rest of the design, as the VRF Lite/ Multi VRF CE configuration on SW1 and SW2 is simply used to simulate more routers than are physically used in the topology.

Like our other previous examples the final verification is to test end-to-end reachability between these sites, as seen below:

```
SW1#show ip route vrf VPN_A

Routing Table: VPN_A
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
```

```
    30.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R      30.10.20.0/24 [120/1] via 30.2.9.2, 00:00:25, Vlan29
R      30.10.10.10/32 [120/1] via 30.2.9.2, 00:00:25, Vlan29
C      30.2.9.0/24 is directly connected, Vlan29
C      30.9.9.9/32 is directly connected, Loopback30
SW1#ping vrf VPN_A 30.10.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
SW1#show ip route vrf VPN_B

Routing Table: VPN_B
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

    40.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R      40.2.10.0/24 [120/1] via 40.9.20.20, 00:00:24, Vlan920
C      40.9.9.9/32 is directly connected, Loopback40
R      40.10.10.10/32 [120/1] via 40.9.20.20, 00:00:24, Vlan920
C      40.9.20.0/24 is directly connected, Vlan920
SW1#ping vrf VPN_B 40.10.10.10


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/9 ms
```

To see how this design is different from previous examples, we need to follow the individual control plane and data plane paths separately of a final end prefix, as many common problems in this design will appear in the data plane that are not completely evident in the control plane. For example you may see that the final customer is learning and installing the prefixes correctly, but they don’t actually have transport between the sites. To verify the individual steps, we first start at the final PE to CE link between R2 in the Customer Carrier network and its final customer

SW2.

```
R2#show ip route vrf VPN_B 40.10.10.10

 Routing Table: VPN_B
 Routing entry for 40.10.10.10/32 Known via "rip"
, distance 120, metric 1
     Redistributing via rip, bgp 100
     Advertised by bgp 100
     Last update from 40.2.10.10 on FastEthernet0/0.210, 00:00:02 ago
     Routing Descriptor Blocks:
     * 40.2.10.10, from 40.2.10.10, 00:00:02 ago, via FastEthernet0/0.210
         Route metric is 1, traffic share count is 1
 R2#show bgp vpnv4 unicast vrf VPN_B 40.10.10.10
 BGP routing table entry for 100:2:40.10.10.10/32
, version 5
 Paths: (1 available, best #1, table VPN_B)
    Advertised to update-groups:
      1
    Local    40.2.10.10 from 0.0.0.0 ( 2.2.2.2
 )
      Origin incomplete, metric 1, localpref 100, weight 32768, valid, sourced,
 best       Extended Community: RT:100:2
  mpls labels in/out 19/nolabel
```

R2 learns the prefix 40.10.10.10/32 in VRF VPN_B via RIP, and redistributes this into VPNv4 BGP. Like our previous designs we can see that this first step creates two important building blocks of the L3VPN network, the MPLS VPN Label and the VPNv4 BGP next-hop value. R2 then advertises this route to its VPNv4 BGP peer XR2, who is servicing the customer sites on the remote end of the network.

```
R2#show bgp vpnv4 unicast all neighbors 20.20.20.20 advertised-routes
 BGP table version is 37, local router ID is 2.2.2.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external
 Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop     Metric LocPrf  Weight Path
 Route Distinguisher: 100:1 (default for vrf VPN_A)
 *> 30.2.9.0/24      0.0.0.0          0           32768 ?
 *> 30.9.9.9/32      30.2.9.9         1           32768 ?
 Route Distinguisher: 100:2 (default for vrf VPN_B)
 *> 40.2.10.0/24     0.0.0.0          0           32768 ?
 *> 40.10.10.10/32 40.2.10.10        1           32768 ?
```

```
Total number of prefixes 4
RP/0/3/CPU0:XR2#show bgp vpnv4 unicast vrf VPN_B 40.10.10.10/32
Wed Mar 21 22:37:11.713 UTC BGP routing table entry for 40.10.10.10/32, Route Distinguisher: 100:2
Versions:
    Process bRIB/RIB    SendTblVer
    Speaker       45            45
Last Modified: Mar 21 21:40:42.099 for 00:56:29
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Local 2.2.2.2
 (metric 20) from 2.2.2.2 (2.2.2.2) Received Label 19
     Origin incomplete, metric 1, localpref 100, valid, internal, best, import-
candidate, imported     Extended community: RT:100:2
```

XR2 receives the VPNv4 route from R2 with a next-hop of 2.2.2.2, a VPN Label of 19, and a Route Target of 100:2. Assuming that XR2 properly imports this route into the VRF and redistributes it into the PE to CE routing process, the next point we need to verify is whether or not XR2 has a Label Switch Path towards the next-hop value 2.2.2.2. To form this LSP we must first know about the route in the global routing table.

```
RP/0/3/CPU0:XR2#show route 2.2.2.2/32
Wed Mar 21 22:39:47.944 UTC

Routing entry for 2.2.2.2/32 Known via "isis 1",
 distance 115, metric 20, type level-2
    Installed Mar 21 21:40:41.915 for 00:59:06
    Routing Descriptor Blocks
        20.6.20.6, from 4.4.4.4, via GigabitEthernet0/4/0/0.620
            Route metric is 20
    No advertising protos.
```

XR2 learns about 2.2.2.2/32 via IS-IS. Since this is an IGP learned prefix, it means that the MPLS Label must be coming from either LDP or RSVP-TE in order to be used. The MPLS FIB will tell us if the label exists, as follows:

```
RP/0/3/CPU0:XR2#show mpls forwarding prefix 2.2.2.2/32
Wed Mar 21 22:40:58.814 UTC
Local   Outgoing    Prefix              Outgoing        Next Hop       Bytes
Label   Label       or ID               Interface                      Switched
------ ----------- ------------------ -----------     --------------- -----------
```

```
16009 18            2.2.2.2/32          Gi0/4/0/0.620 20.6.20.6
       298656
```

XR2 does in fact have an LSP for this prefix, specifically using the label value 18 via the next- hop 20.6.20.6 (R6). The next-hop router R6 likewise learns the route via IS-IS, and has a label value for it derived from LDP.

```
R6#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32 Known via "isis",
 distance 115, metric 10, type level-2
    Redistributing via isis 1
    Last update from 20.4.6.4 on FastEthernet0/0.46, 01:01:59 ago
    Routing Descriptor Blocks:    * 20.4.6.4
, from 4.4.4.4, 01:01:59 ago, via FastEthernet0/0.46
        Route metric is 10, traffic share count is 1
R6#show mpls forwarding-table 2.2.2.2
Local   Outgoing    Prefix          Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id    Switched    interface 18 19
         2.2.2.2/32      377165      Fa0/0.46 20.4.6.4
```

Beyond this we go to R4, who is considered to be the Customer Carrier CE, or the CsC CE router. Here R4 is learning the prefix 2.2.2.2/32 via the EBGP neighbor XR1, who is the CSC PE. R4 and XR1 are regular IPv4 Unicast BGP peers, but are also exchanging MPLS labels. This can be seen from the global routing table output below, as R4 has a BGP derived label for the prefix.

```
R4#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32 Known via "bgp 100",
 distance 20, metric 0
    Tag 17819, type external
    Redistributing via isis 1
    Advertised by isis 1 metric-type internal level-2
    Last update from 20.4.19.19 01:02:56 ago
    Routing Descriptor Blocks:
    * 20.4.19.19, from 20.4.19.19, 01:02:56 ago
        Route metric is 0, traffic share count is 1
        AS Hops 2
        Route tag 17819 MPLS label: 16011
R4#show ip bgp labels
        Network          Next Hop    In label/Out label 2.2.2.2/32       20.4.19.19
 nolabel/16011
        3.3.3.3/32       20.4.19.19  nolabel/16012
        4.4.4.4/32       0.0.0.0     imp-null/nolabel
```

```
5.5.5.5/32      20.4.19.19  nolabel/16013
6.6.6.6/32      20.4.6.6    16/nolabel
20.1.3.0/24     20.4.19.19  nolabel/16014
20.2.5.0/24     20.4.19.19  nolabel/16015
20.3.5.0/24     20.4.19.19  nolabel/16016
20.4.6.0/24     0.0.0.0     imp-null/nolabel
20.4.19.0/24    0.0.0.0     imp-null/nolabel
20.6.20.0/24    20.4.6.6    18/nolabel
20.20.20.20/32  20.4.6.6    17/nolabel
```

R4 is then taking the BGP learned route and label and redistributing it into IS-IS. This is the reason that the rest of the Customer Carrier network (i.e. R6 and XR2) knows about the prefix via IS-IS and LDP. Another option here would be to run BGP + Label everywhere in the Customer Carrier network, however this design is typically more difficult to maintain from an administrative point of view.

From the Core Carrier Provider Edge Router (XR1's) point of view, this route is being learned as a VPNv4 iBGP from the other CSC PE (R1).

```
RP/0/0/CPU0:XR1#show route vrf CSC 2.2.2.2/32
Thu Mar 22 14:12:01.436 UTC

Routing entry for 2.2.2.2/32 Known via "bgp 17819",
 distance 200, metric 20    Tag 100, type internal
    Installed Mar 21 23:10:07.440 for 15:01:54
    Routing Descriptor Blocks  1.1.1.1
, from 1.1.1.1 Nexthop in Vrf: "default"
, Table: "default", IPv4 Unicast, Table Id:
0xe0000000
         Route metric is 20
 No advertising protos.
```

Note that since this is a new VPNv4 route that is being originated, a new VPN Label and next- hop value are being set. This is why this design is sometimes called Hierarchical MPLS VPNs, because it's basically one L3VPN inside of another L3VPN. The impact of this will be evident when we verify the actual traffic flow in the data plane.

From the CSC PE's point of view as seen below, the VPNv4 route 2.2.2.2/32 is learned via the remote PE 1.1.1.1. This means that XR1 needs a LSP for 1.1.1.1, which is solved by running OSPF + LDP in the Core Carrier network.

```
RP/0/0/CPU0:XR1#sh bgp vpnv4 unicast vrf CSC 2.2.2.2
Wed Mar 21 22:56:48.250 UTC BGP routing table entry for 2.2.2.2/32, Route Distinguisher: 17819:1
```

```
Versions:
    Process bRIB/RIB    SendTblVer
    Speaker 68  68 Local Label: 16011
Last Modified: Mar 21 21:40:32.780 for 01:16:15
Paths: (1 available, best #1)
   Not advertised to any peer
   Path #1: Received by speaker 0
   100 1.1.1.1
 (metric 4) from 1.1.1.1 (1.1.1.1) Received Label 27
     Origin IGP, metric 20, localpref 100, valid, internal, best, import-
candidate, imported     Extended community: RT:17819:1
RP/0/0/CPU0:XR1#traceroute 1.1.1.1 source 19.19.19.19
Wed Mar 21 23:00:05.208 UTC
Type escape sequence to abort.
Tracing the route to 1.1.1.1
 1  10.8.19.8 [ MPLS: Label 18 Exp 0
] 6 msec 4 msec  2 msec 2  10.7.8.7 [ MPLS: Label 18 Exp 0
] 3 msec  4 msec  3 msec
 3  10.1.7.1 4 msec *   3 msec
```

At the next CSC PE router R1, this prefix is being learned an IPv4 Unicast Labeled EBGP route from the CSC CE router R3.

```
R1#show bgp vpnv4 unicast vrf CSC 2.2.2.2/32
BGP routing table entry for 17819:1:2.2.2.2/32
, version 86
Paths: (1 available, best #1, table CSC)
   Advertised to update-groups:
     1
100 20.1.3.3
 from 20.1.3.3 (3.3.3.3)
     Origin IGP, metric 20, localpref 100, valid, external, best      Extended Community: RT:17819:1
 mpls labels in/out 27/18
```

The MPLS Label value allocated by BGP from R3 can be verified from the above output, or as follows:

```
R1#show bgp vpnv4 unicast all labels
    Network          Next Hop        In label/Out label
Route Distinguisher: 17819:1 (CSC) 2.2.2.2/32        20.1.3.3        27/18
    3.3.3.3/32      20.1.3.3        31/imp-null
    4.4.4.4/32      19.19.19.19     51/16005
    5.5.5.5/32      20.1.3.3        29/16
    6.6.6.6/32      19.19.19.19     54/16006
```

```
    20.1.3.0/24     20.1.3.3        28/imp-null
    20.2.5.0/24     20.1.3.3        30/17
    20.3.5.0/24     20.1.3.3        32/imp-null
    20.4.6.0/24     19.19.19.19     52/16007
    20.4.19.0/24    19.19.19.19     53/16008
    20.6.20.0/24    19.19.19.19     55/16009
    20.20.20.20/32  19.19.19.19     56/16010
R3#show ip bgp labels
    Network         Next Hop    In label/Out label 2.2.2.2/32       20.3.5.5   18/nolabel

    3.3.3.3/32      0.0.0.0     imp-null/nolabel
    4.4.4.4/32      20.1.3.1    nolabel/51
    5.5.5.5/32      20.3.5.5    16/nolabel
    6.6.6.6/32      20.1.3.1    nolabel/54
    20.1.3.0/24     0.0.0.0     imp-null/nolabel
    20.2.5.0/24     20.3.5.5    17/nolabel
    20.3.5.0/24     0.0.0.0     imp-null/nolabel
    20.4.6.0/24     20.1.3.1    nolabel/52
    20.4.19.0/24    20.1.3.1    nolabel/53
    20.6.20.0/24    20.1.3.1    nolabel/55
    20.20.20.20/32  20.1.3.1    nolabel/56
```

From the CSC CE router R3's perspective, this route is being learned via IGP and has an LDP bound label for outbound traffic. However the inbound label is allocated via IPv4 Labeled Unicast BGP. R3 is the one who is tying these two values together in the MPLS LFIB.

```
R3#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32 Known via "isis"
, distance 115, metric 20, type level-2
    Redistributing via isis 1
    Advertised by bgp 100
    Last update from 20.3.5.5 on FastEthernet0/0.35, 17:04:54 ago
    Routing Descriptor Blocks:
    * 20.3.5.5, from 2.2.2.2, 17:04:54 ago, via FastEthernet0/0.35
        Route metric is 20, traffic share count is 1
R3#show mpls forwarding-table 2.2.2.2
Local   Outgoing    Prefix          Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id    Switched    interface 18
      17          2.2.2.2/32      395524      Fa0/0.35    20.3.5.5
```

The next router, R5, is the Penultimate Hop, and will remove the topmost label for traffic going towards the 2.2.2.2 Loopback of R2.

```
R5#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32 Known via "isis"
, distance 115, metric 10, type level-2
    Redistributing via isis 1
    Last update from 20.2.5.2 on FastEthernet0/0.25, 17:11:38 ago
    Routing Descriptor Blocks:
    * 20.2.5.2, from 2.2.2.2, 17:11:38 ago, via FastEthernet0/0.25
        Route metric is 10, traffic share count is 1
R5#show mpls forwarding-table 2.2.2.2
Local   Outgoing    Prefix          Bytes Label Outgoing    Next Hop
Label   Label       or Tunnel Id    Switched    interface 17        Pop Label
   2.2.2.2/32      518404      Fa0/0.25    20.2.5.2
```

Once the advertisements are completed end-to-end, R2 and XR2 should have an LSP built between their Loopback0 networks. Additionally the output of the traceroute between them should indicate that an additional level of labels is used when traffic is transiting the Core Carrier network, as seen below.

```
RP/0/3/CPU0:XR2#traceroute 2.2.2.2 source 20.20.20.20
Thu Mar 22 14:33:08.817 UTC

Type escape sequence to abort.
Tracing the route to 2.2.2.2

 1  20.6.20.6 [MPLS: Label 18 Exp 0] 6 msec 5 msec  4 msec
 2  20.4.6.4 [MPLS: Label 19 Exp 0] 4 msec  4 msec  4 msec
 3  20.4.19.19 [MPLS: Label 16011 Exp 0] 6 msec 9 msec  6 msec  4  10.8.19.8 [MPLS: Labels 18/27
Exp 0] 4 msec 6 msec  4 msec  5  10.7.8.7 [MPLS: Labels 18/27
Exp 0] 4 msec  6 msec  5 msec
 6  20.1.3.1 [MPLS: Label 27 Exp 0] 4 msec  6 msec  4 msec
 7  20.1.3.3 [MPLS: Label 18 Exp 0] 4 msec  4 msec  4 msec
 8  20.3.5.5 [MPLS: Label 17 Exp 0] 4 msec  5 msec  4 msec
 9  20.2.5.2 4 msec *   5 msec
```

These extra transport labels of 18 seen above are what hide the final customer traffic from the Core Carrier network. Without them the PHP process would happen one hop too soon, and a P router in the core of the topology would be exposed to a VPN Label that it does not know about. The fully functional network should appear in a traceroute similar to the following:

```
RP/0/3/CPU0:XR2#traceroute vrf VPN_B 40.10.10.10

Thu Mar 22 14:35:37.037 UTC

Type escape sequence to abort.
Tracing the route to 40.10.10.10

 1  20.6.20.6 [MPLS: Labels 18/19 Exp 0] 8 msec 7 msec  4 msec
 2  20.4.6.4 [MPLS: Labels 19/19 Exp 0] 5 msec  6 msec  4 msec
 3  20.4.19.19 [MPLS: Labels 16011/19 Exp 0] 7 msec 8 msec  5 msec 4  10.8.19.8 [MPLS: Labels 18/27/19
Exp 0] 5 msec  5 msec  4 msec 5  10.7.8.7 [MPLS: Labels 18/27/19
Exp 0] 6 msec   5 msec  6 msec
 6  10.1.7.1 [MPLS: Labels 27/19 Exp 0] 5 msec  5 msec  4 msec
 7  20.1.3.3 [MPLS: Labels 18/19 Exp 0] 5 msec  5 msec  4 msec
 8  20.3.5.5 [MPLS: Labels 17/19 Exp 0] 4 msec  6 msec  4 msec
 9  40.2.10.2 [MPLS: Label 19 Exp 0] 4 msec 5 msec  4 msec
 10 40.2.10.10 4 msec   *   4 msec
```

If MPLS TE were used anywhere in the network you would see more than three labels in the stack in the Core Carrier.

Now let's look at this topology with a common break in the control plane. Below the CSC CE R3 removes its MPLS Labeling capability under the IPv4 Unicast BGP process.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.R3(config)#router bgp 100
R3(config-router)#no neighbor 20.1.3.1 send-label

%BGP-5-ADJCHANGE: neighbor 20.1.3.1 Down Capability changed
%BGP_SESSION-5-ADJCHANGE: neighbor 20.1.3.1 IPv4 Unicast topology base removed from
session Capability changed
%BGP_LMM-6-MPLS_INIT: MPLS has been disabled for the BGP address-family IPv4 R3(config-router)#end
%BGP-5-ADJCHANGE: neighbor 20.1.3.1 Up
```

Once removed, R3 still learns IPv4 Unicast BGP routes from the Core Carrier, however it does not learn label values for them. The most important ones here are 2.2.2.2 and 20.20.20.20, which need to be via an LSP that is reachable end to end within the Customer Carrier.

```
R3#show ip bgp
BGP table version is 79, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop    Metric  LocPrf  Weight  Path
*>  2.2.2.2/32        20.3.5.5    20               32768
  i
*>  3.3.3.3/32       0.0.0.0      0              32768  i
*>  4.4.4.4/32       20.1.3.1                        0  17819   17819   i
*>  5.5.5.5/32       20.3.5.5    10              32768  i
*>  6.6.6.6/32       20.1.3.1                        0  17819   17819   i
*>  20.1.3.0/24      0.0.0.0      0              32768  i
*>  20.2.5.0/24      20.3.5.5    20             32768   i
*>  20.3.5.0/24      0.0.0.0      0             32768   i
*>  20.4.6.0/24      20.1.3.1                       0   17819   17819   i
*>  20.4.19.0/24     20.1.3.1                       0   17819   17819   i
*>  20.6.20.0/24     20.1.3.1                       0   17819   17819   i
*>  20.20.20.20/32  20.1.3.1                        0   17819  17819  i
R3#show ip bgp labels
Network          Next Hop     In label/Out label2.2.2.2/32      20.3.5.5   nolabel/nolabel
3.3.3.3/32       0.0.0.0      nolabel/nolabel
4.4.4.4/32       20.1.3.1     nolabel/nolabel
5.5.5.5/32       20.3.5.5     nolabel/nolabel
6.6.6.6/32       20.1.3.1     nolabel/nolabel
20.1.3.0/24      0.0.0.0      nolabel/nolabel
20.2.5.0/24      20.3.5.5     nolabel/nolabel
20.3.5.0/24      0.0.0.0      nolabel/nolabel
20.4.6.0/24      20.1.3.1     nolabel/nolabel
20.4.19.0/24     20.1.3.1     nolabel/nolabel
20.6.20.0/24     20.1.3.1     nolabel/nolabel20.20.20.20/32  20.1.3.1   nolabel/nolabel
```

From the final customer's point of view, this does not affect their control plane:

```
SW1#show ip route vrf VPN_B

Routing Table: VPN_B
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

    40.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
```

```
R       40.2.10.0/24 [120/1] via 40.9.20.20, 00:00:04, Vlan920
C       40.9.9.9/32 is directly connected, Loopback40
R       40.10.10.10/32 [120/1] via 40.9.20.20, 00:00:04, Vlan920

C       40.9.20.0/24 is directly connected, Vlan920
```

However it does affect their data plane:

```
SW1#ping vrf VPN_B 40.10.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.10.10.10, timeout is 2 seconds:
..... Success rate is 0 percent
 (0/5)
```

Tracking this problem becomes very difficult because the MPLS Labels used need to be verified on a hop by hop basis. Furthermore it becomes more difficult because when the LSP is broken, a traceroute does not return any useful output:

```
RP/0/3/CPU0:XR2#traceroute vrf VPN_B 40.10.10.10

Wed Mar 21 23:13:54.107 UTC

Type escape sequence to abort.
Tracing the route to 40.10.10.10

 1  *   *   *
 2  *   *   *
 3  *   *   *
 4  *   *   *
<snip>
```

What you would need to do is look at the specific label value that should be being used, and correlate this with the **debug mpls packet** output.

```
R2#show ip cef vrf VPN_B 40.9.9.9
40.9.9.9/32    nexthop 20.2.5.5 FastEthernet0/0.25 label 20 16002
```

R2 above says that the transport label should be 20, and the VPN label should be 16002 for the prefix 40.9.9.9 inside VRF VPN_B.

```
R5#show mpls forwarding-table

Local       Outgoing     Prefix              Bytes Label    Outgoing     Next Hop
Label       Label        or Tunnel Id        Switched       interface
16          Pop Label   3.3.3.3/32            0              Fa0/0.35    20.3.5.3
17          Pop Label   2.2.2.2/32            390045         Fa0/0.25    20.2.5.2
18          19          4.4.4.4/32            0              Fa0/0.35    20.3.5.3
19          20          6.6.6.6/32            0              Fa0/0.35    20.3.5.3
20          24          20.20.20.20/32        1386           Fa0/0.35    20.3.5.3

21          Pop Label   20.1.3.0/24           0              Fa0/0.35    20.3.5.3
22          21          20.4.6.0/24           0              Fa0/0.35    20.3.5.3
23          22          20.4.19.0/24          0              Fa0/0.35    20.3.5.3
24          23          20.6.20.0/24          0              Fa0/0.35    20.3.5.3
```

R5 says that incoming transport label 20 means that traffic is going towards 20.20.20.20/32, and should forward to R3 with label 24.

```
R3#show mpls forwarding-table
Local       Outgoing        Prefix             Bytes Label    Outgoing     Next Hop
Label       Label           or Tunnel Id       Switched       interface
16          Pop Label       5.5.5.5/32         0              Fa0/0.35    20.3.5.5
17          Pop Label       20.2.5.0/24        0              Fa0/0.35    20.3.5.5
18          17              2.2.2.2/32         395524         Fa0/0.35    20.3.5.5
19          No Label        4.4.4.4/32         0              Fa0/0.13    20.1.3.1
20          No Label        6.6.6.6/32         0              Fa0/0.13    20.1.3.1
21          No Label        20.4.6.0/24        0              Fa0/0.13    20.1.3.1
22          No Label        20.4.19.0/24       0              Fa0/0.13    20.1.3.1
23          No Label        20.6.20.0/24       0              Fa0/0.13    20.1.3.1
24          No Label        20.20.20.20/32     1369           Fa0/0.13    20.1.3.1
```

R3 says that when label 24 comes in the *entire stack* should be deposed, and the traffic should be sent to R1. Since R1 does not know about the final destinations, this is where the traffic is getting blackholed. **debug mpls packet** would indicate this because R3 is receiving a label stack from R5 but does not continue to forward it on.

```
R3#debug mpls packet
Packet debugging is on
R2#ping vrf VPN_B 40.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.9.9.9, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)

R3#MPLS turbo: Fa0/0.35: rx:
 Len 126 Stack {24 0 254} {16002 0 255} - ipv4 data MPLS turbo: Fa0/0.35: rx:
 Len 126 Stack {24 0 254} {16002 0 255} - ipv4 data MPLS turbo: Fa0/0.35: rx:
 Len 126 Stack {24 0 254} {16002 0 255} - ipv4 data MPLS turbo: Fa0/0.35: rx:
 Len 126 Stack {24 0 254} {16002 0 255} - ipv4 data MPLS turbo: Fa0/0.35: rx:
 Len 126 Stack {24 0 254} {16002 0 255} - ipv4 data
```

With correct labeling on the CSC CE to CSC PE link the debug output would look similar to the following:

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.R3(config)#router bgp 100
R3(config-router)#address-family ipv4 unicast
R3(config-router-af)#neighbor 20.1.3.1 send-label
R3(config-router-af)#end
R3#
%BGP-5-ADJCHANGE: neighbor 20.1.3.1 Down Capability changed
%BGP_SESSION-5-ADJCHANGE: neighbor 20.1.3.1 IPv4 Unicast topology base removed from
session Capability changed
%BGP-5-ADJCHANGE: neighbor 20.1.3.1 Up
%SYS-5-CONFIG_I: Configured from console by console
R3#debug mpls packet
Packet debugging is on
R2#ping vrf VPN_B 40.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R3#MPLS turbo: Fa0/0.35: rx: Len 126 Stack {24 0 254} {16002 0 255}
 - ipv4 data MPLS turbo: Fa0/0.13: tx: Len 126 Stack {56 0 253} {16002 0 255}
 - ipv4 data MPLS turbo: Fa0/0.13: rx: Len 126 Stack {18 0 248} {18 0 254}
 - ipv4 data MPLS turbo: Fa0/0.35: tx: Len 126 Stack {17 0 247} {18 0 254}
 - ipv4 data
<snip>
```

In the Core Carrier we would see this as a three label stack, which consists of the final customer's VPN label, the Customer Carrier's transport label for their VPNv4 session, and the Core Carrier's transport label for its own VPNv4 session. Notice that the final customer's VPN labels of 16002 and 18 remain in the stack throughout the entire transit path.

```
R7#debug mpls packet
MPLS packet debugging is on
R2#ping vrf VPN_B 40.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

R7# MPLS: Fa0/0.17: recvd: CoS=0, TTL=252, Label(s)=19/16010/16002
MPLS: Fa0/0.78: xmit: CoS=0, TTL=251, Label(s)=19/16010/16002
MPLS: Fa0/0.78: recvd: CoS=0, TTL=250, Label(s)=18/45/18
MPLS: Fa0/0.17: xmit: CoS=0, TTL=249, Label(s)=45/18

<snip>
```

Another important part about this design, like in the previous Inter-AS MPLS L3VPN scenarios, is that IOS XR cannot label switch traffic towards a non /32 next-hop value. This means that XR1 must have the following route statically configured in the CSC VRF table:

```
RP/0/0/CPU0:XR1#sh run router static
Thu Mar 22 14:46:47.473 UTC
router static vrf CSC
  address-family ipv4 unicast 20.4.19.4/32 GigabitEthernet0/1/0/0.419
  !
 !
!
RP/0/0/CPU0:XR1#show route vrf CSC static

Thu Mar 22 14:46:49.244 UTC

S   20.4.19.4/32 is directly connected, 17:04:32, GigabitEthernet0/1/0/0.419
```

If this route is removed, traffic in the data plane fails.

```
R2#ping vrf VPN_B 40.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.9.9.9, timeout is 2 seconds:
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 8/11/16 ms
```

```
RP/0/0/CPU0:XR1#config t
Thu Mar 22 14:47:49.062 UTCRP/0/0/CPU0:XR1(config)#no router static
 RP/0/0/CPU0:XR1(config)#commit
RP/0/0/CPU0:Mar 22 14:47:54.437 : config[65752]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin'. Use 'show configuration commit changes
1000000099' to view the changes.
RP/0/0/CPU0:XR1(config)#
R2#ping vrf VPN_B 40.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.9.9.9, timeout is 2 seconds:
..... Success rate is 0 percent
 (0/5)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.19 6PE (pending update)

- The network is preconfigured as follows:
  - The Service Provider AS 100 consists of R2, R3, R4, R5, R6 and XR1.
  - AS 100 runs OSPF + LDP on all transit links, and is IPv4 only enabled.
  - Customer routers R1 and XR2 run both IPv4 and IPv6 to their PE routers R2 and XR1.
- Configure BGP on R1, R2, XR1, and XR2 as follows:
  - R1 should be in AS 1.
  - R2 and XR1 should be in AS 100.
  - XR2 should be in AS 20.
  - R1 and R2 should peer EBGP using their connected link for both IPv4 and IPv6 Unicast.
  - R2 and XR1 should peer iBGP using the Loopback0 interfaces, for both IPv4 and IPv6 Labeled Unicast, and use **next-hop-self**.
  - XR1 and XR2 should peer EBGP using their connected link for both IPv4 and IPv6 Unicast.
  - Advertise the prefix 1.1.1.1/32 and 2000::1:1:1:1/128 into BGP on R1.
  - Advertise the prefix 20.20.20.20/32 and 2000::20:20:20:20/128 into BGP on XR2.
- When complete, R1 and XR2 should be able to reach each other’s IPv4 and IPv6 Loopback0 interfaces when sourcing traffic from their own Loopback0 interface.

Configuration

```
R1:
ipv6 unicast-routing
ipv6 cef
!
router bgp 1
 neighbor 10.1.2.2 remote-as 100
 neighbor 2001:10:1:2::2 remote-as 100
 !
```

```
 address-family ipv4
  network 1.1.1.1 mask 255.255.255.255
  neighbor 10.1.2.2 activate
  no neighbor 2001:10:1:2::2 activate
exit-address-family
!
address-family ipv6
 network 2001::1:1:1:1/128
 neighbor 2001:10:1:2::2 activate
exit-address-family

R2:
ipv6 unicast-routing
ipv6 cef
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 10.1.2.1 remote-as 1
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 neighbor 2001:10:1:2::1 remote-as 1
 !
 address-family ipv4
 neighbor 10.1.2.1 activate
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 next-hop-self
exit-address-family
!
address-family ipv6
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 send-label
 neighbor 2001:10:1:2::1 activate exit-address-
family

XR1:
route-policy PASS
 pass
end-policy
!
router bgp 100
 address-family ipv4 unicast
 !
address-family ipv6 unicast
 allocate-label all
!
neighbor 2.2.2.2
```

```
 remote-as 100
 update-source Loopback0
 address-family ipv4 unicast
  next-hop-self
 !
 address-family ipv6 labeled-unicast
 !
!
neighbor 10.19.20.20
 remote-as 20
 address-family ipv4 unicast
  route-policy PASS in
  route-policy PASS out
 !
!
neighbor 2001:10:19:20::20
 remote-as 20
 address-family ipv6 unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
!


XR2:
route-policy PASS
 pass
end-policy
!
router bgp 20
 address-family ipv4 unicast
  network 20.20.20.20/32
 !
 address-family ipv6 unicast
  network 2001::20:20:20:20/128
 !
 neighbor 10.19.20.19
  remote-as 100
  address-family ipv4 unicast
  route-policy PASS in
  route-policy PASS out
 !
!
neighbor 2001:10:19:20::19
 remote-as 100
```

```
  address-family ipv6 unicast
    route-policy PASS in
    route-policy PASS out
   !
  !
 !
```

Verification

This example is similar to the “Basic MPLS Tunnels” lab in the terms that the customer’s traffic is tunneled inside MPLS over the Service Provider network, but the provider is not running L3VPN with the customer. If the provider was running L3VPN in this case, this design would be considered 6VPE instead of 6PE, where 6VPE uses VPNv6 BGP extensions, while 6PE simply uses IPv6 Unicast BGP extensions. The basic logic of this 6PE design is as follows.

The Service Provider network is IPv4 IGP and LDP enabled to start. This means that the PE routers can form an MPLS LSP between their Loopback interfaces. The link between the Customer Edge routers and Provider Edge routers is dual-stack enabled, both for IPv4 and for IPv6. Because the PE routers already have label values allocated for each other’s IPv4 Loopbacks, there’s no problem with tunneling the Customer’s IPv4 traffic over the provider network. We can see this below as R1 and XR2 have reachability to each other’s IPv4 Loopbacks, even though the core of the network does not have these routes.

```
R1#traceroute 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Tracing the route to 20.20.20.20

    1   10.1.2.2 0 msec 4 msec 0 msec
    2   20.2.4.4 [MPLS: Label 23 Exp 0] 0 msec 4 msec 0 msec
    3   *   *   *
    4 20.6.19.19 4 msec 0 msec 4 msec
    5 10.19.20.20 4 msec *  4 msec
R4#show ip route 1.1.1.1
% Network not in table
R4#show ip route 20.20.20.20

% Subnet not in table
```

The reason this IPv4 over MPLS tunnel works is that the core of the network is simply label switching packets between the Loopbacks of R2 and XR1, the PE routers. However, for this to work for IPv6 by the same logic, the core of the network would need IPv6 IGP routes to the IPv6 Loopbacks of the PE routers, and have LDPv6 labels for the IPv6 routes. In essence, this would require the Service Provider to be dual-stack enabled everywhere to provide IPv6 transit to their customers. Instead, 6PE offers an alternative “hack” on the MPLS process by allowing the next-hop value of an IPv6 BGP learned prefix to point toward an IPv4 next-hop for which the core of the MPLS network already has a label.

The logic of this is similar to the MPLS L3VPN Inter-AS Option C, where the EBGP neighbors are exchanging IPv4 Unicast BGP routes along with MPLS Labels. However, in this case the routers are exchanging *IPv6* Unicast BGP routes along with MPLS Labels, and have the next-hop value pointing to an IPv4 address.

The step-by-step verification of this process is as follows. First, the customer router R1 forms an IPv6 EBGP peering session with the provider and advertises its IPv6 prefixes. This portion of the network could likewise be IPv6 IGP, but then BGP to IGP redistribution would be required.

```
R1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 3, main routing table version 3
2 network entries using 304 bytes of memory
2 path entries using 152 bytes of memory
2/2 BGP path/bestpath attribute entries using 248 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 728 total bytes of memory
BGP activity 4/0 prefixes, 5/1 paths, scan interval 60 secs

Neighbor            V   AS  MsgRcvd MsgSent TblVer  InQ OutQ  Up/Down
State/PfxRcd
2001:10:1:2::2      4   100      48      49      3    0    0  00:40:26      1

R1#show bgp ipv6 unicast neighbor 2001:10:1:2::2 advertised-routes


BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop    Metric LocPrf   Weight Path
*> 2001::1:1:1:1/128
                        ::              0           32768  i
```

```
Total number of prefixes 1
```

Here we see that R1 is advertising the prefix 2001::1:1:1:1/128 (its Loopback) to R2. R2 learns this in the regular global IPv6 Unicast routing table, and installs it with the link-local next-hop of the connected neighbor.

```
R2#show ipv6 route 2001::1:1:1:1/128
Routing entry for 2001::1:1:1:1/128
    Known via "bgp 100", distance 20, metric 0, type external
    Route count is 1/1, share count 0
    Routing paths: FE80::205:5FFF:FEAD:3800, FastEthernet1/0

        MPLS label: nolabel
        Last updated 00:41:31 ago
```

R2 has two IPv6 BGP peers, the CE router R1 and the PE router XR1. The transport for the BGP session between R1 and R2 uses IPv6, but the transport for the session between R2 and XR1 uses IPv4.

```
R2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3, main routing table version 3
2 network entries using 304 bytes of memory
2 path entries using 152 bytes of memory
2/2 BGP path/bestpath attribute entries using 248 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 752 total bytes of memory
BGP activity 5/1 prefixes, 6/2 paths, scan interval 60 secs

Neighbor           V    AS   MsgRcvd MsgSent TblVer  InQ OutQ    Up/Down
State/PfxRcd
19.19.19.19        4   100      46       54       3      0    0     00:42:45     1
2001:10:1:2::1     4   1        52       51       3      0    0     00:42:53     1
```

When R2 advertises R1's Loopback to XR1, two important things happen. The next-hop value of the IPv6 route gets a special encoding to point it to the IPv4 Loopback0 of R2, and an MPLS Label is allocated. You can think of this label similar to one that would be allocated by VPNv4 BGP in MPLS L3VPN designs. Below we see the label value that R2 assigns, that R2 is advertising the route to XR1, and the XR1 receives it with a next hop value of R2's IPv4 Loopback.

```
R2#show bgp ipv6 unicast 2001::1:1:1:1/128
BGP routing table entry for 2001::1:1:1:1/128, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     4
  1
    2001:10:1:2::1 (FE80::205:5FFF:FEAD:3800) from 2001:10:1:2::1 (1.1.1.1)
     Origin IGP, metric 0, localpref 100, valid, external, best mpls labels in/out 28/nolabel
R2#show bgp ipv6 unicast neighbors 19.19.19.19 advertised-routes
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next Hop        Metric LocPrf Weight Path
*> 2001::1:1:1:1/128
                       2001:10:1:2::1       0             0 1 i

Total number of prefixes 1



RP/0/0/CPU0:XR1#show bgp ipv6 unicast 2001::1:1:1:1/128
Thu Mar 29 21:53:28.991 UTC BGP routing table entry for 2001::1:1:1:1/128
Versions:
    Process  bRIB/RIB   SendTblVer
    Speaker         5            5
Last Modified: Mar 29 21:08:07.554 for 00:45:21
Paths: (1 available, best #1)
   Advertised to peers (in unique update groups):
     2001:10:19:20::20
   Path #1: Received by speaker 0
   1 2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2) Received Label 28

      Origin IGP, metric 0, localpref 100, valid, internal, best
```

When XR1 installs this in the routing table, the next-hop points to the IPv4 compatible address ::ffff:2.2.2.2. This essentially tells the routing process to find the MPLS Transport Label for 2.2.2.2 and use that for the top of the stack. Meanwhile, the IPv6 Unicast BGP learned label is inserted at the bottom of the stack, similar to how an MPLS L3VPN label would be.

```
RP/0/0/CPU0:XR1#show route ipv6
Thu Mar 29 21:58:03.189 UTC

Codes: C - connected, S - static, R - RIP, 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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G - DAGR
       A - access/subscriber

Gateway of last resort is not set
B 2001::1:1:1:1/128
      [200/0] via ::ffff:2.2.2.2 (nexthop in vrf default
), 00:49:56
B   2001::20:20:20:20/128
      [20/0] via fe80::c962:9dff:fee6:66ed, 00:49:00, POS0/6/0/0
C   2001:10:19:20::/64 is directly connected,
      01:28:01, POS0/6/0/0
L   2001:10:19:20::19/128 is directly connected,
      01:28:01, POS0/6/0/0
```

The route is then advertised from the PE router XR1 to the CE router XR2 over their normal IPv6 Unicast BGP session. XR2 receives this route and installs it via XR1's next-hop address.

```
RP/0/3/CPU0:XR2#show bgp ipv6 unicast
Thu Mar 29 22:01:44.952 UTC
BGP router identifier 20.20.20.20, local AS number 20
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0800000
BGP main routing table version 5
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
*> 2001::1:1:1:1/128   2001:10:19:20::19
```

```
                                              0 100 1 i
*> 2001::20:20:20:20/128
                         ::                          0         32768 i

Processed 2 prefixes, 2 paths
RP/0/3/CPU0:XR2#show route ipv6 2001::1:1:1:1
Thu Mar 29 22:01:51.448 UTC

Routing entry for 2001::1:1:1:1/128
    Known via "bgp 20", distance 20, metric 0
    Tag 100, type external
    Installed Mar 29 21:08:26.310 for 00:53:25
    Routing Descriptor Blocks fe80::18c4:6dff:fefe:1027, from 2001:10:19:20::19, via POS0/7/0/0

        Route metric is 0
    No advertising protos.
```

Now let's look at this from a data plane forwarding point of view. XR2, the CE router, sends a native IPv6 packet to the destination 2001::1:1:1:1.

```
RP/0/3/CPU0:XR2#ping 2001::1:1:1:1 source 2001::20:20:20:20

Thu Mar 29 22:05:50.854 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
```

XR1, the PE router, gets the packet and consults the CEF table on what to do with it.

```
RP/0/0/CPU0:XR1#show cef ipv6 2001::1:1:1:1/128 detail
Thu Mar 29 22:06:22.049 UTC
2001::1:1:1:1/128, version 3, internal 0x40040001 (ptr 0x9c71f4fc) [1], 0x0 (0x0),
0x4100 (0x9d5221e0)
 Updated Mar 29 21:08:07.066
 Prefix Len 128, traffic index 0, precedence routine (0)
  gateway array (0x9cdae5cc) reference count 1, flags 0x80700, source rib (3),
                [1 type 1 flags 0x901101 (0x9d5541b8) ext 0x0 (0x0)]
  LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0]
   via ::ffff:2.2.2.2, 3 dependencies, recursive [flags 0x10]
    next hop VRF - 'Unknown', table - 0xe0000000
    next hop ::ffff:2.2.2.2 via ::ffff:2.2.2.2:0
 next hop 20.6.19.6   Gi0/1/0/0.619 labels imposed {18 28}
```

```
Load distribution: 0 (refcount 1)

Hash    OK  Interface    Address
0       Y   Unknown      ::ffff:2.2.2.2:0
```

This output shows that even though XR1 has this as an IPv6 entry in the CEF table, the next-hop of ::ffff:2.2.2.2 recurses toward the IPv4 next-hop of 20.6.19.6, and should be label switched with the stack 18 28.

Debugs in the MPLS forwarding plane of R6 reveal that the packets come in as labeled with these values, and are continued to be switched toward the remote PE of R2.

```
R6#debug mpls packet

Packet debugging is on
R6#MPLS turbo: Fa0/0.619: rx: Len 126 Stack {18 0 59} {28 0 59}
- ipv6 data MPLS turbo: Fa0/0.36: tx: Len 126 Stack {17 0 58} {28 0 59}
 - ipv6 data MPLS turbo: Fa0/0.46: rx: Len 126 Stack {23 0 62} {16011 0 63}
 - ipv6 data MPLS turbo: Fa0/0.619: tx: Len 122 Stack {16011 0 61}
 - ipv6 data
<snip>
```

These four lines indicate the inbound ICMP Echo coming from XR1, the top label being swapped from 18 to 17 and forwarded toward R3, then the ICMP Echo-Reply coming in from R4 with label stack 23 16011, and 23 being popped because R6 is the penultimate Hop for R4, as correlated in the LFIB below.

```
R6#show mpls forwarding-table

Local    Outgoing     Prefix           Bytes Label Outgoing     Next Hop
Label    Label        or Tunnel Id     Switched     interface
16       Pop Label    4.4.4.4/32       0            Fa0/0.46     20.4.6.4
17       Pop Label    3.3.3.3/32       0            Fa0/0.36     20.3.6.3
18       17           2.2.2.2/32       19138        Fa0/0.36     20.3.6.3
         17           2.2.2.2/32       1452         Fa0/0.46     20.4.6.4

19       Pop Label    20.4.5.0/24      0            Fa0/0.46     20.4.6.4
20       Pop Label    20.2.4.0/24      0            Fa0/0.46     20.4.6.4
21       Pop Label    20.2.3.0/24      0            Fa0/0.36     20.3.6.3
22       Pop Label    20.3.4.0/24      0            Fa0/0.36     20.3.6.3
         Pop Label    20.3.4.0/24      0            Fa0/0.46     20.4.6.4
23       Pop Label    19.19.19.19/32   19880        Fa0/0.619    20.6.19.19

24       Pop Label    20.5.19.0/24     0            Fa0/0.619    20.6.19.19
R6#
```

The same thing occurs in the reverse direction here, where XR2 advertises its IPv6 Unicast BGP route to XR1, XR1 sends it as an IPv6 Labeled Unicast route to R2, and finally R2 sends it as a regular IPv6 Unicast BGP route to R1.

```
RP/0/3/CPU0:XR2#show bgp ipv6 unicast neighbors 2001:10:19:20::19 advertised-routes
Thu Mar 29 22:14:33.958 UTC
Network                 Next Hop     From     AS Path 2001::20:20:20:20/128
                          2001:10:19:20::20
RP/0/0/CPU0:XR1#show bgp ipv6 unicast 2001::20:20:20:20/128
Thu Mar 29 22:15:01.972 UTC
BGP routing table entry for 2001::20:20:20:20/128
Versions:
    Process      bRIB/RIB   SendTblVer
    Speaker             6             6 Local Label: 16011
Last Modified: Mar 29 21:08:48.554 for 01:06:13
Paths: (1 available, best #1)
   Advertised to peers (in unique update groups):
      2.2.2.2
   Path #1: Received by speaker 0
   20
     2001:10:19:20::20 from 2001:10:19:20::20 (20.20.20.20)
      Origin IGP, metric 0, localpref 100, valid, external, best
RP/0/0/CPU0:XR1#show bgp ipv6 labeled-unicast neighbors 2.2.2.2 advertised-routes
Thu Mar 29 22:15:28.749 UTC
Network             Next Hop     From     AS Path 2001::20:20:20:20/128
```

```
                        32.1.0.16   2001:10:19:20::20
                                20 i
R2#show bgp ipv6 unicast 2001::20:20:20:20/128
BGP routing table entry for 2001::20:20:20:20/128, version 3
Paths: (1 available, best #1, table default)
   Advertised to update-groups:
      3
   20     ::FFFF:19.19.19.19
 (metric 4) from 19.19.19.19 (19.19.19.19)
       Origin IGP, metric 0, localpref 100, valid, internal, best
       mpls labels in/out nolabel/16011
R2#show bgp ipv6 unicast neighbors 2001:10:1:2::1 advertised-routes
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network         Next Hop    Metric LocPrf  Weight  Path *>i2001::20:20:20:20/128
                    ::FFFF:19.19.19.19
                                   0   100         0  20 i

Total number of prefixes 1

R1#show bgp ipv6 unicast 2001::20:20:20:20/128

BGP routing table entry for 2001::20:20:20:20/128, version 3
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   100 20
    2001:10:1:2::2 (FE80::212:43FF:FE18:CB1C) from 2001:10:1:2::2 (2.2.2.2)
     Origin IGP, localpref 100, valid, external, best
```

Traffic in the data plane goes from R1 to R2, is label encapsulated by R2, is label switched through the core, and then comes back out as unlabeled IPv6 packets on the XR1 to XR2 link.

```
R1#traceroute ipv6
Target IPv6 address: 2001::20:20:20:20
 Source address: 2001::1:1:1:1
Insert source routing header? [no]:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]: Priority [0]:
```

```
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 2001::20:20:20:20

 1  2001:10:1:2::2 4 msec 0 msec 0 msec
2    ::FFFF:20.2.4.4 [MPLS: Labels 23/16011 Exp 0] 4 msec 0 msec 0 msec
3    ::FFFF:20.4.6.6 [MPLS: Labels 23/16011 Exp 0] 4 msec 0 msec 4 msec
4    ::FFFF:20.6.19.19 [MPLS: Label 16011 Exp 0] 108 msec 4 msec 4 msec

 5  2001::20:20:20:20 [AS 20] 44 msec 4 msec 4 msec
```

R2's IPv6 CEF entries point toward and IPv4 Label Switch Path.

```
R2#show ipv6 cef 2001::20:20:20:20/128 detail
2001::20:20:20:20/128, epoch 0, flags rib defined all labels   recursive via 19.19.19.19 label 16011
    nexthop 20.2.3.3 FastEthernet0/0.23 label 24
    nexthop 20.2.4.4 FastEthernet0/0.24 label 23
```

Devices in the transit path, such as R4, simply see labeled packets and do not need to know about the IPv6 payload.

```
R4#debug mpls packet
Packet debugging is on
R1#ping 2001::20:20:20:20 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20:20:20:20, timeout is 2 seconds:
Packet sent with a source address of 2001::1:1:1:1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms

R4# MPLS turbo: Fa0/0.24: rx: Len 126 Stack {23 0 63} {16011 0 63} - ipv6 data
MPLS turbo: Fa0/0.46: tx: Len 126 Stack {23 0 62} {16011 0 63} - ipv6 data

<snip>
```

The transport labels of 23 simply tell R4 to Label Switch traffic toward XR1's Loopback.

```
R4#show mpls forwarding-table
Local   Outgoing     Prefix          Bytes Label     Outgoing     Next Hop
Label   Label        or Tunnel Id    Switched        interface
16      Pop Label   3.3.3.3/32      0               Fa0/0.34     20.3.4.3
```

```
17      Pop Label   2.2.2.2/32      1412            Fa0/0.24    20.2.4.2
18      Pop Label   20.3.6.0/24     0               Fa0/0.34    20.3.4.3
        Pop Label   20.3.6.0/24     0               Fa0/0.46    20.4.6.6
19      Pop Label   20.2.3.0/24     0               Fa0/0.24    20.2.4.2
        Pop Label   20.2.3.0/24     0               Fa0/0.34    20.3.4.3
20      Pop Label   6.6.6.6/32      0               Fa0/0.46    20.4.6.6
21      Pop Label   20.6.19.0/24    0               Fa0/0.46    20.4.6.6
22      Pop Label   20.5.6.0/24     0               Fa0/0.46    20.4.6.6
23      23         19.19.19.19/32  23250            Fa0/0.46    20.4.6.6

24      24          20.5.19.0/24    0               Fa0/0.46    20.4.6.6
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.20 6VPE (pending update)

- The network is preconfigured as follows:
  - The Service Provider AS 100 consists of R2, R3, R4, R5, R6 and XR1.
  - AS 100 runs OSPF + LDP on all transit links, and is IPv4 only enabled.
  - Customer routers R1 and XR2 run both IPv4 and IPv6 to their PE routers R2 and XR1.
- Configure a VRF on R2 and XR1 as follows:
  - VRF Name: A
  - Route Distinguisher: 100:1
  - Route Target Import: 100:1
  - Route Target Export: 100:1
  - Assign the VRF to the links connecting to R1 and XR2, respectively.
- Configure BGP on R2 and XR1 as follows:
  - Use BGP AS 100.
  - R2 and XR1 should be iBGP peers for the VPNv4 and VPNv6 Address Families.
  - Use their Loopback0 interfaces as the source of the BGP session.
- Configure BGP on R1 and XR2 as follows:
  - Use BGP AS 1.
  - R1 and R2 should peer both IPv4 Unicast and IPv6 Unicast EBGP.
  - XR1 and XR2 should peer both IPv4 Unicast and IPv6 Unicast EBGP.
  - Advertise the IPv4 and IPv6 Loopback0 interfaces of R1 and XR2 into BGP.
- When complete, R1 and XR2 should be able to reach each other's IPv4 and IPv6 Loopback0 interfaces when sourcing traffic from their own Loopback0 interface.

Configuration

```
R1:
ipv6 unicast-routing
ipv6 cef
!
router bgp 1
```

```
 neighbor 10.1.2.2 remote-as 100
 neighbor 2001:10:1:2::2 remote-as 100
!
address-family ipv4
 network 1.1.1.1 mask 255.255.255.255
 neighbor 10.1.2.2 activate
 no neighbor 2001:10:1:2::2 activate
exit-address-family
!
address-family ipv6
 network 2001::1:1:1:1/128
 neighbor 2001:10:1:2::2 activate
exit-address-family

R2:
vrf definition A
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
 !
 address-family ipv6
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet1/0
 vrf forwarding A
 ip address 10.1.2.2 255.255.255.0
 ipv6 address 2001:10:1:2::2/64
!
router bgp 100
 no bgp default ipv4-unicast
 neighbor 19.19.19.19 remote-as 100
 neighbor 19.19.19.19 update-source Loopback0
 !
 address-family vpnv4
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
```

```
 address-family vpnv6
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf A
  neighbor 10.1.2.1 remote-as 1
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 as-override
 exit-address-family
 !
 address-family ipv6 vrf A
  neighbor 2001:10:1:2::1 remote-as 1
  neighbor 2001:10:1:2::1 activate
  neighbor 2001:10:1:2::1 as-override
 exit-address-family

XR1:
vrf A
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
 !
!
address-family ipv6 unicast
 import route-target
  100:1
 !
 export route-target
   100:1
  !
 !
!
interface POS0/6/0/0
 vrf A
 ipv4 address 10.19.20.19 255.255.255.0
 ipv6 address 2001:10:19:20::19/64
!
route-policy PASS
 pass end-
policy
!
router bgp 100
```

```
 address-family vpnv4 unicast
 !
 address-family vpnv6 unicast
 !
 neighbor 2.2.2.2
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
 !
 vrf A
  rd 100:1
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
  neighbor 10.19.20.20
   remote-as 1
   address-family ipv4 unicast route-
   policy PASS in
   route-policy PASS out as-
   override
  !
 !
 neighbor 2001:10:19:20::20
  remote-as 1
  address-family ipv6 unicast
    route-policy PASS in
    route-policy PASS out as-
    override
   !
  !
 !
!

XR2:
route-policy PASS
pass
end-policy
!
router bgp 1
address-family ipv4 unicast
network 20.20.20.20/32
!
```

```
address-family ipv6 unicast
network 2001::20:20:20:20/128
!
neighbor 10.19.20.19
remote-as 100
address-family ipv4 unicast
route-policy PASS in
route-policy PASS out
!
!
neighbor 2001:10:19:20::19
remote-as 100
address-family ipv6 unicast
route-policy PASS in
route-policy PASS out
!
!
!
```

Verification

Similar to the previous 6PE example, the goal of this design is to be able to transparently tunnel the customer's IPv6 traffic over the Service Provider's IPv4 only MPLS core. The difference between the previous 6PE and this current 6VPE design are similar to the "Basic MPLS Tunnels" and the "MPLS L3VPN" differences. In 6PE, the customer's routing information is learned in the global routing table, and IPv6 Labeled Unicast BGP is used to allocate MPLS labels. In 6VPE, the customer's routing information is learned in a VRF, and the MPLS Labels are exchanged through VPNv6 BGP.

Because the VRF on the PE to CE link is now running both IPv4 and IPv6 routing, it is required that it be defined with the `vrf definition` command in regular IOS as opposed to the legacy `ip vrf` command. When converting from the legacy syntax to the newer format, you can use the command `vrf upgrade-cli multi-af-mode` to automatically make the changes for you without having to disrupt connectivity within the VRF.

Just like the previous L3VPN examples, verification starts with the final connectivity test between the customer sites. R1 and XR2 should be transparently learning both the IPv4 and IPv6 routing information about each other's sites, as seen below.

```
R1#show ip route
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

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
        10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         10.1.2.0/24 is directly connected, FastEthernet0/0
L         10.1.2.1/32 is directly connected, FastEthernet0/0
        20.0.0.0/32 is subnetted, 1 subnetsB        20.20.20.20 [20/0] via 10.1.2.2, 00:13:58
```

```
R1#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
LC  2001::1:1:1:1/128 [0/0]
      via Loopback0, receiveB 2001::20:20:20:20/128 [20/0]
      via FE80::212:43FF:FE18:CB1C, FastEthernet0/0
C   2001:10:1:2::/64 [0/0]
      via FastEthernet0/0, directly connected
L   2001:10:1:2::1/128 [0/0]
      via FastEthernet0/0, receive L    FF00::/8 [0/0]
      via Null0, receive
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/3/4 ms
R1#ping 2001::20:20:20:20 source 2001::1:1:1:1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20:20:20:20, timeout is 2 seconds:
Packet sent with a source address of 2001::1:1:1:1
```

```
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 0/2/4 ms
```

For detailed verification of the control plane, we start with R1's advertisement of the IPv4 and IPv6 addresses of its Loopback0 interface. These are advertised to the PE router R2 via IPv4 Unicast BGP and IPv6 Unicast BGP, respectively.

```
R1#show bgp ipv4 unicast
BGP table version is 11, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop    Metric  LocPrf  Weight  Path
*> 1.1.1.1/32      0.0.0.0          0            32768
    i
*> 20.20.20.20/32   10.1.2.2                        0  100 100 i


R1#show bgp ipv4 unicast neighbors 10.1.2.2 advertised-routes
BGP table version is 11, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop    Metric LocPrf  Weight Path
*> 1.1.1.1/32      0.0.0.0          0          32768 i

Total number of prefixes 1
R1#show bgp ipv6 unicast
BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop        Metric LocPrf Weight Path*> 2001::1:1:1:1/128
                    ::                   0         32768 i
*> 2001::20:20:20:20/128
                    2001:10:1:2::2                     0 100 100 i
R1#show bgp ipv6 unicast neighbors 2001:10:1:2::2 advertised-routes
BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
     Network              Next Hop     Metric LocPrf Weight Path *> 2001::1:1:1:1/128
                          ::                0         32768  i

 Total number of prefixes 1
```

R2 learns these from the customer router R1 in the VRF A table.

```
R2#show ip route vrf A



Routing Table: A
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets    B      1.1.1.1 [20/0] via 10.1.2.1, 00:22:04

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.2.0/24 is directly connected, FastEthernet1/0
L       10.1.2.2/32 is directly connected, FastEthernet1/0
    20.0.0.0/32 is subnetted, 1 subnets
B       20.20.20.20 [200/0] via 19.19.19.19, 00:17:09
R2#show ipv6 route vrf A

IPv6 Routing Table - A - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 B 2001::1:1:1:1/128 [20/0]

      via FE80::205:5FFF:FEAD:3800, FastEthernet1/0
B   2001::20:20:20:20/128 [200/0]
      via 19.19.19.19%default, indirectly connected
C   2001:10:1:2::/64 [0/0]
      via FastEthernet1/0, directly connected
L   2001:10:1:2::2/128 [0/0]
      via FastEthernet1/0, receive
L   FF00::/8 [0/0]
      via Null0, receive
```

Because these prefixes are already learned from the customer via BGP, no redistribution is required. Instead, R2 automatically converts these routes into

VPNv4 and VPNv6 prefixes, respectively. This is where R2 allocates VPNv4 and VPNv6 MPLS Labels for the prefixes as well. In this example, the Route Target Export policy is the same for both VPNv4 and VPNv6, but they technically are unrelated and can be set independently as desired.

```
R2#show bgp vpnv4 unicast all 1.1.1.1/32
BGP routing table entry for 100:1:1.1.1.1/32
, version 2
Paths: (1 available, best #1, table A)
  Advertised to update-groups:
     4
  1
     10.1.2.1 from 10.1.2.1 (1.1.1.1)
       Origin IGP, metric 0, localpref 100, valid, external, best        Extended Community: RT:100:1
mpls labels in/out 29/nolabel
R2#show bgp vpnv6 unicast all 2001::1:1:1:1/128
BGP routing table entry for [100:1]2001::1:1:1:1/128
, version 2
Paths: (1 available, best #1, table A)
   Advertised to update-groups:
     4
   1
     2001:10:1:2::1 (FE80::205:5FFF:FEAD:3800) from 2001:10:1:2::1 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, external, best      Extended Community: RT:100:1
mpls labels in/out 27/nolabel
```

R2 then advertises these VPNv4 and VPNv6 routes to the remote PE XR1 via the iBGP sessions.

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf A 1.1.1.1/32
Thu Mar 29 23:36:21.432 UTC BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
    Process bRIB/RIB    SendTblVer
    Speaker         4           4
Last Modified: Mar 29 23:13:30.554 for 00:22:51
Paths: (1 available, best #1)
   Not advertised to any peer
   Path #1: Received by speaker 0
   1 2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2) Received Label 29
      Origin IGP, metric 0, localpref 100, valid, internal, best, import-candidate,
imported      Extended community: RT:100:1
```

```
RP/0/0/CPU0:XR1#show bgp vpnv6 unicast vrf A 2001::1:1:1:1/128

Thu Mar 29 23:36:36.027 UTC BGP routing table entry for 2001::1:1:1:1/128, Route Distinguisher: 100:1
Versions:
    Process  bRIB/RIB   SendTblVer
    Speaker         3            3
Last Modified: Mar 29 23:15:25.554 for 00:21:10
Paths: (1 available, best #1)
   Not advertised to any peer
   Path #1: Received by speaker 0
   1 2.2.2.2
 (metric 4) from 2.2.2.2 (2.2.2.2) Received Label 27
      Origin IGP, metric 0, localpref 100, valid, internal, best, import-candidate,
imported      Extended community: RT:100:1
```

Note that both for the VPNv4 and the VPNv6 routes the next-hop is the IPv4 address 2.2.2.2. This is how the Service Provider is able to tunnel IPv6 traffic over the IPv4 only core, because the transport label of both the IPv4 and IPv6 tunnels point toward the IPv4 Loopback addresses of the PE routers. It is assumed that the core of the MPLS network already has IGP routes and LDP labels for these addresses, or labels through some other mechanism like MPLS TE or static bindings.

Note that under both address-families of IPv4 and IPv6 the `as-override` command is needed on both PEs, because the customer's AS number 1 would otherwise prevent the routes from being learned.

The final result of this design is that the customer can transit both IPv4 and IPv6 traffic through the SP network, while the SP core simply uses the LSP between R2 and XR1 to provide the transit. This can be seen from the MPLS data plane debugs in the core as follows.

```
R3#debug mpls packet
Packet debugging is on
R4#debug mpls packet
Packet debugging is on
R1#ping 2001::20:20:20:20 source 2001::1:1:1:1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20:20:20:20, timeout is 2 seconds:
Packet sent with a source address of 2001::1:1:1:1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
```

```
R4# MPLS turbo: Fa0/0.24: rx: Len 126 Stack {23 0 63} {16013 0 63} - ipv6 data
MPLS turbo: Fa0/0.46: tx: Len 126 Stack {23 0 62} {16013 0 63} - ipv6 data
MPLS turbo: Fa0/0.46: rx: Len 126 Stack {17 0 62} {27 0 63} - ipv6 data
MPLS turbo: Fa0/0.24: tx: Len 122 Stack {27 0 61} - ipv6 data
<snip>


R4# MPLS turbo: Fa0/0.24: rx: Len 126 Stack {23 0 254} {16012 0 254} - ipv4 data
MPLS turbo: Fa0/0.46: tx: Len 126 Stack {23 0 253} {16012 0 254} - ipv4 data

R3# MPLS turbo: Fa0/0.36: rx: Len 126 Stack {17 5 253} {29 5 254} - ipv4 data
MPLS turbo: Fa0/0.23: tx: Len 122 Stack {29 5 252} - ipv4 data
```

Note that the transport labels seen on R4 are identical for both the IPv4 and the IPv6 traffic, because both are following the same LSP. Transport labels 23 and 17 on R4 represent the Loopbacks of XR1 and R2, respectively, whereas transport label 17 on R3 represents the Loopback of R2. The LSP is transiting both of these routers because there are multiple equal cost OSPF paths between the PE routers R2 and XR1.

```
R4#show mpls forwarding-table
Local     Outgoing    Prefix           Bytes Label     Outgoing     Next Hop
Label     Label       or Tunnel Id     Switched        interface
16       Pop Label    3.3.3.3/32       0               Fa0/0.34     20.3.4.3
17       Pop Label    2.2.2.2/32       4462            Fa0/0.24     20.2.4.2
18       Pop Label    20.3.6.0/24      0               Fa0/0.34     20.3.4.3
         Pop Label    20.3.6.0/24      0               Fa0/0.46     20.4.6.6
19       Pop Label    20.2.3.0/24      0               Fa0/0.24     20.2.4.2
         Pop Label    20.2.3.0/24      0               Fa0/0.34     20.3.4.3
20       Pop Label    6.6.6.6/32       0               Fa0/0.46     20.4.6.6
21       Pop Label    20.6.19.0/24     0               Fa0/0.46     20.4.6.6
22       Pop Label    20.5.6.0/24      0               Fa0/0.46     20.4.6.6
23       23           19.19.19.19/32 45996             Fa0/0.46     20.4.6.6
24       24           20.5.19.0/24     0               Fa0/0.46     20.4.6.6
R3#show mpls forwarding-table
Local         Outgoing    Prefix           Bytes Label    Outgoing     Next Hop
Label         Label       or Tunnel Id     Switched       interface
16           Pop Label    4.4.4.4/32       0               Fa0/0.34     20.3.4.4
17           Pop Label    2.2.2.2/32       40468           Fa0/0.23     20.2.3.2


18           Pop Label    20.4.6.0/24      0               Fa0/0.34     20.3.4.4
             Pop Label    20.4.6.0/24      0               Fa0/0.36     20.3.6.6
19           Pop Label    20.4.5.0/24      0               Fa0/0.34     20.3.4.4
20           Pop Label    20.2.4.0/24      0               Fa0/0.23     20.2.3.2
```

```
            Pop Label   20.2.4.0/24     0           Fa0/0.34    20.3.4.4
21          Pop Label   6.6.6.6/32      0           Fa0/0.36    20.3.6.6
22          Pop Label   20.6.19.0/24    0           Fa0/0.36    20.3.6.6
23          Pop Label   20.5.6.0/24     0           Fa0/0.36    20.3.6.6
24          23          19.19.19.19/32  0           Fa0/0.36    20.3.6.6
25          24          20.5.19.0/24    0           Fa0/0.36    20.3.6.6
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.21 MPLS L2 VPN with AToM – Ethernet to Ethernet (pending update)

- Configure R2 and XR1 for L2VPN with Any Transport over MPLS as follows:
  - The attachment circuits are the Ethernet links connecting to R1 and R7.
  - R2 and XR1 should form a pseudowire between their Loopback0 interfaces.
- When complete, R1 and R7 should form an OSPFv2 adjacency and have IP reachability to each other's Looopback0 networks.

Configuration

```
R2:
pseudowire-class ETH_TO_ETH
 encapsulation mpls
!
interface FastEthernet1/0
 xconnect 19.19.19.19 1 pw-class ETH_TO_ETH

XR1:
interface GigabitEthernet0/1/0/1
 no cdp
 l2transport
 !
!
l2vpn
 pw-class ETH_TO_ETH
  encapsulation mpls
 !
!
xconnect group GROUP1
 p2p PORT1
  interface GigabitEthernet0/1/0/1
  neighbor 2.2.2.2 pw-id 1
   pw-class ETH_TO_ETH
```

Verification

MPLS L2VPN differs from L3VPN in the fact that the customer does not peer Layer 3 Routing with the Service Provider. Instead, customer sites are on the same emulated layer 2 network, similar to legacy Frame Relay or ATM networks. This means that the customer's Layer 3 Routing happens as an overlay on top of the L2VPN, and all details of the Service Provider MPLS network are completely transparent to the customer.

The first verification for MPLS L2VPN with AToM is to ensure that an LSP can be formed between the PE routers' Loopback interfaces. This is similar to the requirement of L3VPN forming a VPNv4 BGP peering over an LSP between PE Loopbacks, but with AToM the labels are allocated by targeted LDP sessions. As seen below, a traceroute verifies that an LSP does exist between the PE's Loopback interfaces.

```
R2#traceroute 19.19.19.19 source lo0
```

```
Type escape sequence to abort.
Tracing the route to 19.19.19.19

 1  20.2.3.3 [MPLS: Label 26 Exp 0] 4 msec
    20.2.4.4 [MPLS: Label 25 Exp 0] 0 msec
    20.2.3.3 [MPLS: Label 26 Exp 0] 4 msec
 2  20.4.6.6 [MPLS: Label 25 Exp 0] 0 msec
    20.3.6.6 [MPLS: Label 25 Exp 0] 4 msec
    20.4.6.6 [MPLS: Label 25 Exp 0] 0 msec
 3  20.6.19.19 16 msec *    4 msec
```

The next step in AToM is to establish the Pseudowire adjacency between the PE routers. This occurs automatically when the **xconnect** is configured on the Attachment Circuit, which is the CE facing link. If the **xconnect** is successful, the PE routers should form an LDP adjacency, as seen below.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#pseudowire-class ETH_TO_ETH
R2(config-pw-class)# encapsulation mpls
R2(config-pw-class)#!R2(config-pw-class)#interface FastEthernet1/0
R2(config-if)# xconnect 19.19.19.19 1 pw-class ETH_TO_ETH
R2(config-if-xconn)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#%LDP-5-NBRCHG: LDP Neighbor 19.19.19.19:0 (3) is UP



R2#show mpls ldp neighbor 19.19.19.19 detail
    Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 2.2.2.2:0
        TCP connection: 19.19.19.19.25815 - 2.2.2.2.646
        Password: not required, none, in use
        State: Oper; Msgs sent/rcvd: 48/47; Downstream; Last TIB rev sent 30
        Up time: 00:23:12; UID: 3; Peer Id 2;
        LDP discovery sources: Targeted Hello 2.2.2.2 -> 19.19.19.19
, active, passive;
            holdtime: infinite, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
           19.19.19.19  20.5.19.19  20.6.19.19
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
        Clients: Dir Adj Client
        Capabilities Sent:
          [ICCP (type 0x0405) MajVer 1 MinVer 0]
          [Dynamic Announcement (0x0506)]
          [mLDP Point-to-Multipoint (0x0508)]
          [mLDP Multipoint-to-Multipoint (0x0509)]
```

```
        Capabilities Received:
          [None]
RP/0/0/CPU0:XR1#show mpls ldp neighbor 2.2.2.2 detail
Fri Mar 30 13:36:50.871 UTC

Peer LDP Identifier: 2.2.2.2:0
    TCP connection: 2.2.2.2:646 - 19.19.19.19:25815
    Graceful Restart: No
    Session Holdtime: 180 sec
    State: Oper; Msgs sent/rcvd: 47/48
    Up time: 00:23:24
    LDP Discovery Sources: Targeted Hello (19.19.19.19 -> 2.2.2.2, active)

    Addresses bound to this peer:
       2.2.2.2  20.2.3.2    20.2.4.2
    Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
    NSR: Disabled
    Clients: AToM
```

This targeted LDP session is then used between the PE routers to exchange the Pseudowire Label, which is analogous to the VPNv4 BGP Label in MPLS L3VPN. The Pseudowire Label is what the PE routers use to figure out which Attachment Circuit traffic should forwarded toward when labeled packets arrive in the data plane from the Service Provider network. This could likewise be considered the “L2VPN Label.” This label will be used at the bottom of the stack, whereas the transport label between the xconnect interfaces (the PE routers’ Loopbacks) will be on the top of the stack. This label number can be verified just like a normal L3VPN label as follows.

```
R2#show mpls forwarding-table
Local    Outgoing     Prefix          Bytes Label Outgoing     Next Hop
Label     Label       or Tunnel Id    Switched    interface
16   Pop Label       4.4.4.4/32      0           Fa0/0.24     20.2.4.4
17   Pop Label       3.3.3.3/32      0           Fa0/0.23     20.2.3.3
18   Pop Label       20.4.5.0/24     0           Fa0/0.24     20.2.4.4
19   Pop Label       20.4.6.0/24     0           Fa0/0.24     20.2.4.4
20   Pop Label       20.3.4.0/24     0           Fa0/0.23     20.2.3.3
     Pop Label       20.3.4.0/24     0           Fa0/0.24     20.2.4.4
21   Pop Label       20.3.6.0/24     0           Fa0/0.23     20.2.3.3
22   21              6.6.6.6/32      0           Fa0/0.23     20.2.3.3
     16              6.6.6.6/32      0           Fa0/0.24     20.2.4.4
23   17              5.5.5.5/32      0           Fa0/0.24     20.2.4.4
24   25              20.6.19.0/24    0           Fa0/0.23     20.2.3.3
     20              20.6.19.0/24    0           Fa0/0.24     20.2.4.4
25   24              20.5.6.0/24     0           Fa0/0.23     20.2.3.3
```

```
    22              20.5.6.0/24     0           Fa0/0.24    20.2.4.4
26  21              20.5.19.0/24    0           Fa0/0.24    20.2.4.4
27  26              19.19.19.19/32  0           Fa0/0.23    20.2.3.3
    25              19.19.19.19/32  0           Fa0/0.24    20.2.4.4
29 No Label        l2ckt(1)        53727       Fa1/0       point2point
```

```
RP/0/0/CPU0:XR1#show mpls forwarding
Fri Mar 30 13:40:17.607 UTC
Local   Outgoing       Prefix                 Outgoing       Next Hop            Bytes
Label   Label          or ID                  Interface                          Switched
------   -----------   ------------------     ------------   ---------------     ------------
16000   19             2.2.2.2/32             Gi0/1/0/0.519  20.5.19.5           65589
        19             2.2.2.2/32             Gi0/1/0/0.619  20.6.19.6           17291
16001   18             3.3.3.3/32             Gi0/1/0/0.619  20.6.19.6           0
16002   17             4.4.4.4/32             Gi0/1/0/0.519  20.5.19.5           0
        17             4.4.4.4/32             Gi0/1/0/0.619  20.6.19.6           0
16003   Pop            5.5.5.5/32             Gi0/1/0/0.519  20.5.19.5           3454
16004   Pop            6.6.6.6/32             Gi0/1/0/0.619  20.6.19.6           3498
16005   Pop            20.5.6.0/24            Gi0/1/0/0.519  20.5.19.5           0
        Pop            20.5.6.0/24            Gi0/1/0/0.619  20.6.19.6           0
16006   Pop            20.3.6.0/24            Gi0/1/0/0.619  20.6.19.6           0
16007   Pop            20.4.5.0/24            Gi0/1/0/0.519  20.5.19.5           0
16008   Pop            20.4.6.0/24            Gi0/1/0/0.619  20.6.19.6           0
16009   23             20.3.4.0/24            Gi0/1/0/0.519  20.5.19.5           0
        22             20.3.4.0/24            Gi0/1/0/0.619  20.6.19.6           0
16010   21             20.2.4.0/24            Gi0/1/0/0.519  20.5.19.5           0
        23             20.2.4.0/24            Gi0/1/0/0.619  20.6.19.6           0
16011   24             20.2.3.0/24            Gi0/1/0/0.619  20.6.19.6           0
16014   Pop            PW(2.2.2.2:1)          Gi0/1/0/1      point2point        124088
```

In the above output, R2 denotes the Psuedowire Label as the “layer 2 circuit” (l2ckt) label, whereas XR1 denotes this as the Psuedowire (PW) Label. A verification of the data plane should show these labels in the bottom of the stack, as seen from the **debug mpls packet** in the transit path below.

```
R3#debug mpls packet
Packet debugging is on
R4#debug mpls packet
Packet debugging is on
R1#ping 7.7.7.7 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R3#MPLS turbo: Fa0/0.23: rx: Len 86 Stack {26 0 255} {16014 0 255
} CW {1 0 49664}
MPLS turbo: Fa0/0.36: tx: Len 86 Stack {25 0 254} {16014 0 255} CW {1 0 49664}
MPLS turbo: Fa0/0.23: rx: Len 120 Stack {26 0 255} {16014 0 255} CW {1 0 24064}
MPLS turbo: Fa0/0.36: tx: Len 120 Stack {25 0 254} {16014 0 255} CW {1 0 24064}

R4#MPLS turbo: Fa0/0.45: rx: Len 140 Stack {19 0 254} {29 0 254
} CW {0 5 24493}
MPLS turbo: Fa0/0.24: tx: Len 136 Stack {29 0 253} CW {0 5 24493}
MPLS turbo: Fa0/0.45: rx: Len 140 Stack {19 0 254} {29 0 254} CW {0 5 24493}
MPLS turbo: Fa0/0.24: tx: Len 136 Stack {29 0 253} CW {0 5 24493}
```

Label values 16014 and 29 on R3 and R4, respectively, show the L2VPN Pseudowire Label in the transit path. The labels 26, 25, and 19 on the top of the stack represent the transport labels for the Loopbacks of R2 and XR1. The detailed attributes of the Pseudowire between R2 and XR1 can be verified as follows.

```
R2#show mpls l2transport vc detail
Local interface: Fa1/0 up, line protocol up, Ethernet up
  Destination address: 19.19.19.19, VC ID: 1, VC status: up
     Output interface: Fa0/0.23, imposed label stack {26 16014}

     Preferred path: not configured
     Default path: active
     Next hop: 20.2.3.3
   Create time: 00:33:56, last status change time: 00:33:35
   Signaling protocol: LDP, peer 19.19.19.19:0 up
Targeted Hello: 2.2.2.2(LDP Id) -> 19.19.19.19, LDP is UP
    Status TLV support (local/remote)   : enabled/not supported
     LDP route watch                   : enabled
     Label/status state machine        : established, LruRru
     Last local dataplane status rcvd: No fault
     Last local SSS circuit status rcvd: No fault
     Last local SSS circuit status sent: No fault
     Last local LDP TLV status sent: No fault
     Last remote LDP TLV status rcvd: Not sent
     Last remote LDP ADJ   status rcvd: No fault MPLS VC labels: local 29, remote 16014
  Group ID: local 0, remote 33555456
  MTU: local 1500, remote 1500
  Remote interface description: GigabitEthernet0_1_0_1
 Sequencing: receive disabled, send disabled
 Control Word: Off (configured: autosense)
 VC statistics:
```

```
   transit packet totals: receive 266, send 1618
   transit byte totals: receive 60934, send 186416
   transit packet drops:    receive 0, seq error 0, send 0
RP/0/0/CPU0:XR1#show l2vpn xconnect detail
Fri Mar 30 13:48:03.383 UTC
Group GROUP1, XC PORT1, state is up
; Interworking none  AC: GigabitEthernet0/1/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x2000001; interworking none
    Statistics:
      packets: received 283, sent 1666
      bytes: received 75738, sent 147785 PW: neighbor 2.2.2.2, PW ID 1, state is up ( established
)
   PW class ETH_TO_ETH, XC ID 0x2000001
   Encapsulation MPLS, protocol LDP
   PW type Ethernet, control word disabled, interworking none
   PW backup disable delay 0 sec
   Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ ----------------------------
Label       16014                           29


Group ID     0x2000400                      0x0
Interface    GigabitEthernet0/1/0/1         unknown
MTU          1500                           1500
Control word disabled                       disabled
PW type      Ethernet                       Ethernet
VCCV CV type 0x2                            0x2
            (LSP ping verification)         (LSP ping verification)
VCCV CC type 0x6                            0x6
            (router alert label)            (router alert label)
            (TTL expiry)                    (TTL expiry)
------------ ------------------------------ ----------------------------
MIB cpwVcIndex: 1
Create time: 30/03/2012 13:13:21 (00:34:41 ago)
Last time status changed: 30/03/2012 13:13:26 (00:34:36 ago)
Statistics:
   packets: received 1666, sent 283
   bytes: received 147785, sent 75738
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.22 MPLS L2 VPN with AToM – PPP to PPP (pending update)

- Configure PPP encapsulation on the Serial and POS interfaces of R8 and XR2, respectively.
- Configure R2 and XR1 for L2VPN with Any Transport over MPLS as follows:
  - The attachment circuits are the Serial and POS links connecting to R8 and XR2.
  - Use an MTU of 1504 on the POS link between XR1 and XR2.
  - R2 and XR1 should form a pseudowire between their Loopback0 interfaces.
- When complete, R8 and XR2 should form an OSPFv2 adjacency and have IP reachability to each other's Looopback0 networks.

Configuration

```
R2:
pseudowire-class PPP_TO_PPP
 encapsulation mpls
!
interface Serial2/0
 encapsulation ppp
 clock rate 2016000
 xconnect 19.19.19.19 2 pw-class PPP_TO_PPP

R8:
interface Serial0/0
 ip address 10.0.0.8 255.255.255.0
 encapsulation ppp

XR1:
interface POS0/6/0/0
 ! MTU includes layer 2 header
 mtu 1504
 encapsulation ppp
 l2transport
```

```
 !
!
l2vpn
 pw-class PPP_TO_PPP
 encapsulation mpls
 !
!
xconnect group GROUP1
 p2p PORT2
 interface POS0/6/0/0
 neighbor 2.2.2.2 pw-id 2
  pw-class PPP_TO_PPP

XR2:
interface POS0/7/0/0
 ! MTU includes layer 2 header
 mtu 1504
 ipv4 address 10.0.0.20 255.255.255.0
 encapsulation ppp
```

Verification

Like in the previous L2VPN sections, the final verification for this task is to establish end-to-end connectivity between the customer sites, as seen below. Note that the customer sites appear as if they are directly connected.

```
RP/0/3/CPU0:XR2#show route ospf
Fri Mar 30 14:07:12.461 UTC
O 8.8.8.8/32 [110/2] via 10.0.0.8, 00:06:54, POS0/7/0/0
RP/0/3/CPU0:XR2#traceroute 8.8.8.8 source 20.20.20.20
Fri Mar 30 14:07:18.838 UTC

Type escape sequence to abort.
Tracing the route to 8.8.8.8
 1 10.0.0.8 10 msec * 3 msec
```

Because end-to-end connectivity is working, this implies that the Attachment Circuit between the CE to PE is working, the Pseudowire between the PEs is working, and the LSP between the PEs in the core of the MPLS network is working. The summary of these three parts can be verified as follows.

```
R2#show mpls l2transport vc detail
Local interface: Se2/0 up, line protocol up, PPP up
```

```
Destination address: 19.19.19.19, VC ID: 2, VC status: up
    Output interface: Fa0/0.23, imposed label stack {26 16012}

    Preferred path: not configured
    Default path: active
    Next hop: 20.2.3.3
   Create time: 00:09:47, last status change time: 00:08:35
   Signaling protocol: LDP, peer 19.19.19.19:0 up
Targeted Hello: 2.2.2.2(LDP Id) -> 19.19.19.19, LDP is UP
    Status TLV support (local/remote)   : enabled/not supported
     LDP route watch    : enabled
     Label/status state machine : established, LruRru
     Last local dataplane   status rcvd: No fault
     Last local SSS circuit status rcvd: No fault
     Last local SSS circuit status sent: No fault
     Last local LDP TLV status sent: No fault
     Last remote LDP TLV status rcvd: Not sent
     Last remote LDP ADJ   status rcvd: No fault
    MPLS VC labels: local 28, remote 16012
    Group ID: local 0, remote 117441536  MTU: local 1500, remote 1500
    Remote interface description: POS0_6_0_0
   Sequencing: receive disabled, send disabled
   Control Word: On (configured: autosense)
   VC statistics:
    transit packet totals: receive 819, send 415
    transit byte totals:    receive 57610, send 23486
    transit packet drops:   receive 0, seq error 0, send 0
RP/0/0/CPU0:XR1#show l2vpn xconnect detail
Fri Mar 30 14:09:04.589 UTC
Group GROUP1, XC PORT2, state is up
; Interworking none  AC: POS0/6/0/0, state is up
    Type PPP    MTU 1500; XC ID 0x7000001; interworking none
    Statistics:
      packets: received 849, sent 428
      bytes: received 61472, sent 12394 PW: neighbor 2.2.2.2, PW ID 2, state is up ( established )
    PW class PPP_TO_PPP, XC ID 0x7000001
    Encapsulation MPLS, protocol LDP
    PW type PPP, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -----------------------------
Label       16012                          28
Group ID     0x7000400                      0x0
Interface    POS0/6/0/0                     unknown MTU          1500                          1500
```

```
Control word enabled                          enabled
PW type      PPP                              PPP
VCCV CV type 0x2                              0x2
            (LSP ping verification)           (LSP ping verification)
VCCV CC type 0x7                              0x7
            (control word)                    (control word)
            (router alert label)              (router alert label)
            (TTL expiry)                      (TTL expiry)
------------ ------------------------------ -----------------------------
MIB cpwVcIndex: 2
Create time: 30/03/2012 13:59:36 (00:09:29 ago)
Last time status changed: 30/03/2012 14:00:15 (00:08:49 ago)
Statistics:
  packets: received 428, sent 849
  bytes: received 12394, sent 61472
```

An additional consideration that is needed for this PPP to PPP L2VPN is that the MTU of a Packet over SONET interface is by default 4474 bytes, as seen below.

```
RP/0/3/CPU0:XR2#show interfaces pos0/7/0/0
Fri Mar 30 14:11:36.330 UTC
POS0/7/0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Packet over SONET/SDH
  Internet address is 10.0.0.20/24  MTU 4474 bytes
, BW 2488320 Kbit
    reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation PPP, crc 32, controller loopback not set, keepalive set (10 sec)
  LCP Open
  Open: CDPCP, IPCP
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
   11616 packets input, 482025 bytes, 0 total input drops
   0 drops for unrecognized upper-level protocol
   Received 0 runts, 0 giants, 0 throttles, 0 parity
   33 input errors, 33 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   13498 packets output, 809351 bytes, 0 total output drops
   0 output errors, 0 underruns, 0 applique, 0 resets
   0 output buffer failures, 0 output buffers swapped out
```

Because R8 and XR2 will appear as if they are directly connected over their L2VPN, the MTU needs to match not only for OSPF to work, but also for the PPP Link

Control Protocol (LCP) negotiation. In IOS XR, the `mtu` command also includes the layer 2 encapsulation overhead, so it must be set to 1504 bytes to account for the 4 byte PPP encapsulation. When set to 1500 bytes, a log message appears notifying you of the configuration error, as seen below.

```
  RP/0/0/CPU0:XR1#config t
Fri Mar 30 14:22:56.188 UTCRP/0/0/CPU0:XR1(config)#int pos0/6/0/0
 RP/0/0/CPU0:XR1(config-if)#mtu 1500

RP/0/0/CPU0:XR1(config-if)#commit LC/0/6/CPU0:Mar 30 14:23:00.215 : PPP-MA[246]:
%L2-PPP_LCP-4-MTU_WARNING :
POS0/6/0/0 has a PPP MTU of 1496 which is smaller than the minimum value (1500)
required for correct operation
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.23 MPLS L2 VPN with AToM – Frame Relay to Frame Relay (pending update)

- Configure Frame Relay on the Serial interfaces between R2 and R8 and the POS interfaces between XR1 and XR2 as follows:
  - Use an MTU of 1500 on the POS link of XR1.
  - Use an MTU of 1504 on the POS link of XR2.
  - Use a Frame Relay PVC of 100.
  - Use the main Serial interface on R8.
  - Use the subinterface .100 on XR2.
  - Enable OSPF on XR2's Frame Relay subinterface.
- Configure R2 and XR1 for L2VPN with Any Transport over MPLS as follows:
  - The attachment circuits are the Serial and POS links connecting to R8 and XR2.
  - R2 and XR1 should form a pseudowire between their Loopback0 interfaces.
- When complete, R8 and XR2 should form an OSPFv2 adjacency and have IP reachability to each other's Looopback0 networks.

Configuration

```
R2:
frame-relay switching
!
pseudowire-class FR_TO_FR
 encapsulation mpls
!
interface Serial2/0
 encapsulation frame-relay
 clock rate 2016000
 frame-relay intf-type dce
!
connect FR Serial2/0 100 l2transport
 xconnect 19.19.19.19 3 pw-class FR_TO_FR
```

```
R8:
interface Serial0/0
 ip address 10.0.0.8 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-point
 frame-relay map ip 10.0.0.20 100 broadcast

XR1:
interface POS0/6/0/0
 no cdp
 mtu 1500
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface POS0/6/0/0.100 l2transport
 pvc 100
 !
!
l2vpn
 pw-class FR_TO_FR
  encapsulation mpls
  !
 !
xconnect group GROUP1
 p2p PORT3
  interface POS0/6/0/0.100 neighbor 2.2.2.2 pw-id 3
  pw-class FR_TO_FR

XR2:
interface POS0/7/0/0
 no cdp
 encapsulation frame-relay
 mtu 1504
!
interface POS0/7/0/0.100 point-to-point
 ipv4 address 10.0.0.20 255.255.255.0
 pvc 100
```

Verification

This example is similar to the previous AToM PPP to PPP scenario, but in this case Frame Relay encapsulation is used on the Attachment Circuit. The caveats with the Frame Relay configuration include that regular IOS must use the `frame-relay switching` command, that the MTU of IOS XR must be lowered to match the low speed Serial MTU of regular IOS, and the OSPF network type mismatch between the customer routers. Final verification again is the end-to-end connectivity between the customer routers.

```
R8#show ip route ospf
    20.0.0.0/32 is subnetted, 1 subnets
O       20.20.20.20 [110/65] via 10.0.0.20, 00:37:04, Serial0/0
R8#ping 20.20.20.20 source 8.8.8.8



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The same commands are used for the Pseudowire verification on R2 and XR1 as before.

```
R2#show mpls l2transport vc detail
Local interface: Se2/0 up, line protocol up, FR DLCI 100 up
  Destination address: 19.19.19.19, VC ID: 3, VC status: up
     Output interface: Fa0/0.24, imposed label stack {25 16013}

     Preferred path: not configured
     Default path: active
     Next hop: 20.2.4.4
    Create time: 00:49:00, last status change time: 00:39:03
    Signaling protocol: LDP, peer 19.19.19.19:0 up
Targeted Hello: 2.2.2.2(LDP Id) -> 19.19.19.19, LDP is UP
     Status TLV support (local/remote)  : enabled/not supported
      LDP route watch       : enabled Label/status state machine    : established, LruRru
      Last local dataplane  status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local LDP TLV status sent: No fault
      Last remote LDP TLV status rcvd: Not sent
      Last remote LDP ADJ   status rcvd: No fault
    MPLS VC labels: local 28, remote 16013
    Group ID: local 0, remote 117441536 MTU: local 1500, remote 1500
    Remote interface description: POS0_6_0_0.100
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VC statistics:
```

```
    transit packet totals: receive 292, send 321
    transit byte totals:    receive 24312, send 36268
    transit packet drops:   receive 0, seq error 0, send 0


RP/0/0/CPU0:XR1#show l2vpn xconnect detail
Fri Mar 30 15:18:10.076 UTC
 Group GROUP1, XC PORT3, state is up
; Interworking none  AC: POS0/6/0/0.100, state is up
 Type Frame Relay DLCI; DLCI = 100
MTU 1500; XC ID 0x7000001; interworking none
Statistics:
packets: received 292, sent 317
bytes: received 24896, sent 26912 PW: neighbor 2.2.2.2, PW ID 3, state is up ( established )
PW class FR_TO_FR, XC ID 0x7000001
Encapsulation MPLS, protocol LDP
PW type Frame Relay DLCI, control word enabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -----------------------------
 Label        16013                          28
Group ID     0x7000400                      0x0
Interface    POS0/6/0/0.100                 unknown MTU          1500                           1500

Control word enabled                        enabled
PW type      Frame Relay DLCI               Frame Relay DLCI
VCCV CV type 0x2                            0x2
             (LSP ping verification)        (LSP ping verification)
VCCV CC type 0x7                            0x7
             (control word)                 (control word)
             (router alert label)           (router alert label)
             (TTL expiry)                   (TTL expiry)
------------ ------------------------------ -----------------------------
MIB cpwVcIndex: 3
Create time: 30/03/2012 14:32:12 (00:45:58 ago)
Last time status changed: 30/03/2012 14:38:54 (00:39:16 ago)
Statistics:
  packets: received 317, sent 292
  bytes: received 26912, sent 24896
```

Without the MTU change on the PE router XR1, the Pseudowire will fail to form, and will indicate an error due to MTU mismatch. This can be seen as follows.

```
RP/0/0/CPU0:XR1#config t
Fri Mar 30 15:29:51.633 UTCRP/0/0/CPU0:XR1(config)#int pos0/6/0/0
 RP/0/0/CPU0:XR1(config-if)#no mtu
 RP/0/0/CPU0:XR1(config-if)#commit
RP/0/0/CPU0:Mar 30 15:29:57.389 : config[65753]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin'. Use 'show configuration commit changes
1000000166' to view the changes.
RP/0/0/CPU0:XR1(config-if)#end
RP/0/0/CPU0:Mar 30 15:29:57.621 : config[65753]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xradmin
R8#
%OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.20 on Serial0/0 from FULL to DOWN, Neighbor
 Down: Dead timer expired
RP/0/0/CPU0:XR1#show l2vpn xconnect detail
Fri Mar 30 15:30:30.256 UTC
 Group GROUP1, XC PORT3, state is down
; Interworking none
  AC: POS0/6/0/0.100, state is up
    Type Frame Relay DLCI; DLCI = 100
    MTU 4474; XC ID 0x7000001; interworking none
    Statistics:
      packets: received 340, sent 366
      bytes: received 29084, sent 31104
  PW: neighbor 2.2.2.2, PW ID 3, state is down ( all ready )
    PW class FR_TO_FR, XC ID 0x7000001
    Encapsulation MPLS, protocol LDP
    PW type Frame Relay DLCI, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -----------------------------
Label        16013                          28
Group ID     0x7000400                      0x0
Interface    POS0/6/0/0.100                 unknownMTU          4474                          1500
Control word enabled                        enabled
PW type      Frame Relay DLCI               Frame Relay DLCI
VCCV CV type 0x2                            0x2
(LSP ping verification)                     (LSP ping verification)
VCCV CC type 0x7                            0x7
            (control word)                  (control word)
            (router alert label)            (router alert label)
            (TTL expiry)                    (TTL expiry)
```

```
------------ ----------------------------- ----------------------------
MIB cpwVcIndex: 3
Create time: 30/03/2012 14:32:12 (00:58:18 ago)
Last time status changed: 30/03/2012 15:29:56 (00:00:34 ago) Error: MTU mismatched
```

XR1's MTU must be set to 1500 to match the other end of the Pseudowire. If XR2's MTU is the default of 4474, it won't break the basic layer 2 connectivity, but it will break the OSPF adjacency.

```
RP/0/0/CPU0:XR1#config t
Fri Mar 30 15:32:18.946 UTCRP/0/0/CPU0:XR1(config)#int pos0/6/0/0
 RP/0/0/CPU0:XR1(config-if)#mtu 1500

RP/0/0/CPU0:XR1(config-if)#commit
RP/0/0/CPU0:Mar 30 15:32:24.615 : config[65753]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin'. Use 'show configuration commit changes
1000000167' to view the changes.

RP/0/3/CPU0:XR2#config t
Fri Mar 30 15:32:10.701 UTCRP/0/3/CPU0:XR2(config)#int pos0/7/0/0
RP/0/3/CPU0:XR2(config-if)#no mtu
RP/0/3/CPU0:XR2(config-if)#commit
RP/0/3/CPU0:Mar 30 15:32:16.677 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin@admin'. Use 'show configuration commit
changes 1000000140' to view the changes.
R8#ping 10.0.0.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.20, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5),
 round-trip min/avg/max = 4/4/4 ms
R8#debug ip ospf adj
OSPF adjacency events debugging is on
R8#
OSPF: Send DBD to 20.20.20.20 on Serial0/0 seq 0x204C opt 0x52 flag 0x7 len 32
OSPF: Retransmitting DBD to 20.20.20.20 on Serial0/0 [4]
OSPF: Rcv DBD from 20.20.20.20 on Serial0/0 seq 0x71D1 opt 0x52 flag 0x7 len 32 mtu 4470
 state EXSTART OSPF: Nbr 20.20.20.20 has larger interface MTU
```

Because XR2's MTU accounts for the layer 2 header as well, a value of 1500 is too low:

```
RP/0/3/CPU0:XR2#config t
Fri Mar 30 15:34:24.217 UTCRP/0/3/CPU0:XR2(config)#int pos0/7/0/0
 RP/0/3/CPU0:XR2(config-if)#mtu 1500

RP/0/3/CPU0:XR2(config-if)#commit
RP/0/3/CPU0:Mar 30 15:34:28.790 : ospf[361]: %ROUTING-OSPF-5-ADJCHG : Process 1,
Nbr 8.8.8.8 on POS0/7/0/0.100 in area 0 from DOWN to DOWN, Neighbor Down: interface
down or detached,vrf default vrfid 0x60000000
RP/0/3/CPU0:Mar 30 15:34:30.173 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin@admin'. Use 'show configuration commit
changes 1000000141' to view the changes.
R8#debug ip ospf adj
OSPF adjacency events debugging is on
R8#
OSPF: Rcv DBD from 20.20.20.20 on Serial0/0 seq 0x2563 opt 0x52 flag 0x7 len 32 mtu 1496
 state EXCHANGE OSPF: Nbr 20.20.20.20 has smaller interface MTU

OSPF: Send DBD to 20.20.20.20 on Serial0/0 seq 0x2563 opt 0x52 flag 0x2 len 72
```

Instead, XR2’s MTU should be set to 1504 to account for the 4-byte Frame Relay header.

```
RP/0/3/CPU0:XR2#config t
Fri Mar 30 15:35:41.718 UTCRP/0/3/CPU0:XR2(config)#int pos0/7/0/0
 RP/0/3/CPU0:XR2(config-if)#mtu 1504

RP/0/3/CPU0:XR2(config-if)#commit
RP/0/3/CPU0:Mar 30 15:35:46.601 : ospf[361]: %ROUTING-OSPF-5-ADJCHG : Process 1,
Nbr 8.8.8.8 on POS0/7/0/0.100 in area 0 from DOWN to DOWN, Neighbor Down: interface
down or detached,vrf default vrfid 0x60000000
RP/0/3/CPU0:Mar 30 15:35:46.918 : ospf[361]: %ROUTING-OSPF-5-ADJCHG : Process 1,
 Nbr 8.8.8.8 on POS0/7/0/0.100 in area 0 from LOADING to FULL
, Loading Done,vrf
default vrfid 0x60000000
RP/0/3/CPU0:Mar 30 15:35:48.311 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin@admin'. Use 'show configuration commit
changes 1000000142' to view the changes.
RP/0/3/CPU0:XR2(config-if)#end
RP/0/3/CPU0:Mar 30 15:35:48.352 : config[65734]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xradmin@admin
RP/0/3/CPU0:XR2#show route ospf
Fri Mar 30 15:36:32.301 UTC
 O    8.8.8.8/32
 [110/2] via 10.0.0.8, 00:00:44, POS0/7/0/0.100
RP/0/3/CPU0:XR2#ping 8.8.8.8
```

```
Fri Mar 30 15:36:36.258 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!! Success rate is 100 percent
 (5/5), round-trip min/avg/max = 3/3/6 ms
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.24 MPLS L2 VPN with AToM – Ethernet to Frame Relay Interworking (pending update)

- Configure Frame Relay on the POS interfaces between XR1 and XR2 as follows:
  - Use an MTU of 1500 on the POS link of XR1.
  - Use an MTU of 1504 on the POS link of XR2.
  - Use a Frame Relay PVC of 100.
  - Use the subinterface .100 on XR2.
  - Enable OSPF on XR2’s Frame Relay subinterface.
- Configure R2 and XR1 for L2VPN with Any Transport over MPLS as follows:
  - The attachment circuits are the Ethernet link connecting to R1 and the POS link connecting to and XR2.
  - R2 and XR1 should form a pseudowire between their Loopback0 interfaces.
  - Enable IPv4 Interworking for this pseudowire.
- When complete, R1 and XR2 should form an OSPFv2 adjacency and have IP reachability to each other’s Looopback0 networks.

Configuration

```
R1:
interface FastEthernet0/0
 ip ospf network point-to-point

R2:
pseudowire-class ETH_TO_FR_INTERWORKING
 encapsulation mpls
 interworking ip
!
interface FastEthernet1/0
 xconnect 19.19.19.19 4 pw-class ETH_TO_FR_INTERWORKING

XR1:
interface POS0/6/0/0
 no cdp
 mtu 1500
```

```
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface POS0/6/0/0.100 l2transport
 pvc 100
 !
!
l2vpn
 pw-class ETH_TO_FR_INTERWORKING
  encapsulation mpls
  !
 !
 xconnect group GROUP1
  p2p PORT4
   interface POS0/6/0/0.100
   neighbor 2.2.2.2 pw-id 4
    pw-class ETH_TO_FR_INTERWORKING
   !
   interworking ipv4

XR2:
interface POS0/7/0/0
 no cdp
 encapsulation frame-relay
 mtu 1504
!
interface POS0/7/0/0.100 point-to-point
 ipv4 address 10.0.0.20 255.255.255.0
 pvc 100
```

Verification

One of the key features of Any Transport over MPLS is that it supports any-to-any connectivity of Attachment Circuits. This means that one end of the customer link can be running Ethernet, while the other end can be running Frame Relay, ATM, PPP, etc. In this example, the Attachment Circuit to R1 is Ethernet, whereas the Attachment Circuit to XR2 is Frame Relay. Because the protocols must be translated between the two endpoints, only IPv4 payloads are supported. Other non-IP or IPv6 payloads will not able to transit over the circuit without an additional encapsulation like GRE.

Like in the previous examples, a few of the caveats of this configuration are the MTU mismatch between the Attachment Circuits (Ethernet with 1500 bytes and

POS with 4474) and the OSPF network type mismatch (Broadcast on R1 and Point-to-Point on XR2). The only other configuration change compared with the other examples, though, is the addition of the `interworking` command under the Pseudowire Class in regular IOS and the `interworking ipv4` under the xconnect group's port of IOS XR. When complete, final verification should be the end-to-end connectivity between the customer routers.

```
R1#show ip route ospf
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    20.0.0.0/32 is subnetted, 1 subnets
O      20.20.20.20 [110/2] via 10.0.0.20, 00:11:08, FastEthernet0/0
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!Success rate is 100 percent
 (5/5), round-trip min/avg/max = 1/2/4 ms
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Fri Mar 30 15:55:40.838 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

1   10.0.0.1 5 msec *   2 msec
```

Again, note that the customer routers think that they are directly connected.

The Pseudowire verification is the same as previous AToM tasks, as seen below.

```
R2#show mpls l2transport vc detail
Local interface: Fa1/0 up, line protocol up, Ethernet up
  Interworking type is IP
```

```
   Destination address: 19.19.19.19, VC ID: 4, VC status: up
     Output interface: Fa0/0.23, imposed label stack {26 16012}

     Preferred path: not configured
     Default path: active
     Next hop: 20.2.3.3
   Create time: 00:13:10, last status change time: 00:13:05
   Signaling protocol: LDP, peer 19.19.19.19:0 up
Targeted Hello: 2.2.2.2(LDP Id) -> 19.19.19.19, LDP is UP
     Status TLV support (local/remote)   : enabled/not supported
      LDP route watch                   : enabled
      Label/status state machine       : established, LruRru
      Last local dataplane status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local LDP TLV status sent: No fault
      Last remote LDP TLV status rcvd: Not sent
      Last remote LDP ADJ   status rcvd: No fault
   MPLS VC labels: local 28, remote 16012
   Group ID: local 0, remote 117441536 MTU: local 1500, remote 1500
   Remote interface description: POS0_6_0_0.100
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
VC statistics:
  transit packet totals: receive 106, send 138
  transit byte totals:  receive 8718, send 14454
  transit packet drops: receive 30, seq error 0, send 1


RP/0/0/CPU0:XR1#show l2vpn xconnect detail
Fri Mar 30 15:56:56.806 UTC
Group GROUP1, XC PORT4, state is up; Interworking IPv4
 AC: POS0/6/0/0.100, state is up
   Type Frame Relay DLCI; DLCI = 100
   MTU 1500; XC ID 0x7000001; interworking IPv4
   Statistics:
     packets: received 140, sent 141
     bytes: received 11200, sent 11016 PW: neighbor 2.2.2.2, PW ID 4, state is up ( established )
   PW class ETH_TO_FR_INTERWORKING, XC ID 0x7000001
   Encapsulation MPLS, protocol LDP   PW type IP, control word enabled, interworking IPv4

   PW backup disable delay 0 sec
   Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -----------------------------
Label       16012                            28
```

```
Group ID     0x7000400                     0x0
Interface    POS0/6/0/0.100                unknown MTU          1500                           1500
Control word enabled                       enabled PW type      IP                             IP

VCCV CV type 0x2                           0x2
            (LSP ping verification)        (LSP ping verification)
VCCV CC type 0x7                           0x7
            (control word)                 (control word)
            (router alert label)           (router alert label)
            (TTL expiry)                   (TTL expiry)
------------ ----------------------------- -----------------------------
MIB cpwVcIndex: 4
Create time: 30/03/2012 15:43:09 (00:13:46 ago)
Last time status changed: 30/03/2012 15:43:41 (00:13:14 ago)
Statistics:
   packets: received 141, sent 140
   bytes: received 11016, sent 11200
```

The only major difference from the above output and the previous examples is that the Pseudowire Type is IP only, because Interworking for IPv4 is on.

Again, this means that non IP protocols, such as IPv6, are not supported over the layer 2 circuit, as seen below.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.R1(config)#int f0/0
R1(config-if)#ipv6 address 2001:10::1/64
R1(config-if)#end
R1#

RP/0/3/CPU0:XR2#config t
Fri Mar 30 16:02:27.082 UTCRP/0/3/CPU0:XR2(config)#int pos0/7/0/0.100
 RP/0/3/CPU0:XR2(config-subif)#ipv6 address 2001:10::20/64
 RP/0/3/CPU0:XR2(config-subif)#commit
RP/0/3/CPU0:Mar 30 16:02:34.746 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin@admin'. Use 'show configuration commit
changes 1000000144' to view the changes.
R1#ping 2001:10::20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::20, timeout is 2 seconds:
..... Success rate is 0 percent (0/5)
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 4: VPN v4

4.25 VPLS (pending update)

- The network is preconfigured as follows:
  - R1 and R3 are in the subnet 10.1.3.0/24, and are connected to access ports in VLAN 13.
  - R2 and R4 are in the subnet 10.2.4.0/24, and are connected to access ports in VLAN 24.
  - SW1’s uplink to XR1 and SW2’s uplink to XR2 are configured at 802.1q trunk links.
  - OSPF is enabled on all interfaces of R1, R2, R3, and R4.
  - The POS link between XR1 and XR2 is OSPF and LDP enabled to form an LSP between their Loopback0 networks.
- Configure VPLS as follows on XR1 and XR2 to bridge the VLAN 13 and 24 segments together:
  - Using the interface numbering in the diagram, configure Ethernet subinterfaces 13 and 24 on XR1 and XR2 for l2transport of VLANs 13 and 24, respectively.
  - Configure a Pseudowire Class named VPLS_CLASS with MPLS encapsulation and an Ethernet transport mode
  - Configure a Bridge Group named VPLS with bridge domains 13 and 24.
  - Bridge domain 13 should have the Attachment Circuit of the VLAN 13 subinterface, use Virtual Forwarding Interface 13, and form a Pseudowire between the Loopbacks of XR1 and XR2 with an ID of 13 and the VPLS_CLASS.
  - Bridge domain 24 should have the Attachment Circuit of the VLAN 24 subinterface, use Virtual Forwarding Interface 24, and form a Pseudowire between the Loopbacks of XR1 and XR2 with an ID of 24 and the VPLS_CLASS.
- When complete, the following reachability should be achieved:
  - R1 and R3 should form OSPF adjacencies and have reachability to each other’s Loopback networks.
  - R2 and R4 should form OSPF adjacencies and have reachability to each

other’s Loopback networks.

Configuration

```
XR1:
interface GigabitEthernet0/1/0/0.13 l2transport
 dot1q vlan 13
!
interface GigabitEthernet0/1/0/0.24 l2transport
 dot1q vlan 24
!
l2vpn
 pw-class VPLS_CLASS
  encapsulation mpls
   transport-mode ethernet
!
bridge group VPLS
 bridge-domain 13
  interface GigabitEthernet0/1/0/0.13
  !
  vfi 13
   neighbor 20.20.20.20 pw-id 13
    pw-class VPLS_CLASS
!
bridge-domain 24
 interface GigabitEthernet0/1/0/0.24
 !
 vfi 24
  neighbor 20.20.20.20 pw-id 24
   pw-class VPLS_CLASS

XR2:
interface GigabitEthernet0/4/0/1.13 l2transport
  dot1q vlan 13
!
interface GigabitEthernet0/4/0/1.24 l2transport
dot1q vlan 24
!
l2vpn
 pw-class VPLS_CLASS
  encapsulation mpls
!
bridge group VPLS
 bridge-domain 13
```

```
  interface GigabitEthernet0/4/0/1.13
  !
  vfi 13
   neighbor 19.19.19.19 pw-id 13
    pw-class VPLS_CLASS
!
bridge-domain 24
 interface GigabitEthernet0/4/0/1.24
 !
 vfi 24
  neighbor 19.19.19.19 pw-id 24
   pw-class VPLS_CLASS
```

Verification

Virtual Private LAN Services (VPLS) is similar to Any Transport over MPLS (AToM) L2VPN, with the exception that VPLS emulates a multipoint topology, whereas AToM only emulates point-to-point topologies. In this example, because there are only two PE routers, the topology is effectively point-to-point, but in normal VPLS designs, there would be three or more PEs that participate in the same bridge domain.

The vast majority of VPLS-related verifications fall under the major command `show l2vpn bridge-domain` , with the below `brief` and `summary` arguments giving a quick overview of the status of Attachment Circuits and Pseudowires. This output shows us that there are two bridge domains, each with one Attachment Circuit and one Pseudowire apiece. Again, in normal VPLS designs there would be more Pseudowires because there would be more than two PE routers.

```
RP/0/0/CPU0:XR1#show l2vpn bridge-domain brief
Fri Mar 30 17:40:49.624 UTC
Bridge Group/Bridge-Domain Name  ID    State      Num ACs/up     Num PWs/up
-------------------------------- ----- ---------- -------------- --------------
VPLS/13                            1     up         1/1            1/1
VPLS/24                            2     up         1/1            1/1
RP/0/0/CPU0:XR1#show l2vpn bridge-domain summary
Fri Mar 30 17:40:53.326 UTC
Number of groups: 1, bridge-domains: 2, Up: 2, Shutdown: 0
Default: 2, pbb-edge: 0, pbb-core: 0 Number of ACs: 2 Up: 2
, Down: 0 Number of PWs: 2 Up: 2
, Down: 0
```

The below command `show l2vpn bridge-domain detail` shows all the specific options for the bridge groups, their ACs and PWs, such as whether MAC Address learning and flooding is enabled, the number of MAC addresses that can be in the bridge group's table, the MTU, the MPLS Labels, the signaling details of the PWs, etc.

```
RP/0/0/CPU0:XR1#show l2vpn bridge-domain detail
Fri Mar 30 17:43:09.970 UTCBridge group: VPLS, bridge-domain: 13, id: 1, state: up, ShgId: 0, MSTi: 0
   MAC learning: enabled
   MAC withdraw: enabled
   Flooding:
     Broadcast & Multicast: enabled
     Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
Security: disabled
Split Horizon Group: none
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 2
Filter MAC addresses:
Create time: 30/03/2012 17:23:17 (00:19:53 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
List of ACs: AC: GigabitEthernet0/1/0/0.13, state is up
    Type VLAN; Num Ranges: 1  VLAN ranges: [13, 13]
    MTU 1500; XC ID 0x2000002; interworking none
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 4000, Action: none, Notification: syslog
    MAC limit reached: no
    MAC port down flush: enabled
    Security: disabled
    Split Horizon Group: none
    DHCPv4 snooping: disabled
    IGMP Snooping profile: none
    Storm Control: disabled
    Static MAC addresses:
    Statistics:
      packets: received 135, sent 704
      bytes: received 13192, sent 51854
    Storm control drop counters:
```

```
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
List of Access PWs:
List of VFIs: VFI 13
PW: neighbor 20.20.20.20, PW ID 13, state is up ( established )
      PW class VPLS_CLASS, XC ID 0xff000002
      Encapsulation MPLS, protocol LDP
      PW type Ethernet, control word disabled, interworking none
      PW backup disable delay 0 sec
      Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -------------------------
Label        16000                         16003
Group ID     0x1                            0x1
Interface    13                             13 MTU          1500                          1500
Control word disabled                       disabled PW type      Ethernet                      Ethernet
VCCV CV type 0x2                            0x2
             (LSP ping verification)        (LSP ping verification)
VCCV CC type 0x6                            0x6
             (router alert label)           (router alert label)
             (TTL expiry)                   (TTL expiry)
------------ ------------------------------ -------------------------
  MIB cpwVcIndex: 7
  Create time: 30/03/2012 17:23:17 (00:19:53 ago)

  Last time status changed: 30/03/2012 17:23:40 (00:19:30 ago)
  MAC withdraw message: send 0 receive 0
  Static MAC addresses: Statistics:
     packets: received 712, sent 135
     bytes: received 52428, sent 13192
  IGMP Snooping profile: none
  VFI Statistics:
    drops: illegal VLAN 0, illegal length 0Bridge group: VPLS, bridge-domain: 24, id: 2, state: up
, ShgId: 0, MSTi: 0
 MAC learning: enabled
 MAC withdraw: enabled
   Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: no
 MAC port down flush: enabled
 Security: disabled
 Split Horizon Group: none
```

```
 DHCPv4 snooping: disabled
 IGMP Snooping profile: none
 Bridge MTU: 1500
 MIB cvplsConfigIndex: 3
 Filter MAC addresses:
 Create time: 30/03/2012 17:23:17 (00:19:53 ago)
 No status change since creation
 ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
 List of ACs: AC: GigabitEthernet0/1/0/0.24, state is up
   Type VLAN; Num Ranges: 1 VLAN ranges: [24, 24]
   MTU 1500; XC ID 0x2000003; interworking none MAC learning: enabled
   Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
 MAC aging time: 300 s, Type: inactivity
 MAC limit: 4000, Action: none, Notification: syslog
 MAC limit reached: no
 MAC port down flush: enabled
Security: disabled
Split Horizon Group: none
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 136, sent 704
bytes: received 13290, sent 51854
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0 List of Access PWs:
List of VFIs:
VFI 24 PW: neighbor 20.20.20.20, PW ID 24, state is up ( established )

  PW class VPLS_CLASS, XC ID 0xff000003
  Encapsulation MPLS, protocol LDP
  PW type Ethernet, control word disabled, interworking none
  PW backup disable delay 0 sec
  Sequencing not set

MPLS         Local                          Remote
------------ ------------------------------ -------------------------
Label        16001                          16004
Group ID     0x2                            0x2
Interface    24                             24 MTU          1500                          1500

Control word disabled                       disabled
```

```
PW type      Ethernet                       Ethernet
VCCV CV type 0x2                            0x2
             (LSP ping verification)        (LSP ping verification)
VCCV CC type 0x6                            0x6
             (router alert label)           (router alert label)
             (TTL expiry)                   (TTL expiry)
------------ ------------------------------ -------------------------
MIB cpwVcIndex: 8
Create time: 30/03/2012 17:23:17 (00:19:56 ago)
Last time status changed: 30/03/2012 17:23:40 (00:19:33 ago) MAC withdraw message: send 0 receive 0
Static MAC addresses: Statistics:
   packets: received 713, sent 135
   bytes: received 52526, sent 13192
IGMP Snooping profile: none
VFI Statistics:
   drops: illegal VLAN 0, illegal length 0
```

Because VPLS is a multipoint layer 2 tunneling technology, the Service Provider Edge devices must participate in MAC address learning, flooding, and loop prevention with the customer, similar to how Spanning-Tree Protocol works. To verify the actual traffic that the customer is forwarding, as well as the MAC address table for the VPLS bridge group, use the `show l2vpn forwarding` subcommands, such as the one listed below.

```
RP/0/0/CPU0:XR1#show l2vpn forwarding bridge-domain mac-address location 0/1/CPU0
Fri Mar 30 17:50:23.801 UTC
Mac Address     Type    Learned from/Filtered on    LC learned  Age
Mapped to
--------------------------------------------------------------------------------0005.5fad.3800
 dynamic  Gi0/1/0/0.13                0/1/CPU0    0d 0h 0m 30s
N/A 000c.3001.b21a
 dynamic  (20.20.20.20, 13)           0/1/CPU0    0d 0h 0m 22s
N/A 0014.a88c.961c
 dynamic  (20.20.20.20, 13)           0/1/CPU0    0d 0h 0m 24s
N/A 000c.3001.b21a
 dynamic (20.20.20.20, 24)            0/1/CPU0    0d 0h 0m 16s
N/A 000c.86ba.081c
 dynamic (20.20.20.20, 24)            0/1/CPU0    0d 0h 2m 28s
N/A 0012.4318.cb00
 dynamic  Gi0/1/0/0.24                0/1/CPU0    0d 0h 2m 40s
N/A
```

The “location 0/1/CPU0” in the above output refers to the linecard that has the

Attachment Circuit to the customer. Specifically in this case, it is the interface Gig0/1/0/0 and its subinterfaces. Here we see three different MAC addresses per bridge-group, which can be correlated against the ARP cache or CAM tables of the customer devices.

Specifically, four of them are the interface MAC addresses of the routers R1, R2, R3, and R4, and the other is a MAC address that belongs to the customer switch SW2.

```
R1#show arp
Protocol    Address     Age (min)   Hardware Addr   Type    Interface
Internet    10.1.3.1        - 0005.5fad.3800
  ARPA    FastEthernet0/0 Internet    10.1.3.3        52 0014.a88c.961c
  ARPA    FastEthernet0/0
R2#show arp
Protocol    Address     Age (min)   Hardware Addr   Type    Interface
Internet    10.2.4.2        - 0012.4318.cb00
  ARPA    FastEthernet0/0 Internet    10.2.4.4        54 000c.86ba.081c
  ARPA    FastEthernet0/0
SW2#show mac address-table address 000c.3001.b21a
            Mac Address Table
-------------------------------------------


Vlan    Mac Address       Type      Ports
----    -----------       --------  -----All 000c.3001.b21a
    STATIC     CPU
Total Mac Addresses for this criterion: 1
```

The end result of this design is similar to AToM, where the customers appear directly attached to each other, but the difference is that VPLS can be a multipoint tunnel, where AToM cannot. Additionally, AToM supports different types of Attachment Circuits like Ethernet, ATM, Frame Relay, PPP, and HDLC, whereas VPLS supports just Ethernet.

```
R1#show ip ospf neighbor

Neighbor ID Pri State   Dead Time   Address     Interface
3.3.3.3     1   FULL/DR 00:00:34    10.1.3.3    FastEthernet0/0
R1#show ip route ospf
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.1.3.3, 00:36:23, FastEthernet0/0
R1#traceroute 3.3.3.3


Type escape sequence to abort.
Tracing the route to 3.3.3.3

    1 10.1.3.3 0 msec * 0 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.1 MPLS Traffic Engineering with OSPF (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively. However, the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the OSPF area 0 core.
  - Set the OSPF MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running OSPF in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2’s Loopback0 interface.
  - Set the tunnel destination as XR1’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the OSPF core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1’s Loopback0 interface.
  - Set the tunnel destination as R2’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the OSPF core can use it for dynamic routing.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 dynamic
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
  ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 dynamic
!
router ospf 1
 area 0
  mpls traffic-eng
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

This example essentially shows the minimum configuration needed to build two basic MPLS TE tunnels between the PE routers of the Service Provider's network.

Additionally in this case, the TE tunnels replace the need for Label Distribution Protocol (LDP) in the SP core. Instead of automatically allocating a label value for each route advertised via IGP, MPLS TE only allocates labels for destinations that have a TE tunnel built toward them. This is why two tunnels are needed in this example; the first tunnel is unidirectional from R2 to XR1, which allocates the transport label to get to XR1, and the second tunnel is unidirectional from XR1 back to R2, which allocates the transport label to get to R2.

Note an important caveat of IOS XR here: Even though LDP is not used for label distribution, the command `mpls ldp` must be entered globally to allow the forwarding of MPLS-labeled packets. Without this, the MPLS TE tunnels will form and labels will be allocated for the tunnel endpoints, but the end customer traffic will not actually be able to use the tunnels. This is a rather obscure problem, though, because typically the SP core network would be running LDP already to service L3VPN or L2VPN customers, and then run MPLS TE on top of this. It only becomes a problem in this example because LDP is not already running in the SP core.

The final verification of this task is to check whether the customer sites have reachability to each other. The end result is just like a normal MPLS L3VPN. The customer sites see no difference between the transport labels being allocated via MPLS TE vs. being allocated via LDP.

```
R1#traceroute 20.20.20.20 source lo0

 Type escape sequence to abort.
 Tracing the route to 20.20.20.20

   1 10.1.2.2 0 msec 0 msec 0 msec 2 20.2.4.4 [MPLS: Labels 16/16015 Exp 0] 4 msec 0 msec 4 msec
 3 20.4.5.5 [MPLS: Labels 16/16015 Exp 0] 0 msec 4 msec 0 msec
   4 20.5.19.19 8 msec 12 msec 8 msec
   5 10.19.20.20 16 msec *   12 msec
 RP/0/3/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
 Tue Apr 3 21:40:07.078 UTC

 Type escape sequence to abort.
 Tracing the route to 1.1.1.1

   1 10.19.20.19 15 msec 11 msec 10 msec 2 20.6.19.6 [MPLS: Labels 16/16 Exp 5] 10 msec  11 msec 9 msec
 3 20.3.6.3  [MPLS: Labels 16/16 Exp 5] 10 msec  11 msec 9 msec
     4 10.1.2.2  [MPLS: Label 16 Exp 6] 10 msec  10 msec 10 msec

   5 10.1.2.1 10 msec  *  9 msec
```

In the above output, we see that a two-label stack is used in the core for forwarding the L3VPN customer's traffic. From R1 to XR2, the bottom label 16015 is the VPN label that was allocated by the VPNv4 process of R2 and XR1, whereas the top labels 16 are the transport labels that were allocated by RSVP for the MPLS TE tunnel. Likewise, on the way back from XR2 to R1, the bottom label is the VPNv4 BGP-derived label, whereas the top label is the MPLS TE label.

The details of the MPLS TE tunnels can be verified on both the head end and the tail end, as seen below.

```
R2#show mpls traffic-eng tunnels detail

P2P TUNNELS/LSPs:
Name: R2_t0                              (Tunnel0) Destination: 19.19.19.19

  Status: Admin: up          Oper: up      Path: valid        Signalling: connected

    path option 10, type dynamic (Basis for Setup, path weight 3)

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled LockDown: disabled Loadshare: 0         bw-based
    auto-bw: disabled
  Active Path Option Parameters: State: dynamic path option 10 is active
    BandwidthOverride: disabled LockDown: disabled  Verbatim: disabled


InLabel : - OutLabel : FastEthernet0/0.24, 16
Next Hop : 20.2.4.4
RSVP Signalling Info:
     Src 2.2.2.2, Dst 19.19.19.19, Tun Id 0, Tun Instance 1
  RSVP Path Info:
    My Address: 20.2.4.2 Explicit Route: 20.2.4.4 20.4.5.4 20.4.5.5 20.5.19.5
20.5.19.19 19.19.19.19
    Record   Route:   NONE
    Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record   Route:   NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
History:
  Tunnel:
    Time since created: 21 minutes, 59 seconds
    Time since path change: 21 minutes, 58 seconds
    Number of LSP IDs (Tun Instances) used: 1
  Current LSP: [ID: 1]
    Uptime: 21 minutes, 58 seconds
```

```
LSP Tunnel XR1_t0 is signalled, connection is up
   InLabel  : FastEthernet0/0.23, implicit-null

  Prev Hop : 20.2.3.3



OutLabel :  -
RSVP Signalling Info: Src 19.19.19.19, Dst 2.2.2.2
, Tun Id 0, Tun Instance 2
  RSVP Path Info:
    My Address: 2.2.2.2
    Explicit Route:  NONE
    Record   Route:  NONE
    Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record  Route:  NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

P2MP TUNNELS:

P2MP SUB-LSPS:
```

In the above output, R2 sees that two separate TE tunnels are terminating on it. The first is the local tunnel to XR1; R2 is the head end (the originator) of the tunnel. The second is the remote tunnel from XR1; R2 is the tail end (the destination).

The important aspects of the above output are that the tunnel is up, that the path is valid, and that signaling is connected. This means that whichever path option was chosen (such as dynamic, explicit, or verbatim) was acceptable, and that RSVP was able to send the PATH messages and get the RESV message responses to actually build the tunnel. Additionally, we see the label value that R2 uses for the top of the stack for traffic routed out the tunnel, and the resulting path that the dynamic path option computed.

For the second tunnel output, we can tell that R2 is the tail because the label value is implicit NULL, and the destination is the local address 2.2.2.2.

Note that neither of these tunnels has asked for additional path requirements such as bandwidth values, affinity bits, fast reroute protection, etc. All of these features are optional parameters of the tunnels and are not required for the most basic design.

Likewise, in the below output we see that XR1 is the head end for a tunnel going to R2, and the tail end for a tunnel coming from R2.

```
RP/0/0/CPU0:XR1#show mpls traffic-eng tunnels detail

Tue Apr  3 21:51:29.921 UTC
Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 2155 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 55 seconds
          Auto-bw enabled tunnels:  0 (disabled)
Name: tunnel-te0 Destination: 2.2.2.2

  Status: Admin:    up Oper:  up   Path:  valid    Signalling: connected
path option 1,  type dynamic
 (Basis for Setup, path weight 3)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps CT0

Config Parameters:
  Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
  Metric Type: TE (default)
  AutoRoute:  enabled  LockDown: disabled   Policy class: not set
  Forwarding-Adjacency: disabled
  Loadshare:          0 equal loadshares
  Auto-bw: disabled
  Fast Reroute: Disabled, Protection Desired: None
  Path Protection: Not Enabled
History:
  Tunnel has been up for: 00:28:39 (since Tue Apr 03 21:22:51 UTC 2012)
  Current LSP:
    Uptime: 00:28:39 (since Tue Apr 03 21:22:51 UTC 2012)
  Reopt. LSP:
    Last Failure:
      LSP not signalled, identical to the [CURRENT] LSP
      Date/Time: Tue Apr 03 21:27:26 UTC 2012 [00:24:04 ago]
Current LSP Info:
  Instance: 2, Signaling Area: OSPF 1 area 0
  Uptime: 00:28:39 (since Tue Apr 03 21:22:51 UTC 2012)
Outgoing Interface: GigabitEthernet0/1/0/0.619, Outgoing Label: 16
  Router-IDs: local      19.19.19.19
            downstream 6.6.6.6 Path Info:
    Outgoing:
    Explicit Route: Strict, 20.6.19.6
Strict, 20.3.6.6
Strict, 20.3.6.3
```

```
 Strict, 20.2.3.3
  Strict, 20.2.3.2
 Strict, 2.2.2.2
     Record Route: Disabled
     Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

     Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
   Resv Info: None
     Record Route: Disabled
     Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
 LSP Tunnel 2.2.2.2 0 [1] is signalled, connection is up
    Tunnel Name: R2 t0 Tunnel Role: Tail
   InLabel: GigabitEthernet0/1/0/0.519, implicit-null

   Signalling Info:    Src 2.2.2.2 Dst 19.19.19.19
, Tun ID 0, Tun Inst 1, Ext ID 2.2.2.2
     Router-IDs: upstream   5.5.5.5
                 local      19.19.19.19
     Bandwidth: 0 kbps (CT0) Priority:  7  7 DSTE-class: 0
     Path Info:
       Incoming:
       Explicit Route:
         Strict, 20.5.19.19
         Strict, 19.19.19.19
       Record Route: Disabled
       Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
       Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
     Resv Info: None
       Record Route: Disabled
       Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
 Displayed 1 (of 1) heads, 0 (of 0) midpoints, 1 (of 1) tails
 Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Again, the important information that `show mpls traffic-eng tunnels detail` gives us is that the tunnel is up, the path calculation is valid, and RSVP successfully made the reservation and label allocation. Here we see that the label value 16 was allocated, and the next-hop of the tunnel is R6. The path information shows the specific end-to-end path of the tunnel, which in this case is XR1 to R6 to R3 to R2.

For the second tunnel, XR1 knows that it is the tail (destination) of the tunnel, and is advertising label value implicit null, because the destination is connected.

Devices in the core of the network, or what is considered the midpoints of the tunnel, should also know about the end-to-end signaling, as seen below.

```
R3#show mpls traffic-eng tunnels detail



P2P TUNNELS/LSPs:


LSP Tunnel XR1 t0 is signalled, connection is up
  InLabel   : FastEthernet0/0.36, 16
  Prev Hop : 20.3.6.6
  OutLabel : FastEthernet0/0.23, implicit-null
  Next Hop : 20.2.3.2
  RSVP Signalling Info:
       Src 19.19.19.19, Dst 2.2.2.2, Tun Id 0, Tun Instance 2
    RSVP Path Info:
      My Address: 20.2.3.3
      Explicit Route: 20.2.3.2 2.2.2.2
      Record   Route:   NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits


P2MP TUNNELS:


P2MP SUB-LSPS:
R4#show mpls traffic-eng tunnels detail


P2P TUNNELS/LSPs:
 LSP Tunnel R2 t0 is signalled, connection is up
  InLabel : FastEthernet0/0.24, 16
  Prev Hop : 20.2.4.2 OutLabel : FastEthernet0/0.45, 16
  Next Hop : 20.4.5.5
  RSVP Signalling Info: Src 2.2.2.2, Dst 19.19.19.19
, Tun Id 0, Tun Instance 1
    RSVP Path Info:
      My Address: 20.4.5.4
      Explicit Route: 20.4.5.5 20.5.19.5 20.5.19.19 19.19.19.19
      Record   Route:   NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits


P2MP TUNNELS:
```

```
P2MP SUB-LSPS:
```

The above output tells us that R3 is a midpoint for a tunnel that is coming from XR1 and going to R2. R3 is the penultimate (next to last) hop for the tunnel, because the outgoing label is implicit null. Likewise, R4 is a midpoint for the tunnel coming from R2 and going to XR1. Just like in the previous L3VPN and L2VPN examples we saw, the core of the SP network does not care what kind of traffic transits over the tunnel. It only cares about moving traffic from the tunnel head end to the tail end. As long as the LSP for the transport label is end to end (that is, the TE tunnel is up), it doesn't need to know about the final end customer traffic.

Another key requirement of establishing the MPLS TE tunnels is that the core of the network agrees on the traffic engineering topology. In this example, the TE topology is calculated based on the OSPF topology, but additional attributes such as the TE metrics, available link bandwidth, reservable link bandwidth, etc. make up what is considered the Constrained topology. These additional attributes are they used to run the Constrained Shortest Path First (CSPF) calculation, to result in the Constrained Shortest Path Tree (CSPT). The idea behind this calculation is that whereas OSPF normally just takes link costs into account when making a routing decision, with MPLS TE you might also want to consider other attributes, such as the amount of already reserved bandwidth on a link.

The below output of `show mpls traffic-eng topology` is similar to what `show ip ospf database` or `show isis database detail` would convey, but it also shows the additional attributes for the CSPF calculation. The IGP IDs are the nodes in the MPLS TE topology graph, similar to what the OSPF Type 1 Router LSA is used to advertise.

```
R3#show mpls traffic-eng topology
My_System_id: 3.3.3.3 (ospf 1   area 0)

Signalling error holddown: 10 sec Global Link Generation 31
 IGP Id: 2.2.2.2, MPLS TE Id:2.2.2.2 Router Node (ospf 1 area 0)

      link[0]: Broadcast, DR: 20.2.4.4, nbr_node_id:3, gen:31
          frag_id 10, Intf Address:20.2.4.2
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0          75000            0
```

```
          bw[1]:              0           75000             0
          bw[2]:              0           75000             0
          bw[3]:              0           75000             0
          bw[4]:              0           75000             0
          bw[5]:              0           75000             0
          bw[6]:              0           75000             0
          bw[7]:              0           75000             0

  link[1]: Broadcast, DR: 20.2.3.3, nbr_node_id:2, gen:31
      frag_id 9, Intf Address:20.2.3.2
      TE metric:1, IGP metric:1, attribute flags:0x0
      SRLGs: None
      physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
      max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
          bw[0]:              0           75000             0
          bw[1]:              0           75000             0
          bw[2]:              0           75000             0
          bw[3]:              0           75000             0
          bw[4]:              0           75000             0
          bw[5]:              0           75000             0
          bw[6]:              0           75000             0
          bw[7]:              0           75000             0


  IGP Id: 3.3.3.3, MPLS TE Id:3.3.3.3 Router Node (ospf 1 area 0)

        link[0]: Broadcast, DR: 20.2.3.3, nbr_node_id:2, gen:16
            frag_id 5, Intf Address:20.2.3.3
            TE metric:1, IGP metric:1, attribute flags:0x0
            SRLGs: None
            physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
            max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
          bw[0]:              0           75000             0
          bw[1]:              0           75000             0
          bw[2]:              0           75000             0
          bw[3]:              0           75000             0
```

```
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0


link[1]: Broadcast, DR: 20.3.4.4, nbr_node_id:4, gen:16
    frag_id 6, Intf Address:20.3.4.3
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:              0           75000             0
        bw[1]:              0           75000             0
        bw[2]:              0           75000             0
        bw[3]:              0           75000             0
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0


link[2]: Broadcast, DR: 20.3.6.6, nbr_node_id:5, gen:16
    frag_id 7, Intf Address:20.3.6.3
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:              0           75000             0
        bw[1]:              0           75000             0
        bw[2]:              0           75000             0
        bw[3]:              0           75000             0
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0
```

```
IGP Id: 4.4.4.4, MPLS TE Id:4.4.4.4 Router Node (ospf 1 area 0)

      link[0]: Broadcast, DR: 20.4.6.6, nbr_node_id:7, gen:20
          frag_id 8, Intf Address:20.4.6.4
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None
          physical bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0           75000            0
        bw[1]:            0           75000            0
        bw[2]:            0           75000            0
        bw[3]:            0           75000            0
        bw[4]:            0           75000            0
        bw[5]:            0           75000            0
        bw[6]:            0           75000            0
        bw[7]:            0           75000            0

link[1]: Broadcast, DR: 20.4.5.5, nbr_node_id:6, gen:20
    frag_id 7, Intf Address:20.4.5.4
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0           75000            0
        bw[1]:            0           75000            0
        bw[2]:            0           75000            0
        bw[3]:            0           75000            0
        bw[4]:            0           75000            0
        bw[5]:            0           75000            0
        bw[6]:            0           75000            0
        bw[7]:            0           75000            0

link[2]: Broadcast, DR: 20.3.4.4, nbr_node id:4, gen:20
    frag_id 6, Intf Address:20.3.4.4
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
```

```
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0           75000              0
        bw[1]:            0           75000              0
        bw[2]:            0           75000              0
        bw[3]:            0           75000              0
        bw[4]:            0           75000              0
        bw[5]:            0           75000              0
        bw[6]:            0           75000              0
        bw[7]:            0           75000              0

link[3]: Broadcast, DR: 20.2.4.4, nbr_node_id:3, gen:20
    frag_id 5, Intf Address:20.2.4.4
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0           75000              0
        bw[1]:            0           75000              0
        bw[2]:            0           75000              0
        bw[3]:            0           75000              0
        bw[4]:            0           75000              0
        bw[5]:            0           75000              0
        bw[6]:            0           75000              0
        bw[7]:            0           75000              0
IGP Id: 5.5.5.5, MPLS TE Id:5.5.5.5 Router Node (ospf 1 area 0)

      link[0]: Broadcast, DR: 20.5.19.5, nbr_node_id:9, gen:23
          frag_id 7, Intf Address:20.5.19.5
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
```

```
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0          75000            0
        bw[1]:            0          75000            0
        bw[2]:            0          75000            0
        bw[3]:            0          75000            0
        bw[4]:            0          75000            0
        bw[5]:            0          75000            0
        bw[6]:            0          75000            0
        bw[7]:            0          75000            0

link[1]: Broadcast, DR: 20.4.5.5, nbr_node_id:6, gen:23
    frag_id 5, Intf Address:20.4.5.5
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0          75000            0
        bw[1]:            0          75000            0
        bw[2]:            0          75000            0
        bw[3]:            0          75000            0
        bw[4]:            0          75000            0
        bw[5]:            0          75000            0
        bw[6]:            0          75000            0
        bw[7]:            0          75000            0

link[2]: Broadcast, DR: 20.5.6.6, nbr_node_id:8, gen:23
    frag_id 6, Intf Address:20.5.6.5
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                                 Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:            0          75000            0
        bw[1]:            0          75000            0
        bw[2]:            0          75000            0
        bw[3]:            0          75000            0
```

```
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0
 IGP Id: 6.6.6.6, MPLS TE Id:6.6.6.6 Router Node (ospf 1 area 0)

      link[0]: Broadcast, DR: 20.6.19.6, nbr_node_id:10, gen:27
          frag_id 8, Intf Address:20.6.19.6
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable bw global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:              0           75000             0
        bw[1]:              0           75000             0
        bw[2]:              0           75000             0
        bw[3]:              0           75000             0
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0

      link[1]: Broadcast, DR: 20.5.6.6, nbr_node_id:8, gen:27
          frag_id 7, Intf Address:20.5.6.6
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                Global Pool    Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:              0           75000             0
        bw[1]:              0           75000             0
        bw[2]:              0           75000             0
        bw[3]:              0           75000             0
        bw[4]:              0           75000             0
        bw[5]:              0           75000             0
        bw[6]:              0           75000             0
        bw[7]:              0           75000             0
```

```
link[2]: Broadcast, DR: 20.4.6.6, nbr_node_id:7, gen:27
    frag_id 6, Intf Address:20.4.6.6
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                           Global Pool    Sub Pool
          Total Allocated  Reservable     Reservable
          BW (kbps)        BW (kbps)      BW (kbps)
          ---------------  -----------    ----------
  bw[0]:            0           75000            0
  bw[1]:            0           75000            0
  bw[2]:            0           75000            0
  bw[3]:            0           75000            0
  bw[4]:            0           75000            0
  bw[5]:            0           75000            0
  bw[6]:            0           75000            0
  bw[7]:            0           75000            0

link[3]: Broadcast, DR: 20.3.6.6, nbr_node_id:5, gen:27
    frag id 5, Intf Address:20.3.6.6
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

                           Global Pool    Sub Pool
          Total Allocated  Reservable     Reservable
          BW (kbps)        BW (kbps)      BW (kbps)
          ---------------  -----------    ----------
  bw[0]:            0           75000            0
  bw[1]:            0           75000            0
  bw[2]:            0           75000            0
  bw[3]:            0           75000            0
  bw[4]:            0           75000            0
  bw[5]:            0           75000            0
  bw[6]:            0           75000            0
  bw[7]:            0           75000            0
IGP Id: 19.19.19.19, MPLS TE Id:19.19.19.19 Router Node (ospf 1 area 0)

link[0]: Broadcast, DR: 20.5.19.5, nbr_node_id:9, gen:29
    frag_id 17, Intf Address:20.5.19.19
    TE metric:1, IGP metric:1, attribute flags:0x0
    SRLGs: None
    physical_bw: 1000000 (kbps), max_reservable_bw_global: 0 (kbps)
```

```
        max_reservable_bw_sub: 0 (kbps)

                              Global Pool    Sub Pool
              Total Allocated  Reservable     Reservable
              BW (kbps)        BW (kbps)      BW (kbps)
              ---------------  -----------    ----------
       bw[0]:            0            0             0
       bw[1]:            0            0             0
       bw[2]:            0            0             0
       bw[3]:            0            0             0
       bw[4]:            0            0             0
       bw[5]:            0            0             0
       bw[6]:            0            0             0
       bw[7]:            0            0             0

      link[1]: Broadcast, DR: 20.6.19.6, nbr_node_id:10, gen:29
        frag_id 18, Intf Address:20.6.19.19
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None
        physical_bw: 1000000 (kbps), max_reservable_bw_global: 0 (kbps)
        max_reservable_bw_sub: 0 (kbps)

                              Global Pool    Sub Pool
              Total Allocated  Reservable     Reservable
              BW (kbps)        BW (kbps)      BW (kbps)
              ---------------  -----------    ----------
       bw[0]:            0            0             0
       bw[1]:            0            0             0
       bw[2]:            0            0             0
       bw[3]:            0            0             0
       bw[4]:            0            0             0
       bw[5]:            0            0             0
       bw[6]:            0            0             0
       bw[7]:            0            0             0

IGP Id: 20.2.3.3, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 3.3.3.3, nbr_node_id:1, gen:4

      link[1]: Broadcast, Nbr IGP Id: 2.2.2.2, nbr_node_id:15, gen:4

IGP Id: 20.2.4.4, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 4.4.4.4, nbr_node_id:11, gen:5

      link[1]: Broadcast, Nbr IGP Id: 2.2.2.2, nbr_node_id:15, gen:5

IGP Id: 20.3.4.4, Network Node  (ospf 1 area 0)
```

```
      link[0]: Broadcast, Nbr IGP Id: 4.4.4.4, nbr_node_id:11, gen:6

      link[1]: Broadcast, Nbr IGP Id: 3.3.3.3, nbr_node_id:1, gen:6

IGP Id: 20.3.6.6, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 6.6.6.6, nbr_node_id:13, gen:7

      link[1]: Broadcast, Nbr IGP Id: 3.3.3.3, nbr_node_id:1, gen:7

IGP Id: 20.4.5.5, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 5.5.5.5, nbr_node_id:12, gen:8

      link[1]: Broadcast, Nbr IGP Id: 4.4.4.4, nbr_node_id:11, gen:8

IGP Id: 20.4.6.6, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 6.6.6.6, nbr_node_id:13, gen:9

      link[1]: Broadcast, Nbr IGP Id: 4.4.4.4, nbr_node_id:11, gen:9

IGP Id: 20.5.6.6, Network Node  (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 6.6.6.6, nbr_node_id:13, gen:10

      link[1]: Broadcast, Nbr IGP Id: 5.5.5.5, nbr_node_id:12, gen:10

IGP Id: 20.5.19.5, Network Node (ospf 1 area 0)
      link[0]: Broadcast, Nbr IGP Id: 5.5.5.5, nbr_node_id:12, gen:11

      link[1]: Broadcast, Nbr IGP Id: 19.19.19.19, nbr_node_id:14, gen:11

IGP Id: 20.6.19.6, Network Node (ospf 1 area 0)

      link[0]: Broadcast, Nbr IGP Id: 6.6.6.6, nbr_node_id:13, gen:12

      link[1]: Broadcast, Nbr IGP Id: 19.19.19.19, nbr_node_id:14, gen:12
R3#
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.2 MPLS Traffic Engineering with IS-IS (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2's Loopback0 interface.
  - Set the tunnel destination as XR1's Loopback0 interface.
  - Set the tunnel's path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1's Loopback0 interface.
  - Set the tunnel destination as R2's Loopback0 interface.
  - Set the tunnel's path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
```

```
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 dynamic
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

This example is similar to the previous MPLS Traffic Engineering with OSPF, except that IS-IS is used to compute the MPLS TE topology in the core of the network. Note that with IS-IS, you must enable the wide metric styles for the MPLS TE attributes to be encoded in the IS-IS TLVs. This can be done with either the `metric-style wide` command or the `metric-style transition` command, depending on whether all routers in the IS-IS network run the wide metric style or if some still run narrow.

Verification of this configuration is identical to the last, except that the MPLS TE topology shows IS-IS-related information. Below we see output similar to the last example, but the IGP identifiers are the routers' IS-IS NET addresses as opposed to the IPv4-formatted OSPF Router-IDs.

```
RP/0/0/CPU0:XR1#show mpls traffic-eng topology
 Wed Apr 4 00:18:34.506 UTC
 My_System_id: 0000.0000.0019.00 (IS-IS 1 level-2)
 My_BC_Model_Type: RDM

 Signalling error holddown: 10 sec Global Link Generation 339
 IGP Id: 0000.0000.0002.00
, MPLS TE Id: 2.2.2.2 Router Node  (IS-IS 1 level-2)

   Link[0]:Broadcast, DR:0000.0000.0002.02, Nbr Node Id:2, gen:304
       Frag Id:0, Intf Address:20.2.4.2, Intf Id:0
       Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
       TE Metric:10, IGP Metric:10, Attribute Flags:0x0
       Attribute Names:
       Switching Capability:, Encoding:
       BC Model ID:RDM
       Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
       Max Reservable BW Sub:0 (kbps)
                                 Global Pool    Sub Pool
              Total Allocated    Reservable     Reservable
              BW (kbps)          BW (kbps)      BW (kbps)
              ---------------    -----------    ----------
         bw[0]:           0          75000             0
         bw[1]:           0          75000             0
         bw[2]:           0          75000             0
         bw[3]:           0          75000             0
         bw[4]:           0          75000             0
         bw[5]:           0          75000             0
         bw[6]:           0          75000             0
         bw[7]:           0          75000             0
```

```
Link[1]:Broadcast, DR:0000.0000.0003.01, Nbr Node Id:4, gen:305
    Frag Id:0, Intf Address:20.2.3.2, Intf Id:0
    Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
    TE Metric:10, IGP Metric:10, Attribute Flags:0x0
    Attribute Names:
    Switching Capability:, Encoding:
    BC Model ID:RDM
    Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)

    Max Reservable BW Sub:0 (kbps)

                             Global Pool       Sub Pool
             Total Allocated   Reservable        Reservable
             BW (kbps)         BW (kbps)         BW (kbps)
             ---------------   -----------       ----------
       bw[0]:           0          75000                0
       bw[1]:           0          75000                0
       bw[2]:           0          75000                0
       bw[3]:           0          75000                0
       bw[4]:           0          75000                0
       bw[5]:           0          75000                0
       bw[6]:           0          75000                0
       bw[7]:           0          75000                0
 IGP Id: 0000.0000.0003.00
, MPLS TE Id: 3.3.3.3 Router Node  (IS-IS 1 level-2)

  Link[0]:Broadcast, DR:0000.0000.0003.03, Nbr Node Id:6, gen:308
      Frag Id:0, Intf Address:20.3.6.3, Intf Id:0
      Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Attribute Names:
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
      Max Reservable BW Sub:0 (kbps)
                               Global Pool       Sub Pool
               Total Allocated   Reservable        Reservable
               BW (kbps)         BW (kbps)         BW (kbps)
               ---------------   -----------       ----------
        bw[0]:           0          75000                0
        bw[1]:           0          75000                0
        bw[2]:           0          75000                0
        bw[3]:           0          75000                0
        bw[4]:           0          75000                0
        bw[5]:           0          75000                0
```

```
        bw[6]:           0          75000                 0
        bw[7]:           0          75000                 0

  Link[1]:Broadcast, DR:0000.0000.0003.02, Nbr Node Id:5, gen:309
      Frag Id:0, Intf Address:20.3.4.3, Intf Id:0
      Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Attribute Names:
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
      Max Reservable BW Sub:0 (kbps)
                                 Global Pool       Sub Pool
               Total Allocated   Reservable        Reservable
               BW (kbps)         BW (kbps)         BW (kbps)
               ---------------   -----------       ----------
        bw[0]:           0          75000                 0
        bw[1]:           0          75000                 0
        bw[2]:           0          75000                 0
<snip>
```

The goal of this verification is still the same, however, which is to check the constraint attributes of the individual links in the core of the network, and to identify current and available bandwidth reservations.

An additional verification that is useful for troubleshooting the setup of the MPLS TE tunnels is the debug of either the RSVP PATH & RESV messages or the `debug mpls traffic-eng tunnels signalling`, which essentially shows the same thing. Below, the routers R2, R4, R6, and XR1 have this debug enabled, and R2 configures its TE tunnel to XR1.

```
R2#debug mpls traffic-eng tunnels signalling

MPLS traffic-eng tunnels signalling debugging is on
R4#debug mpls traffic-eng tunnels signalling

MPLS traffic-eng tunnels signalling debugging is on
R6#debug mpls traffic-eng tunnels signalling

MPLS traffic-eng tunnels signalling debugging is on
RP/0/0/CPU0:XR1#debug mpls traffic-eng tunnel signaling


R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Tunnel0
R2(config-if)# ip unnumbered Loopback0
R2(config-if)# tunnel mode mpls traffic-eng
R2(config-if)# tunnel destination 19.19.19.19
R2(config-if)# tunnel mpls traffic-eng autoroute announce
R2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

When R2 initiates the tunnel, this should cause an RSVP reservation request message to be generated along the path. In this case, the path option is dynamic, so the RSVP messages follow the IGP path to XR1's Loopback 19.19.19.19/32.

```
R2#
TE-SIG-HE: Tunnel0 [1]->19.19.19.19: RSVP head-end open
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: received ADD RESV request
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: path next hop is 20.2.4.4 (Fa0/0.24)
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: sending ADD RESV reply
TE-SIG-HE: Tunnel0 [1]->19.19.19.19: received RESV CREATE
TE-SIG-HE: Tunnel0 [1]->19.19.19.19: notified of new label information
 FastEthernet0/0.24, nhop 20.2.4.4, frame, 16
TE-SIG-HE: Tunnel0 [1]->19.19.19.19: label information Changed
TE-SIG-HE: Tunnel0: route change: :none->FastEthernet0/0.24:16
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
%SYS-5-CONFIG_I: Configured from console by console
R2#

R4#TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: received ADD RESV request
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: path previous hop is 20.2.4.2 (Fa0/0.24)
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: path next hop is 20.4.6.6 (Fa0/0.46)
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: sending ADD RESV reply
```

```
R6#TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: received ADD RESV request
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: path previous hop is 20.4.6.4 (Fa0/0.46)
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: path next hop is 20.6.19.19 (Fa0/0.619)
TE-SIG-LM: 2.2.2.2_1->19.19.19.19_0 {7}: sending ADD RESV reply
RP/0/0/CPU0:XR1#debug mpls traffic-eng tunnel signaling
Wed Apr 4 00:12:12.701 UTC
RP/0/0/CPU0:XR1#RP/0/0/CPU0:Apr 4 00:12:21.069 : te_control[340]: DBG-TUNNEL-
SIG[1]: te_sig_rsvp_api_perf_handler:354: batch_size: 1, direction: 1
te_control[340]: DBG-TUNNEL-SIG[1]: te_sig_rsvp_api_recv_path:1133
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Successfully processed PATH_CR
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_validate_incoming_if:779
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
te_s2l_validate_incoming_if: Ingress interface GigabitEthernet0_1_0_0.619 validated
te_control[340]: DBG-TUNNEL-SIG[1]: te_rsvp_api_check_class_type_priority:391
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7): CT:
0, Setup_priority: 7, Hold_priority: 7, DS-TE mode: 1
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_compute_and_set_local_rid:543
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Setting Local RID to 19.19.19.19
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_compute_and_set_downstream_rid:630
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Setting Downstream RID to 0.0.0.0
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_compute_and_set_upstream_rid:669
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Existing upstream RID (0.0.0.0) may change
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_compute_and_set_upstream_rid:744
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Setting Upstream RID to 6.6.6.6
te_control[340]: DBG-TUNNEL-SIG[1]: te_s2l_proc_recovery_lbl:1852
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Recovery label is not set
te_control[340]: DBG-TUNNEL-SIG[1]: te_sig_rsvp_api_handler_resv_send:1925
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Successfully sent RESV_CR to RSVP
te_control[340]: DBG-TUNNEL-SIG[1]: te_sig_rsvp_api_perf_handler:354: batch_size: 1, direction: 0
te_control[340]: DBG-TUNNEL-SIG[1]: te_sig_rsvp_api_perf_handler:354: batch_size: 1, direction: 1
te_control[340]: DBG-TUNNEL-SIG[1]: te_sig_rsvp_api_recv_resv_resp:1365
(T:0,L:1,P:2147483647,E:2.2.2.2,SI:0,SO:0.0.0.0,S:2.2.2.2,D:19.19.19.19,CT:7):
Successfully processed RESV_RESP
```

This output means that each router along the path asks the next router if it can make a reservation based on the particular constraints of this tunnel. Specifically, this is what the RSVP PATH message does. If all the routers agree that the reservation can be fulfilled, the tail of the tunnel will reply with the RESV message to actually make the reservation, which then occurs on a hop-by-hop basis back toward the head of the tunnel (the originator). Because in this case the reservation is successful, R2 learns the MPLS TE transport label binding for the tunnel. This successful result can be verified as follows.

```
R2#show mpls traffic-eng tunnels

P2P TUNNELS/LSPs:
Name: R2_t0                                (Tunnel0) Destination: 19.19.19.19

  Status: Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type dynamic (Basis for Setup, path weight 30)

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled  LockDown: disabled Loadshare: 0        bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : FastEthernet0/0.24, 18
  Next Hop : 20.2.4.4
  RSVP Signalling Info:
       Src 2.2.2.2, Dst 19.19.19.19, Tun_Id 0, Tun_Instance 3
    RSVP Path Info:
      My Address: 20.2.4.2 Explicit Route: 20.2.4.4 20.4.6.4 20.4.6.6 20.6.19.6
20.6.19.19 19.19.19.19

      Record   Route:   NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  History:
    Tunnel:
      Time since created: 17 hours, 11 minutes
      Time since path change: 16 hours, 55 minutes
```

```
      Number of LSP IDs (Tun_Instances) used: 3
    Current LSP: [ID: 3]
      Uptime: 16 hours, 55 minutes
    Prior LSP: [ID: 2]
      ID: path option unknown
      Removal Trigger: tunnel shutdown

<snip>
```

The reverse is also true when XR1 initiates its tunnel. In the below output, we see the `debug ip rsvp signalling` in on R6, which is in the transit path of the tunnel from XR1 to R2.

```
R6#debug ip rsvp signalling

RP/0/0/CPU0:XR1#conf t
Wed Apr 4 17:28:35.824 UTC
RP/0/0/CPU0:XR1(config)#interface tunnel-te0
RP/0/0/CPU0:XR1(config-if)# ipv4 unnumbered Loopback0
RP/0/0/CPU0:XR1(config-if)# autoroute announce
RP/0/0/CPU0:XR1(config-if)# destination 2.2.2.2
RP/0/0/CPU0:XR1(config-if)# path-option 1 dynamic RP/0/0/CPU0:XR1(config-if)#commit

R6# RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Received Path message from 20.6.19.19
 (on
FastEthernet0/0.619)
RSVP: new path message passed parsing, continue...
RSVP: Triggering outgoing Path due to incoming Path change or new Path
RSVP: Triggering outgoing Path refresh
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Path refresh, Event: rmsg not enabled or
ack rcvd, State: trigger to normal
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Path refresh (msec), config: 30000 curr:
30000 xmit: 30000
RSVP: Triggering outgoing Path due to incoming Path change or new Path
RSVP: Triggering outgoing Path refresh
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Path refresh, Event: rmsg not enabled or
ack rcvd, State: trigger to normal
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Path refresh (msec), config: 30000 curr:
30000 xmit: 30000 RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Sending Path message to 20.3.6.3

RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: building hop object with src addr:
20.3.6.6
RSVP: session 2.2.2.2_0[19.19.19.19] (7): Received Resv message from 20.3.6.3
 (on
FastEthernet0/0.36)
```

```
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Successfully parsed Resv message from
20.3.6.3 (on FastEthernet0/0.36)
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: reservation not found--new one
RSVP-RESV: Admitting new reservation: 6657A648 RSVP-RESV:
 reservation (RSB 0x6657A648) was installed on FastEthernet0/0.36
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: start requesting 0 kbps SE reservation on
FastEthernet0/0.619, neighbor 20.6.19.19
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Refresh RESV, req=665A6DF8 [cleanup timer
is not awake]
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Resv refresh, Event: rmsg not enabled or
ack rcvd, State: trigger to normal
RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: Resv refresh (msec), config: 30000 curr:
30000 xmit: 30000 RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}:
 Sending Resv message to 20.6.19.19 from 20.6.19.6

RSVP: 19.19.19.19_3->2.2.2.2_0[Src] {7}: building hop object with src addr:
20.6.19.6   R6#
R6#
```

The above output shows that R6 receives the RSVP PATH message from XR1, which is XR1 requesting that the MPLS TE tunnel be established. R6 then forwards the PATH message to R3 to continue on to the final destination. The reservation then occurs in the reverse path, with R3 replying to R6 with the RSVP RESV message, and then R6 sending RESV to XR1.

The final result of having both tunnels established is that the customer's MPLS L3VPN traffic is tunneled over the MPLS TE tunnels in the Service Provider core.

```
R1#traceroute 20.20.20.20 source 1.1.1.1

Type escape sequence to abort. Tracing the route to 20.20.20.20

  1 10.1.2.2 4 msec 0 msec 0 msec 2 20.2.4.4 [MPLS: Labels 16/16000 Exp 0] 4 msec 0 msec 0 msec
 3 20.4.6.6 [MPLS: Labels 16/16000 Exp 0] 4 msec 0 msec 0 msec
  4 20.6.19.19 12 msec 4 msec 0 msec
  5 10.19.20.20 116 msec *  4 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
Wed Apr 4 17:36:32.207 UTC

Type escape sequence to abort. Tracing the route to 1.1.1.1

 1 10.19.20.19 6 msec  4 msec  2 msec 2 20.6.19.6 [MPLS: Labels 17/16 Exp 5] 3 msec  5 msec  2 msec
 3 20.3.6.3   [MPLS:  Labels 17/16 Exp 5] 2 msec  3 msec  3 msec
    4 10.1.2.2   [MPLS:  Label 16 Exp 5] 5 msec  4 msec  2 msec
```

```
5 10.1.2.1 2 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.3 MPLS TE Explicit Paths (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2's Loopback0 interface.
  - Set the tunnel destination as XR1's Loopback0 interface.
  - Set the tunnel's path option to explicitly follow the path from R2 to R3 to R4 to R6 to R5 to XR1.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1's Loopback0 interface
  - Set the tunnel destination as R2's Loopback0 interface.
  - Set the tunnel's path option to explicitly follow the path from XR1 to R6 to R5 to R4 to R3 to R2.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
ip explicit-path name TO_XR1 enable
 next-address 20.2.3.3
 next-address 20.3.4.4
 next-address 20.4.6.6
 next-address 20.5.6.5
 next-address 20.5.19.19
 next-address 19.19.19.19
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name TO_XR1
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
```

```
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
```

```
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
explicit-path name TO_R2
 index 1 next-address strict ipv4 unicast 20.6.19.6
 index 2 next-address strict ipv4 unicast 20.5.6.5
 index 3 next-address strict ipv4 unicast 20.4.5.4
 index 4 next-address strict ipv4 unicast 20.3.4.3
 index 5 next-address strict ipv4 unicast 20.2.3.2
 index 6 next-address strict ipv4 unicast 2.2.2.2
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 explicit name TO_R2
!
router isis 1
 ddress-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
```

```
  mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

The previous examples that used dynamic path calculation for the MPLS TE tunnels didn't really show any advantage of using MPLS TE in the core over LDP. With LDP you simply enable it on all IGP interfaces, and all IGP learned routes then have MPLS labels allocated for them. With MPLE TE, RSVP will only allocate labels for destinations that you manually have tunnels configured for. For example, if you had 10 PE routers and wanted labels for all of their Loopbacks, with MPLS TE you would have to configure a full mesh of MPLS tunnels between them, i.e. n*(n-1)/2 tunnels, or 45 tunnels. In a case like this, LDP becomes much more scalable.

The real advantage of using MPLS TE, as shown in this particular example, is that you have much more granular control over how traffic routes through the core of the network. Instead of simply relying on the IGP shortest path to the destination, MPLS TE essentially allows you to do source routing, because the head-end of the tunnel can control the path that its traffic is going to use.

When configuring explicit paths, the most common problems that occur are that the path is entered incorrectly (such as a typo in the addresses) or that one of the requested links along the path can't satisfy the reservation. To make sure that the path is valid, use the `show mpls traffic-eng tunnels` command, as seen below.

```
R2#show mpls traffic-eng tunnels

P2P TUNNELS/LSPs:

Name: R2_t0                              (Tunnel0) Destination: 19.19.19.19
  Status: Admin: up         Oper: up      Path: valid       Signalling: connected
path option 1, type explicit TO_XR1
 (Basis for Setup, path weight 50)
```

```
  Config Parameters:
    Bandwidth: 0    kbps (Global)   Priority: 7 7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled  LockDown: disabled Loadshare: 0    bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


InLabel  :  -
OutLabel : FastEthernet0/0.23, 16
Next Hop : 20.2.3.3 RSVP Signalling Info:
 Src 2.2.2.2, Dst 19.19.19.19
, Tun_Id 0, Tun_Instance 1
  RSVP Path Info:
    My Address: 20.2.3.2 Explicit Route: 20.2.3.3 20.3.4.3 20.3.4.4 20.4.6.4
 20.4.6.6 20.5.6.6 20.5.6.5 20.5.19.5
 20.5.19.19 19.19.19.19
    Record   Route:   NONE
    Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record  Route:  NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
History:
  Tunnel:
    Time since created: 23 minutes, 37 seconds
    Time since path change: 23 minutes, 35 seconds
    Number of LSP IDs (Tun_Instances) used: 1
  Current LSP: [ID: 1]
    Uptime: 23 minutes, 35 seconds
 LSP Tunnel XR1_t0 is signalled, connection is up

  InLabel  : FastEthernet0/0.23, implicit-null
  Prev Hop : 20.2.3.3
  OutLabel :  -
  RSVP Signalling Info:
       Src 19.19.19.19, Dst 2.2.2.2, Tun_Id 0, Tun_Instance 2
    RSVP Path Info:
      My Address: 2.2.2.2
      Explicit Route:  NONE
      Record   Route:  NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  NONE
```

```
      Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

P2MP TUNNELS:

P2MP SUB-LSPS:
```

From this output we need to verify that the path is valid and that the signaling is connected. In the above case both the path and the signaling are working, hence the tunnels are working. Final verification of a traceroute from the customer sites should show traffic following the requested explicit paths.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
  1 10.1.2.2
 0 msec 0 msec 4 msec  2 20.2.3.3 [MPLS: Labels 16/16000
 Exp 0] 0 msec 4 msec 0 msec  3 20.3.4.4 [MPLS: Labels 17/16000
 Exp 0] 4 msec 0 msec 4 msec  4 20.4.6.6 [MPLS: Labels 19/16000
 Exp 0] 0 msec 4 msec 0 msec  5 20.5.6.5 [MPLS: Labels 16/16000
 Exp 0] 4 msec 0 msec 4 msec  6 20.5.19.19
 4 msec 4 msec 0 msec
  7 10.19.20.20 8 msec *    4 msec

RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 5 msec   5 msec  3 msec   2 20.6.19.6 [MPLS: Labels 18/16 Exp 5] 3 msec
  5 msec  4 msec 3 20.5.6.5 [MPLS: Labels 17/16
Exp 5] 4 msec  5 msec  2 msec  4 20.4.5.4 [MPLS: Labels 18/16
Exp 5] 3 msec  4 msec  2 msec  5 20.3.4.3 [MPLS: Labels 17/16
Exp 5] 3 msec  5 msec  2 msec  6 10.1.2.2 [MPLS: Label 16 Exp
5] 3 msec  4 msec  3 msec
 7 10.1.2.1 3 msec  *  3 msec
```

The potential problem with this design, however, is that there is no fallback path option if one of the hops along the explicit path fails. For example, if the links of R5 go down, both of these tunnels will fail even though there are other potentially valid paths that could be used in the core of the topology. This is shown below.

```
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#int fa0/0R5(config-if)#shutdown
```

```
R5(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

R2#%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
R2#show mpls traffic-eng tunnels

P2P TUNNELS/LSPs:

Name: R2_t0                               (Tunnel0) Destination: 19.19.19.19
  Status: Admin: up         Oper: down   Path: not valid   Signalling: Down

    path option 1, type explicit TO_XR1

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
    auto-bw: disabled

History:
  Tunnel:
    Time since created: 56 minutes, 31 seconds
    Time since path change: 1 minutes, 33 seconds
    Number of LSP IDs (Tun_Instances) used: 10
  Prior LSP: [ID: 1]
    ID: path option 1 [10] Removal Trigger: path error
    Last Error: CTRL:: Explicit path has unknown address, 20.5.19.19
```

When R5's link is disabled, R2's tunnel interface goes down. From the output above, we can see that there is a path calculation error, because R2 cannot reach the link between R5 and XR1. Even though R2 can still reach the Loopback of XR1, which is the tunnel destination, traffic cannot be routed over the tunnel because there is no valid path option. The result is that R2 and XR1 can still reach each other, but the end customers cannot.

```
R2#traceroute 19.19.19.19 source 2.2.2.2

Type escape sequence to abort.
Tracing the route to 19.19.19.19

  1 20.2.4.4 0 msec
    20.2.3.3 4 msec
    20.2.4.4 0 msec
```

```
  2 20.3.6.6 4 msec
    20.4.6.6 0 msec
    20.3.6.6 0 msec
  3 20.6.19.19 4 msec * 4 msec
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 4 msec 0 msec 0 msec
  2  *  *  *
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Wed Apr 4 19:43:34.986 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1  10.19.20.19 !N  *  !N
```

To avoid this problem, either Fast Reroute (FRR) Link or Node Protection can be configured to automatically heal around the broken link or router, or a lower-priority dynamic path option can be configured. The second way is the easiest from a configuration point of view, and can be seen below.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int tunnel0R2(config-if)#tunnel mpls traffic-eng path-option 2 dynamic
R2(config-if)#end
R2# %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

RP/0/0/CPU0:XR1#config t
Wed Apr 4 19:46:01.789 UTC
RP/0/0/CPU0:XR1(config)#interface tunnel-te0
RP/0/0/CPU0:XR1(config-if)#path-option 2 dynamicRP/0/0/CPU0:XR1(config-if)#commit

RP/0/0/CPU0:Apr 4 19:46:13.412 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin'. Use 'show configuration commit changes
1000000232' to view the changes.
```

Now, with alternate paths, the customer traffic falls back to follow the normal IGP shortest path tree.

```
R1#traceroute 20.20.20.20
```

```
Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 0 msec 0 msec 4 msec  2 20.2.4.4 [MPLS: Labels 16/16000
 Exp 0] 0 msec 0 msec 0 msec  3 20.4.6.6 [MPLS: Labels 16/16000
 Exp 0] 0 msec 4 msec 0 msec
  4 20.6.19.19 4 msec 0 msec 0 msec
  5 10.19.20.20 4 msec *    4 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
Wed Apr 4 19:46:48.483 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 7 msec  5 msec  2 msec  2 20.6.19.6 [MPLS: Labels 17/16
 Exp 5] 4 msec  3 msec  2 msec  3 20.3.6.3 [MPLS: Labels 16/16
 Exp 5] 2 msec  3 msec  2 msec  4 10.1.2.2 [MPLS: Label 16
 Exp 5] 3 msec  3 msec  3 msec
 5 10.1.2.1 2 msec  *  22 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.4 MPLS TE Bandwidth Reservations (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
  - Configure R3 and R6 so that 30 Mbps can be reserved via RSVP on any of their interfaces.
  - Configure all other routers in the core so that 75 Mbps can be reserved via RSVP on any of their interfaces.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2’s Loopback0 interface.
  - Set the tunnel destination as XR1’s Loopback0 interface.
  - Set the tunnel to request a bandwidth reservation of 50 Mbps.
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1’s Loopback0 interface.
  - Set the tunnel destination as R2’s Loopback0 interface.
  - Set the tunnel to request a bandwidth reservation of 35 Mbps
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute

should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng bandwidth 50000
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth 30000
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth 30000
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth 30000
!
```

```
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
```

```
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
ip rsvp bandwidth 30000
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
ip rsvp bandwidth 30000
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
ip rsvp bandwidth 30000
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
ip rsvp bandwidth 30000
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 signalled-bandwidth 35000
 destination 2.2.2.2
 path-option 1 dynamic
!
router isis 1
 address-family ipv4 unicast
 metric-style wide
 mpls traffic-eng level-2-only
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
  bandwidth 75000
 !
 interface GigabitEthernet0/1/0/0.619
```

```
  bandwidth 75000
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

MPLS TE tunnel bandwidth reservations are used to help ensure that a Service Provider can conform to the Service Level Agreements (SLAs) they are selling to customers. Instead of simply using the addition of the bandwidth-based link costs as the deciding path selection metric, like OSPF does, MPLS TE tunnels can use the total bandwidth and available bandwidth values on a per-link basis that RSVP reports as part of the TE topology to calculate the path for an individual tunnel.

The basic logic behind this is that if the Service Provider has 10 customers, each of which have two sites and SLAs that guarantee 1 Gbps of transit bandwidth, the SP can provision 20 MPLS TE tunnels, each requesting 1 Gbps of bandwidth. Remember that because TE tunnels are unidirectional, there must be a tunnel from PE1 to PE2 and from PE2 back to PE1 to provide bidirectional tunneling. When the tunnels are provisioned, the actual path that they take through the SP core can be automatically determined based on the amount of available bandwidth. If the core consists of GigE, OC-48, TenGigE, and OC-192 links, the tunnels will automatically be arranged in a way that gives each customer a dedicated 1Gbps reservation.

Note, however, that the MPLS TE tunnel bandwidth reservation is only a reservation in the control plane; it is not a reservation in the data plane. This means that there is nothing preventing traffic going over a tunnel from actually using more bandwidth than the reservation says it is guaranteed. You must still enforce at the Service Provider edge the amount of bandwidth that is admitted to the network with some form of admission control, such as policing.

In this example, the core of the network is staged to support reservations up to 75 Mbps everywhere, and reservations up to 30 Mbps on R3 and R6. These values can be verified as follows:

```
R3#show ip rsvp interface
interface     rsvp       allocated i/f max
  flow max   sub max Fa0/0        ena         0 0
  0          0 Fa0/0.23     ena         0 30M
  30M        0
```

```
Fa0/0.24     ena        0 30M
  30M       0 Fa0/0.34     ena        0 30M
  30M       0 Fa0/0.36     ena        0 30M
  30M       0
R4#show ip rsvp interface
interface    rsvp allocated  i/f max
  flow max  sub max Fa0/0        ena 0           0
  0         0 Fa0/0.24     ena 35M        75M
  75M       0 Fa0/0.34     ena 0          75M
  75M       0 Fa0/0.45     ena 50M        75M
  75M       0 Fa0/0.46     ena 0          75M
  75M       0
RP/0/0/CPU0:XR1#show rsvp interface
Wed Apr 4 21:55:41.656 UTC

*: RDM: Default I/F B/W %: 75% [default] (max resv/bc0), 0% [default] (bc1)
 Interface MaxBW (bps)  MaxFlow (bps) Allocated (bps)
      MaxSub (bps)
-----------  ------------ ------------- ------------------- -------------Gi0/1/0/0.519
    75M            75M
      35M ( 46%)            0* Gi0/1/0/0.619    75M           75M
        0 (  0%)            0*
```

The above output shows that R3 can support up to 30 Mbps of reservations, but currently has no reservations actually in use. R4 can support up to 75 Mbps of reservations, and it currently has reservations of 35 Mbps and 50 Mbps on interfaces Fa0/0.24 and Fa0/0.45. XR1 can support up to 75 Mbps of reservations, and it currently has 35 Mbps reserved on Gig0/1/0/0.519. Note that in regular IOS when you issue the `ip rsvp bandwidth` command at the interface level, the default amount of reservable bandwidth is 75% of the configured `bandwidth` command. In IOS XR, there is no default and the amount of bandwidth available for reservations must be manually specified.

The details of all links through the entire TE topology, along with their current reservations and available bandwidth, can be verified at any point in the core network as follows.

```
R5#show mpls traffic-eng topology 4.4.4.4

IGP Id: 0000.0000.0004.00, MPLS TE Id:4.4.4.4 Router Node  (isis  level-2) id 31
      link[0]: Broadcast, DR: 0000.0000.0004.04, nbr_node_id:28, gen:90
          frag_id 0, Intf Address:20.4.6.4
          TE metric:10, IGP metric:10, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
```

```
        max_reservable_bw_sub: 0 (kbps)

                          Global Pool       Sub Pool
             Total Allocated   Reservable        Reservable
             BW (kbps)         BW (kbps)         BW (kbps)
             ---------------   -----------       ----------
      bw[0]:            0         75000                0
      bw[1]:            0         75000                0
      bw[2]:            0         75000                0
      bw[3]:            0         75000                0
      bw[4]:            0         75000                0
      bw[5]:            0         75000                0
      bw[6]:            0         75000                0
      bw[7]:            0         75000                0

    link[1]: Broadcast, DR: 0000.0000.0004.03, nbr_node_id:22, gen:90       frag_id 0,
 Intf Address:20.4.5.4
        TE metric:10, IGP metric:10, attribute flags:0x0
        SRLGs: None physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)

        max_reservable_bw_sub: 0 (kbps)

                          Global Pool       Sub Pool
             Total Allocated   Reservable        Reservable
             BW (kbps)         BW (kbps)         BW (kbps)
             ---------------   -----------       ----------
      bw[0]:            0         75000                0
      bw[1]:            0         75000                0
      bw[2]:            0         75000                0
      bw[3]:            0         75000                0
      bw[4]:            0         75000                0
      bw[5]:            0         75000                0
      bw[6]:            0         75000                0
 bw[7]:        50000          25000                0

    link[2]: Broadcast, DR: 0000.0000.0002.02, nbr_node_id:35, gen:90       frag_id 0,
 Intf Address:20.2.4.4
        TE metric:10, IGP metric:10, attribute flags:0x0
        SRLGs: None physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)

        max_reservable_bw_sub: 0 (kbps)

                          Global Pool       Sub Pool
             Total Allocated   Reservable        Reservable
             BW (kbps)         BW (kbps)         BW (kbps)
             ---------------   -----------       ----------
```

```
    bw[0]:            0          75000               0
    bw[1]:            0          75000               0
    bw[2]:            0          75000               0
    bw[3]:            0          75000               0
    bw[4]:            0          75000               0
    bw[5]:            0          75000               0
    bw[6]:            0          75000               0
bw[7]:          35000          40000               0



  link[3]: Broadcast, DR: 0000.0000.0003.02, nbr_node_id:24, gen:90
      frag_id 0, Intf Address:20.3.4.4
      TE metric:10, IGP metric:10, attribute flags:0x0
      SRLGs: None
      physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
      max_reservable_bw_sub: 0 (kbps)

                           Global Pool       Sub Pool
           Total Allocated   Reservable        Reservable
           BW (kbps)         BW (kbps)         BW (kbps)
           ---------------   -----------       ----------
    bw[0]:            0          75000               0
    bw[1]:            0          75000               0
    bw[2]:            0          75000               0
    bw[3]:            0          75000               0
    bw[4]:            0          75000               0
    bw[5]:            0          75000               0
    bw[6]:            0          75000               0
    bw[7]:            0          75000               0
```

Like the OSPF or IS-IS databases, this output can show all routers in the topology at the same time, or it can show just an individual node by referencing its MPLS TE Router-ID, as seen above. In this case, we see that the node with Router-ID 4.4.4.4 (R4) has a link with address 20.4.5.4 (the link to R5), which has a total bandwidth of 100 Mbps, a maximum reservable bandwidth of 75 Mbps (75% by default of the total bandwidth), 50 Mbps actually reserved, and 25 Mbps left over. The number 7 of the reservation refers to the TE tunnel’s setup and hold priority that actually made the reservation. If a new reservation were to come in for 65 Mbps, with a higher setup priority (lower numerical value), the new tunnel could preempt the old tunnel’s reservation. In this manner, the core of the network can offer prioritization of tunnel preference.

The final result of this configuration is that the tunnel from R2 to XR1 and the tunnel from XR1 to R2 avoid the links of R3 and R6, because they do not have enough available bandwidth for reservation. This can be seen in the traceroute outputs below.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 4 msec 0 msec 0 msec
  2 20.2.4.4 [MPLS: Labels 18/16000 Exp 0] 4 msec 0 msec 0 msec
  3 20.4.5.5 [MPLS: Labels 17/16000 Exp 0] 0 msec 0 msec 4 msec
  4 20.5.19.19 0 msec 4 msec 4 msec
  5 10.19.20.20 4 msec *  8 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Wed Apr 4 22:14:40.335 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 6 msec  4 msec  2 msec
 2 20.5.19.5 [MPLS: Labels 16/16 Exp 5] 3 msec  4 msec  3 msec
 3 20.4.5.4 [MPLS: Labels 17/16 Exp 5] 3 msec  5 msec  2 msec
 4 10.1.2.2 [MPLS: Label 16 Exp 5] 1 msec  3 msec  3 msec
 5 10.1.2.1 2 msec  *  3 msec
```

The disadvantage of the design of this specific scenario is that if any of the links of either R4 or R5 go down, both tunnels will go down, because there is not enough bandwidth for them to recalculate to use the paths via R3 or R6. The link failure and resulting tunnel teardown are shown below.

```
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.R5(config)#int fa0/0
R5(config-if)#shut

R5(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
down
R5(config-if)#
R2#debug mpls traffic-eng tunnel error

MPLS traffic-eng tunnels errors debugging is on
TE-SIG-HE: Tunnel0 [64]: path verification failed (unprotected) [Can't use link
20.5.19.5 on node 5.5.5.5]
 %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
```

Because R2 has no alternate path in the topology with an available bandwidth of 50 Mbps, the tunnel cannot reroute around the failure.

If the bandwidth requirements were lowered, the tunnel would automatically set up again via the R3 and R6 path, as shown below.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Tunnel0R2(config-if)# tunnel mpls traffic-eng bandwidth 10000
R2(config-if)#end
R2#%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R2#show mpls traffic-eng tunnels

P2P TUNNELS/LSPs:

Name: R2_t0                              (Tunnel0) Destination: 19.19.19.19
  Status: Admin: up            Oper: up  Path: valid       Signalling: connected

    path option 1, type dynamic (Basis for Setup, path weight 30)

  Config Parameters: Bandwidth: 10000
    kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled  LockDown: disabled Loadshare: 10000    bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: dynamic path option 1 is active
```

```
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled



InLabel  :  -
OutLabel : FastEthernet0/0.24, 20
Next Hop : 20.2.4.4
RSVP Signalling Info:
     Src 2.2.2.2, Dst 19.19.19.19, Tun_Id 0, Tun_Instance 81
  RSVP Path Info:
    My Address: 20.2.4.2 Explicit Route: 20.2.4.4 20.4.6.4 20.4.6.6 20.6.19.6
 20.6.19.19 19.19.19.19

    Record   Route:  NONE
    Tspec: ave rate=10000 kbits, burst=1000 bytes, peak rate=10000 kbits
  RSVP Resv Info:
    Record   Route:  NONE
    Fspec: ave rate=10000 kbits, burst=1000 bytes, peak rate=10000 kbits
History:
  Tunnel:
    Time since created: 1 hours, 36 minutes
    Time since path change: 13 seconds
    Number of LSP IDs (Tun_Instances) used: 81
  Current LSP: [ID: 81]
    Uptime: 13 seconds
  Prior LSP: [ID: 64]
    ID: path option unknown
    Removal Trigger: path verification failed
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.5 MPLS TE Metric Manipulation (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2’s Loopback0 interface.
  - Set the tunnel destination as XR1’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1’s Loopback0 interface.
  - Set the tunnel destination as R2’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure MPLS TE metrics as follows:
  - The preferred path from R2 to XR1 should be R2 to R3 to R4 to R6 to XR1.
  - The preferred path from XR1 to R2 should be XR1 to R6 to R4 to R3 to R2.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
 !
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 no mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
ip rsvp bandwidth
 !
```

```
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
```

```
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 1000
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 dynamic
!
router isis 1
 address-family ipv4 unicast
 metric-style wide
 mpls traffic-eng level-2-only
 mpls traffic-eng router-id Loopback0
!
```

```
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
  admin-weight 1000
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

When OSPF or IS-IS is used in the SP core for the purpose of MPLS Traffic Engineering, two different metrics are advertised for each link: the IGP metric and the TE metric. By default, the TE metric is inherited from the IGP metric. If the IGP metric is changed (that is, the OSPF cost or the IS-IS metric), the TE metric will likewise change. However, the TE metric can be manually changed separately from the IGP metric, as is the case in this example. Additionally, by default all MPLS TE tunnels will prefer to use the TE metric value for their dynamic path selection. This can be controlled globally or on a per-tunnel basis with the command `tunnel mpls traffic-eng path-selection metric igp` in regular IOS or `path-selection metric igp` in IOS XR at the tunnel interface level.

The TE metrics can be verified by viewing the MPLS TE topology, as follows.

```
R2#show mpls traffic-eng topology | include (TE Id|Intf Address|TE metric)
IGP Id: 0000.0000.0002.00, MPLS TE Id:2.2.2.2
 Router Node  (isis  level-2)           frag_id 0, Intf Address:20.2.4.2
TE metric:1000
, IGP metric:10, attribute flags:0x0           frag_id 0, Intf Address:20.2.3.2
TE metric:10
, IGP metric:10, attribute flags:0x0 IGP Id: 0000.0000.0003.00, MPLS TE Id:3.3.3.3
 Router Node  (isis  level-2)          frag_id 0, Intf Address:20.3.6.3
TE metric:1000
, IGP metric:10, attribute flags:0x0           frag_id 0, ntf Address:20.3.4.3
TE metric:10
, IGP metric:10, attribute flags:0x0           frag_id 0, Intf Address:20.2.3.
TE metric:10
, IGP metric:10, attribute flags:0x0 IGP Id: 0000.0000.0004.00, MPLS TE Id:4.4.4.4
 Router Node  (isis  level-2)           frag_id 0, Intf Address:20.4.6.4
```

```
TE metric:10
, IGP metric:10, attribute flags:0x0           frag_id 0, Intf Address:20.2.4.4
TE metric:1000
, IGP metric:10, attribute flags:0x0          frag_id 0, Intf Address:20.3.4.4
TE metric:10
, IGP metric:10, attribute flags:0x0 IGP Id: 0000.0000.0006.00, MPLS TE Id:6.6.6.6
 Router Node  (isis  level-2)          frag_id 0, Intf Address:20.6.19.6
TE metric:10
, IGP metric:10, attribute flags:0x0          frag_id 0, Intf Address:20.3.6.6
TE metric:1000
, IGP metric:10, attribute flags:0x0          frag_id 0, Intf Address:20.4.6.6
TE metric:10
, IGP metric:10, attribute flags:0x0 IGP Id: 0000.0000.0019.00, MPLS TE Id:19.19.19.19
 Router Node  (isis  level-2)          frag_id 0, Intf Address:20.6.19.19
, Nbr Intf Address:20.6.19.6  TE metric:10
, IGP metric:10, attribute flags:0x0
```

Note that the interfaces that did not have their TE metrics changed use the default cost of 10 that comes from the IS-IS cost.

The final result of this configuration is that the R3 to R4 to R6 path is preferred bidirectionally for the tunnels from R2 to XR1 and from XR1 to R2, as shown below.

```
R1#traceroute 20.20.20.20



Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 0 msec 4 msec 0 msec   2 20.2.3.3 [MPLS: Labels 16/16013
 Exp 0] 0 msec 4 msec 0 msec   3 20.3.4.4 [MPLS: Labels 20/16013
 Exp 0] 4 msec 0 msec 0 msec   4 20.4.6.6 [MPLS: Labels 16/16013
 Exp 0] 0 msec 0 msec 4 msec
  5 20.6.19.19 4 msec 0 msec 4 msec
  6 10.19.20.20 4 msec *  4 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Wed Apr 4 22:56:21.243 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 7 msec   4 msec  1 msec  2 20.6.19.6 [MPLS: Labels 17/16
 Exp 5] 3 msec  4 msec  4 msec  3 20.4.6.4 [MPLS: Labels 17/16
 Exp 5] 2 msec  3 msec  3 msec  4 20.3.4.3 [MPLS: Labels 17/16
 Exp 5] 3 msec  4 msec  3 msec  5 10.1.2.2 [MPLS: Label 16
 Exp 5] 3 msec  4 msec  2 msec
 6 10.1.2.1 2 msec  *  3 msec
```

If one of these links or nodes fails, the tunnels will automatically recalculate to the next lowest cost path based on the TE metric, as shown below.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0R3(config-if)#shut
R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
down
R2#debug mpls traffic-eng topology change
MPLS traffic-eng topology change events debugging is onR2#debug mpls traffic-eng tunnel signalling
MPLS traffic-eng tunnels signalling debugging is on

TE-SIG-HE: Tunnel0 [16]->19.19.19.19: received RESV UPDATE TE-SIG-HE: Tunnel0 [16]->19.19.19.19:
notified of new label information
        FastEthernet0/0.24, nhop 20.2.4.4, frame, 18
TE-SIG-HE: Tunnel0 [16]->19.19.19.19: label information No Change
```

```
TE-PCALC-LSA: NODE_CHANGE_UPDATE isis   level-2        link flags: LINK_CHANGE_DOWN
        system_id: 0000.0000.0002.00, link 20.2.3.2
        nbr_system_id: 0000.0000.0003.01, link 0.0.0.0
TE-PCALC-LSA: NODE_CHANGE_UPDATE isis   level-2        link flags: LINK_CHANGE_DOWN
        system_id: 0000.0000.0004.00, link 20.3.4.4
        nbr_system_id: 0000.0000.0003.02, link 0.0.0.0
TE-PCALC-LSA: NODE_CHANGE_UPDATE isis   level-2        link flags: LINK_CHANGE_DOWN
        system_id: 0000.0000.0006.00, link 20.3.6.6

        nbr_system_id: 0000.0000.0003.03, link 0.0.0.0
```

R2 detects that there is a change in the TE topology, and RSVP is re-signaled to bind a new label via the new path. The customers traffic is likewise rerouted via this new tunnel path.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 0 msec 0 msec 0 msec  2 20.2.4.4 [MPLS: Labels 18/16013 Exp 0] 0 msec 4 msec 0 msec
  3 20.4.6.6 [MPLS: Labels 18/16013 Exp 0] 4 msec 0 msec 0 msec
  4 20.6.19.19 4 msec 4 msec 4 msec
  5 10.19.20.20 4 msec *  4 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
Wed Apr 4 23:12:25.823 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 6 msec   4 msec  2 msec  2 20.6.19.6 [MPLS: Labels 19/16 Exp 5] 3 msec  3 msec  2 msec
 3 20.4.6.4 [MPLS: Labels 19/16 Exp 5] 2 msec  3 msec  2 msec
 4 10.1.2.2 [MPLS: Label 16 Exp 5] 2 msec  3 msec  2 msec

 5 10.1.2.1 2 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.6 MPLS TE with Static Routing (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2’s Loopback0 interface.
  - Set the tunnel destination as XR1’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure a static route for XR1’s Loopback0 interface via the tunnel.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1’s Loopback0 interface.
  - Set the tunnel destination as R2’s Loopback0 interface.
  - Set the tunnel’s path option to dynamic.
  - Configure a static route for R2’s Loopback0 interface via the tunnel.
- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
interface Tunnel0
 ip unnumbered Loopback0
```

```
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip route 19.19.19.19 255.255.255.255 Tunnel0

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
```

```
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 2.2.2.2
 path-option 1 dynamic
!
router static
 address-family ipv4 unicast
  2.2.2.2/32 tunnel-te0
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
!
 interface GigabitEthernet0/1/0/0.619
!
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

In the previous examples, the MPLS TE tunnels of R2 and XR1 were advertised into the IGP process with the `autoroute announce` option. Because a TE tunnel is a unidirectional tunnel, there is no actual IGP adjacency that is established over it, but it can be used as a one-way link in the OSPF or IS-IS database. The alternative to this, as seen in this example, is to simply install a static route to the desired destination out the tunnel interface. All other verifications for this task are identical to the previous tasks, with the final result being that the customer traffic is routed over the TE tunnel in the core.

```
R2#show ip route 19.19.19.19
Routing entry for 19.19.19.19/32  Known via "static
", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:  * directly connected, via Tunnel0
      Route metric is 0, traffic share count is 1
RP/0/0/CPU0:XR1#show route 2.2.2.2
Wed Apr 4 23:28:14.285 UTC

Routing entry for 2.2.2.2/32  Known via "static
", distance 1, metric 0 (connected)
  Installed Apr  4 23:25:42.080 for 00:02:32
  Routing Descriptor Blocks    directly connected, via tunnel-te0

      Route metric is 0
  No advertising protos.
R1#traceroute 20.20.20.20

Type escape sequence to abort. Tracing the route to 20.20.20.20

  1 10.1.2.2 0 msec 4 msec 0 msec  2 20.2.4.4 [MPLS: Labels 16/16000 Exp 0]
 0 msec 4 msec 0 msec  3 20.4.6.6 [MPLS: Labels 16/16000 Exp 0]
 0 msec 0 msec 0 msec
  4 20.6.19.19 4 msec 4 msec 4 msec
  5 10.19.20.20 4 msec *  0 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
Wed Apr 4 23:28:34.162 UTC

Type escape sequence to abort. Tracing the route to 1.1.1.1

 1 10.19.20.19 6 msec  3 msec  3 msec  2 20.6.19.6 [MPLS: Labels 17/16 Exp 5]
 3 msec  4 msec  2 msec  3 20.3.6.3 [MPLS: Labels 16/16 Exp 5]
 2 msec  2 msec  2 msec  4 10.1.2.2 [MPLS: Label 16 Exp 5]
 1 msec  4 msec  2 msec
```

```
5 10.1.2.1 3 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.7 MPLS TE with Targeted LDP Adjacencies (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to R6 as follows:
  - Unnumber the tunnel to R2's Loopback0 interface.
  - Set the tunnel destination as R6's Loopback0 interface.
  - Set the tunnel's path option to explicitly follow the path from R2 to R3 to R4 to R5 to R6.
  - Configure a static route on R2 for XR1's Loopback0 interface via the TE tunnel to R6.
- Configure an MPLS TE tunnel from XR1 to R3 as follows:
  - Unnumber the tunnel to XR1's Loopback0 interface.
  - Set the tunnel destination as R3's Loopback0 interface.
  - Set the tunnel's path option to explicitly follow the path from XR1 to R6 to R5 to R4 to R3.
  - Configure a static route on XR1 for R2's Loopback0 interface via the TE tunnel to R3.
- Configure LDP in the core of the network as follows:
  - Enable LDP on the link between R2 and R3.
  - Enable LDP on the link between R6 and XR1.
  - Enable LDP on the MPLS TE tunnel from R2 to R6.
  - Enable LDP on the MPLS TE tunnel from XR1 to R3.
  - Configure R3 and R6 to accept target LDP sessions.

- When complete, the following reachability should be achieved:
  - R1 and XR2 should have full IP reachability to each other, and a traceroute should indicate that their L3VPN tunnel is transiting over the MPLS TE tunnels in the core of the SP network.

Configuration

```
R2:
mpls traffic-eng tunnels
!
ip explicit-path name TO_R6 enable
 next-address 3.3.3.3
 next-address 4.4.4.4
 next-address 5.5.5.5
 next-address 6.6.6.6
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name TO_R6
 mpls ip
!
interface FastEthernet0/0.23
 mpls ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip route 19.19.19.19 255.255.255.255 Tunnel0

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
```

```
 mpls ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
mpls ldp discovery targeted-hello accept

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
```

```
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
mpls ldp discovery targeted-hello accept

XR1:
explicit-path name TO_R3
```

```
 index 1 next-address strict ipv4 unicast 6.6.6.6
 index 2 next-address strict ipv4 unicast 5.5.5.5
 index 3 next-address strict ipv4 unicast 4.4.4.4
 index 4 next-address strict ipv4 unicast 3.3.3.3
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 3.3.3.3
 path-option 1 explicit name TO_R3
!
router static
 address-family ipv4 unicast
  2.2.2.2/32 tunnel-te0
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
 interface GigabitEthernet0/1/0/0.619
 !
 interface tunnel-te0
 !
```

Verification

All of the previous MPLS TE examples up to this point have shown tunnels always being built from PE to PE. TE Tunnels can also be built between two P routers, or between a PE router and a P router, as in this example. The advantage of doing P to P, PE to P, or P to PE tunneling is that you can have multiple levels of hierarchy in the network, where tunnels can sit inside of other tunnels. This is the same type of logic used in the Carrier Supporting Carrier (CSC) MPLS L3VPN design. Using P to P tunnels and the other variants also helps to limit highly meshed MPLS TE designs, because tunnels can terminate in a centralized point and then branch off from there. This design is sometimes called “tunnel stitching,” because you are essentially combining multiple tunnels together to make one seamless path through the core of the network.

The main caveat with the design shown in this example is that because L3VPN customers’ traffic is transiting over the MPLS TE tunnel, a targeted LDP adjacency is needed on top of the TE tunnel. This configuration is a common point of confusion for many people in MPLS TE design, so to make this clearer we’re going to look at the final working verification, and then work backward to see what happens when LDP is not enabled on the tunnel.

Like in other examples, the final verification is the transit between the final customer sites. What you should immediately notice about the output below, though, is that there is an additional label in the stack in the core of the Service Provider network.

```
R1#traceroute 20.20.20.20

 Type escape sequence to abort.
 Tracing the route to 20.20.20.20

   1 10.1.2.2 0 msec 4 msec 0 msec  2 20.2.3.3 [MPLS: Labels 27/20/16014
  Exp 0] 4 msec 4 msec 8 msec  3 20.3.4.4 [MPLS: Labels 17/20/16014
  Exp 0] 4 msec 4 msec 4 msec  4 20.4.5.5 [MPLS: Labels 17/20/16014
  Exp 0] 4 msec 8 msec 4 msec  5 20.5.6.6 [MPLS: Labels 20/16014
  Exp 0] 4 msec 4 msec 4 msec
   6 20.6.19.19 8 msec 4 msec 4 msec
   7 10.19.20.20 8 msec *  8 msec
 RP/0/3/CPU0:XR2#traceroute 1.1.1.1
 Thu Apr 5 00:41:17.507 UTC

 Type escape sequence to abort.
 Tracing the route to 1.1.1.1

  1 10.19.20.19 6 msec   5 msec  3 msec 2 20.6.19.6 [MPLS: Labels 26/16/16
  Exp 5] 7 msec  6 msec  6 msec 3 20.5.6.5 [MPLS: Labels 16/16/16
  Exp 5] 6 msec  7 msec  5 msec 4 20.4.5.4 [MPLS: Labels 16/16/16
  Exp 5] 6 msec  6 msec  7 msec 5 20.3.4.3 [MPLS: Labels 16/16
  Exp 5] 6 msec  6 msec  6 msec 6 10.1.2.2 [MPLS: Label 16
  Exp 5] 6 msec  6 msec  6 msec
  7 10.1.2.1 6 msec  *  6 msec
```

The bottom label of the stack, as usual, is the L3VPN label that was allocated by VPNv4 BGP. Specifically in this design, the PE router XR1 is allocating label value 16014 for the customer prefix 20.20.20.20/32, whereas PE router R2 is allocating the label value 16 for the customer prefix 1.1.1.1/32, as shown below.

```
R2#show bgp vpnv4 unicast all 20.20.20.20/32
BGP routing table entry for 100:1:20.20.20.20/32, version 23
Paths: (1 available, best #1, table VPN_A)
  Not advertised to any peer
  Local 19.19.19.19
 from 19.19.19.19 (19.19.19.19)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 mpls labels in/out nolabel/16014
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf VPN_A 1.1.1.1/32
Thu Apr 5 01:30:35.714 UTC
BGP routing table entry for 1.1.1.1/32, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  6           6
Last Modified: Apr  5 00:41:01.776 for 00:49:34
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Local 2.2.2.2
 from 2.2.2.2 (2.2.2.2) Received Label 16

      Origin IGP, metric 0, localpref 100, valid, internal, best, import-candidate, imported
      Extended community: RT:100:1
```

The next-hop values of the VPNv4 learned routes are the Loopback0 networks of XR1 and R2, respectively, just like the previous L3VPN designs. R2 and XR1 must now find a labeled path through the Service Provider core to reach each other's Loopbacks. This LSP will be the tunnel that hides the final customer prefix from the core of the network. To do this, they must find the next-hop on the global/default routing table and find the associated transport label. In this case, these next-hops are being statically routed via the TE tunnels to R6 and R3, respectively, as shown below.

```
R2#show ip route 19.19.19.19
Routing entry for 19.19.19.19/32  Known via " static
", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:  * directly connected, via Tunnel0
      Route metric is 0, traffic share count is 1
RP/0/0/CPU0:XR1#show route 2.2.2.2
```

```
Thu Apr  5 01:33:23.727 UTC

Routing entry for 2.2.2.2/32  Known via " static
", distance 1, metric 0 (connected)
  Installed Apr  5 00:41:01.677 for 00:52:22
  Routing Descriptor Blocks    directly connected, via tunnel-te0

      Route metric is 0
  No advertising protos.
```

A traceroute between these addresses of the PE routers indicates that they are following the LSP via the MPLS TE tunnel. However, there are two labels in the stack for traffic going over the tunnel, as shown below.

```
R2#traceroute 19.19.19.19

Type escape sequence to abort. Tracing the route to 19.19.19.19
  1 20.2.3.3 [MPLS: Labels 27/20
 Exp 0] 4 msec 8 msec 4 msec  2 20.3.4.4 [MPLS: Labels 17/20
 Exp 0] 4 msec 4 msec 4 msec  3 20.4.5.5 [MPLS: Labels 17/20
 Exp 0] 4 msec 4 msec 4 msec  4 20.5.6.6 [MPLS: Label 20
 Exp 0] 4 msec 4 msec 0 msec
  5 20.6.19.19 4 msec *  4 msec

RP/0/0/CPU0:XR1#traceroute 2.2.2.2
Thu Apr 5 01:34:51.475 UTC

Type escape sequence to abort. Tracing the route to 2.2.2.2
 1 20.6.19.6 [MPLS: Labels 26/16
 Exp 0] 8 msec  5 msec  4 msec 2 20.5.6.5 [MPLS: Labels 16/16
 Exp 0] 3 msec  5 msec  4 msec 3 20.4.5.4 [MPLS: Labels 16/16
 Exp 0] 4 msec  4 msec  3 msec 4 20.3.4.3 [MPLS: Label 16
 Exp 0] 3 msec  5 msec  3 msec
 5 20.2.3.2 3 msec  *  4 msec
```

R2 appears to be using a new VPN label on the bottom of the stack to reach the Loopback of XR1, whereas XR1 is using a new VPN label on the bottom of the stack to reach R2. There is more than one label here because, in addition to the RSVP allocated label for the MPLS TE tunnel, there is an LDP label that has been allocated for the Loopbacks of R2 and XR1. This is because LDP has been enabled on the TE tunnel itself, as shown below.

```
R2#show mpls interface
```

```
Interface              IP            Tunnel   BGP Static Operational
FastEthernet0/0.23     Yes (ldp)     Yes      No  No     Yes
FastEthernet0/0.24     No            Yes      No  No     Yes
Tunnel0                Yes           No       No  No
     Yes
RP/0/0/CPU0:XR1#show mpls interfaces
Thu Apr  5 01:37:07.321 UTC
Interface                  LDP      Tunnel   Enabled
-------------------------- -------- -------- --------tunnel-te0                 Yes      No       Yes


GigabitEthernet0/1/0/0.519 No       Yes      Yes
GigabitEthernet0/1/0/0.619 Yes      Yes      Yes
```

The TE tunnels though do not go directly between the PE routers. Instead, R2's tunnel terminates on the P router R6, and XR1's tunnel terminates on the P router R3. For LDP to work, these P routers must listen for multihop unicast LDP adjacency requests. This is what is considered the "targeted" LDP session. This is similar to an LDP session that is used for L2VPN applications such as AToM. This is where the `mpls ldp discovery targeted-hello accept` command comes in, which allows R3 and R6 to listen for the sessions. The targeted adjacencies can be seen below.

```
R3#show mpls ldp neighbor
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 3.3.3.3:0
        TCP connection: 2.2.2.2.646 - 3.3.3.3.37402
        State: Oper; Msgs sent/rcvd: 142/141; Downstream
        Up time: 01:49:11
        LDP discovery sources:
          FastEthernet0/0.23, Src IP addr: 20.2.3.2
        Addresses bound to peer LDP Ident:
          20.2.3.2        20.2.4.2        2.2.2.2 Peer LDP Ident: 19.19.19.19
:0; Local LDP Ident 3.3.3.3:0
        TCP connection: 19.19.19.19.44308 - 3.3.3.3.646
        State: Oper; Msgs sent/rcvd: 83/84; Downstream Up time: 00:57:30
        LDP discovery sources: Targeted Hello 3.3.3.3 -> 19.19.19.19
, passive
        Addresses bound to peer LDP Ident:
          19.19.19.19     20.5.19.19      20.6.19.19

R6#show mpls ldp neighbor
Peer LDP Ident: 2.2.2.2
:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 2.2.2.2.646 - 6.6.6.6.52117
        State: Oper; Msgs sent/rcvd: 142/141; Downstream Up time: 01:49:01
        LDP discovery sources: Targeted Hello 6.6.6.6 -> 2.2.2.2
, passive
```

```
        Addresses bound to peer LDP Ident:
          20.2.3.2        20.2.4.2        2.2.2.2
    Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 19.19.19.19.35458 - 6.6.6.6.646
        State: Oper; Msgs sent/rcvd: 86/84; Downstream
        Up time: 00:57:41
        LDP discovery sources:
          FastEthernet0/0.619, Src IP addr: 20.6.19.19
        Addresses bound to peer LDP Ident:
          19.19.19.19     20.5.19.19      20.6.19.19
```

Because LDP is running on the TE tunnels, and we have static routes pointing out the TE tunnels, it should mean that there are LDP labels associated with these destinations. These is where the second level of labels comes in, as shown below.

```
R2#show mpls forwarding-table
Local      Outgoing    Prefix           Bytes Label   Outgoing   Next Hop
Label      Label       or Tunnel Id     Switched      interface
16         No Label    1.1.1.1/32[V]    232320        Fa1/0      10.1.2.1
17         No Label    10.1.2.0/24[V]   200200        aggregate/VPN_A
18         Pop Label   3.3.3.3/32       0             Fa0/0.23   20.2.3.3
19         No Label    4.4.4.4/32       0             Fa0/0.24   20.2.4.4
20         No Label    5.5.5.5/32       0             Fa0/0.24   20.2.4.4
21         19          6.6.6.6/32       0             Fa0/0.23   20.2.3.3
           No Label    6.6.6.6/32       0             Fa0/0.24   20.2.4.4
22    [T]  20          19.19.19.19/32   0             Tu0        point2point
23         Pop Label   20.3.4.0/24      0             Fa0/0.23   20.2.3.3
           No Label    20.3.4.0/24      0             Fa0/0.24   20.2.4.4
24         Pop Label   20.3.6.0/24      0             Fa0/0.23   20.2.3.3
25         No Label    20.4.5.0/24      0             Fa0/0.24   20.2.4.4
26         No Label    20.4.6.0/24      0             Fa0/0.24   20.2.4.4
27         24          20.5.6.0/24      0             Fa0/0.23   20.2.3.3
           No Label    20.5.6.0/24      0             Fa0/0.24   20.2.4.4
28         No Label    20.5.19.0/24     0             Fa0/0.24   20.2.4.4
29         26          20.6.19.0/24     0             Fa0/0.23   20.2.3.3
           No Label    20.6.19.0/24     0             Fa0/0.24   20.2.4.4

[T] Forwarding through a LSP tunnel.
View additional labelling info with the 'detail' option

RP/0/0/CPU0:XR1#show mpls forwarding
Thu Apr  5 01:42:02.365 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
```

```
16001  Pop         6.6.6.6/32         Gi0/1/0/0.619 20.6.19.6       7482
16002  Unlabelled  5.5.5.5/32         Gi0/1/0/0.519 20.5.19.5       0
16003  Unlabelled  4.4.4.4/32         Gi0/1/0/0.519 20.5.19.5       0
       18          4.4.4.4/32         Gi0/1/0/0.619 20.6.19.6       0
16004  17          3.3.3.3/32         Gi0/1/0/0.619 20.6.19.6       34986
16005  Unlabelled  20.5.6.0/24        Gi0/1/0/0.519 20.5.19.5       0
       Pop         20.5.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16006  Pop         20.4.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16007  Unlabelled  20.4.5.0/24        Gi0/1/0/0.519 20.5.19.5       0
16008  Unlabelled  20.2.4.0/24        Gi0/1/0/0.519 20.5.19.5       0
       22          20.2.4.0/24        Gi0/1/0/0.619 20.6.19.6       0
16009  Pop         20.3.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16010  Unlabelled  20.3.4.0/24        Gi0/1/0/0.519 20.5.19.5       0
       23          20.3.4.0/24        Gi0/1/0/0.619 20.6.19.6       0
16011  21          20.2.3.0/24        Gi0/1/0/0.619 20.6.19.6       0
16012  16          2.2.2.2/32         tt0           point2point
      12074
16014  Aggregate   VPN_A: Per-VRF Aggr[V]   \
                                      VPN_A                         150
```

The outgoing label values 20 and 16 on R2 and XR1, respectively, are the LDP-bound labels for the Loopbacks of XR1 and R2, respectively, via the TE tunnel. This means that in addition to the RSVP-bound MPLS TE transport label, there is now the LDP-bound label that is acting like a VPN label. A debug of the data plane in the transit path of the Service Provider network further verifies this.

```
R4#debug mpls packet
Packet debugging is on
R5#debug mpls packet
Packet debugging is on
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R4# MPLS turbo: Fa0/0.34: rx: Len 130 Stack {17 0 253} {20 0 254} {16014 0 254}
- ipv4
data MPLS turbo: Fa0/0.45: tx: Len 130 Stack {17 0 252} {20 0 254} {16014 0 254}
- ipv4
data MPLS turbo: Fa0/0.45: rx: Len 130 Stack {16 5 252} {16 5 254} {16 5 254}
- ipv4
data
```

```
MPLS turbo: Fa0/0.34: tx: Len 126 Stack {16 5 251} {16 5 254}
- ipv4 data
<snip>

R5# MPLS turbo: Fa0/0.45: rx: Len 130 Stack {17 0 252} {20 0 254} {16014 0 254}
- ipv4
data MPLS turbo: Fa0/0.56: tx: Len 126 Stack {20 0 251} {16014 0 254}
- ipv4 data MPLS turbo: Fa0/0.56: rx: Len 130 Stack {16 5 253} {16 5 254} {16 5 254}
- ipv4
data MPLS turbo: Fa0/0.45: tx: Len 130 Stack {16 5 252} {16 5 254} {16 5 254}
- ipv4
data
<snip>
```

Based on the logical topology diagram, we know that R4 is the Penultimate Hop for R3, and R5 is the Penultimate Hop for R6. This is why the top label is being deposed when R4 forwards traffic toward R3, and when R5 forwards traffic toward R6. Verification of the MPLS LFIBs of R4 and R5 indicate that the topmost label numbers they are switching are the RSVP-derived transport labels for the MPLS TE tunnels, as shown below.

```
R4#show mpls forwarding-table
Local      Outgoing    Prefix           Bytes Label   Outgoing    Next Hop
Label      Label       or Tunnel Id     Switched      interface
16         Pop Label   19.19.19.19 0 [5]   \
                                        19668         Fa0/0.34    20.3.4.3
17         17          2.2.2.2 0 [1]    279010        Fa0/0.45    20.4.5.5
R5#show mpls forwarding-table
Local      Outgoing    Prefix           Bytes Label   Outgoing    Next Hop
Label      Label       or Tunnel Id     Switched      interface   16         16         19.19.19.19 0 [5]
   \                                           19694         Fa0/0.45    20.4.5.4
17         Pop Label   2.2.2.2 0 [1]    272512        Fa0/0.56    20.5.6.6
```

At this point, everything is working fine from the customer's point of view and in the core with both the MPLS TE and LDP labels. Now let's see what happens when LDP is removed from the TE tunnels in the core.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int tun0R2(config-if)#no mpls ip
R2(config-if)#end
R2# %LDP-5-NBRCHG: LDP Neighbor 6.6.6.6:0 (2) is DOWN (TE interface disabled targeted session)
```

```
R6#
%LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (2) is DOWN (Received error notification from
peer: Holddown time expired)

RP/0/0/CPU0:XR1#config t
Thu Apr  5 01:54:56.549 UTC
RP/0/0/CPU0:XR1(config)#mpls ldp RP/0/0/CPU0:XR1(config-ldp)#no  interface tunnel-te0

RP/0/0/CPU0:XR1(config-ldp)#commit
RP/0/0/CPU0:Apr 5 01:55:05.230 : config[65710]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xradmin'. Use 'show configuration commit changes
1000000278' to view the changes.
RP/0/0/CPU0:XR1(config-ldp)#end

R3#
%LDP-5-NBRCHG: LDP Neighbor 19.19.19.19:0 (1) is DOWN (Received error notification
from peer: Holddown time expired)
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1.....
Success rate is 0 percent (0/5)
```

Without LDP on the MPLS TE tunnels, transit between the customer sites is broken. To determine why, we must look back at the data plane debug and see the label stack that is now sent through the core.

```
R1#ping 20.20.20.20 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
R3#debug mpls packet

Packet debugging is on
R3# MPLS turbo: Fa0/0.23: rx: Len 126 Stack {27 0 254} {16014 0 254}
 - ipv4 data MPLS turbo: Fa0/0.34: tx: Len 126 Stack {17 0 253} {16014 0 254}
 - ipv4 data
<snip>
R4#debug mpls packet
```

```
Packet debugging is on
R4#MPLS turbo: Fa0/0.34: rx: Len 126 Stack {17 0 253} {16014 0 254}
 - ipv4 dataMPLS turbo: Fa0/0.45: tx: Len 126 Stack {17 0 252} {16014 0 254}
 - ipv4 data
<snip>
R5#debug mpls packet

Packet debugging is on
R5#MPLS turbo: Fa0/0.45: rx: Len 126 Stack {17 0 252} {16014 0 254
} - ipv4 dataMPLS turbo: Fa0/0.56: tx: Len 122 Stack {16014 0 251}
 - ipv4 data
<snip>
R6#debug mpls packet

Packet debugging is on
R6#MPLS turbo: Fa0/0.56: rx: Len 122 Stack {16014 0 251}
 - ipv4 data
<snip>
```

Traffic comes from R1 to R2, and R2 encapsulates it inside the TE tunnel. From here it is sent to R3 with a 2-label stack. R3 swaps the top label and forwards it to R4 with a 2-label stack. R4 swaps the top label and forwards it to R5 with a 2-label stack. R5 pops the top label, because it is the Penultimate Hop for R6, and forwards it to R6 with a single-label stack. R6 receives the labeled packets inbound, but appears to do nothing with them. R6 is blackholing the traffic, but why? The answer lies in the label value 16014 that R6 is receiving inbound from R5.

If we were to correlate this label value 16014 in R6's MPLS LFIB, the value does not exist, as seen below.

```
R6#show mpls forwarding-table

Local      Outgoing    Prefix           Bytes Label    Outgoing    Next Hop
Label      Label       or Tunnel Id     Switched       interface
16         No Label    2.2.2.2/32       7560           Fa0/0.36    20.3.6.3
           No Label    2.2.2.2/32       148            Fa0/0.46    20.4.6.4
17         No Label    3.3.3.3/32       59436          Fa0/0.36    20.3.6.3
18         No Label    4.4.4.4/32       0              Fa0/0.46    20.4.6.4
19         No Label    5.5.5.5/32       0              Fa0/0.56    20.5.6.5
20         Pop Label   19.19.19.19/32   19124          Fa0/0.619   20.6.19.19
21         No Label    20.2.3.0/24      0              Fa0/0.36    20.3.6.3
22         No Label    20.2.4.0/24      0              Fa0/0.46    20.4.6.4
23         No Label    20.3.4.0/24      0              Fa0/0.36    20.3.6.3
           No Label    20.3.4.0/24      0              Fa0/0.46    20.4.6.4
24         No Label    20.4.5.0/24      0              Fa0/0.46    20.4.6.4
```

```
             No Label   20.4.5.0/24     0             Fa0/0.56   20.5.6.5
25           Pop Label  20.5.19.0/24    0             Fa0/0.619  20.6.19.19
             No Label   20.5.19.0/24    0             Fa0/0.56   20.5.6.5
26           16         19.19.19.19 0 [5]  \
                                         21425        Fa0/0.56   20.5.6.5
```

Label 16014 is the VPNv4 BGP label value that XR1 allocated for the prefix 20.20.20.20/32, as seen below.

```
RP/0/0/CPU0:XR1#show mpls forwarding
Thu Apr  5 02:08:25.077 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- -----------
16001  Pop         6.6.6.6/32         Gi0/1/0/0.619 20.6.19.6       10662
16002  Unlabelled  5.5.5.5/32         Gi0/1/0/0.519 20.5.19.5       0
16003  Unlabelled  4.4.4.4/32         Gi0/1/0/0.519 20.5.19.5       0
       18          4.4.4.4/32         Gi0/1/0/0.619 20.6.19.6       0
16004  17          3.3.3.3/32         Gi0/1/0/0.619 20.6.19.6       42592
16005  Unlabelled  20.5.6.0/24        Gi0/1/0/0.519 20.5.19.5       0
       Pop         20.5.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16006  Pop         20.4.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16007  Unlabelled  20.4.5.0/24        Gi0/1/0/0.519 20.5.19.5       0
16008  Unlabelled  20.2.4.0/24        Gi0/1/0/0.519 20.5.19.5       0
       22          20.2.4.0/24        Gi0/1/0/0.619 20.6.19.6       0
16009  Pop         20.3.6.0/24        Gi0/1/0/0.619 20.6.19.6       0
16010  Unlabelled  20.3.4.0/24        Gi0/1/0/0.519 20.5.19.5       0
       23          20.3.4.0/24        Gi0/1/0/0.619 20.6.19.6       0
16011  21          20.2.3.0/24        Gi0/1/0/0.619 20.6.19.6       0
16012  Pop         2.2.2.2/32         tt0          point2point      1542
16014  Aggregate   VPN_A: Per-VRF Aggr[V]   \
                                         VPN_A
                    150
```

So why is R6 receiving a packet with a label value that only XR1 and R2 know about? Because the Penultimate Hop Popping (PHP) process is happening one hop too soon.

Without LDP on the MPLS TE tunnel interface, R2 is building the original label stack by imposing two labels, the VPNv4 BGP label that was allocated by XR1, and the MPLS TE label for R6 that was allocated by RSVP. When this label stack arrives at R5, R5 knows that it is the next-to-last hop for the TE tunnel. Based on this, R5 pops the top label off and forwards the packet onto R6, as seen below.

```
R1#ping 20.20.20.20 source 1.1.1.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
R5#debug mpls packet

Packet debugging is on
R5# MPLS turbo: Fa0/0.45: rx: Len 126 Stack {17 0 252} {16014 0 254}
- ipv4 data MPLS turbo: Fa0/0.56: tx: Len 122 Stack {16014 0 251}
- ipv4 data
<snip>
```

The problem with this, however, is that R5 is now exposing the VPNv4 label to R6, a P router that is not participating in the VPNv4 BGP topology. Therefore, to fix this problem, we need at least one additional level of labels in the stack. This additional label needs must a transport label that eventually gets the traffic to XR1 without exposing the final VPNv4 label. This is where LDP comes in. By running LDP over the TE tunnels, and by running LDP with the PE routers, the P routers that the TE tunnels terminate on will be able to direct traffic toward the proper egress point of the Service Provider network. When the traffic arrives at the final PE router, the final VPNv4 label will be exposed, and the traffic can forward on to the final customer.

An alternate solution to this design would have been to configure a TE tunnel from R6 to the Loopback of XR1, and a TE tunnel from R3 to the Loopback of R2; either of these solutions would result in traffic continuing to be labeled properly until it reached the final egress point of the network.

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.8 MPLS TE Fast Reroute (pending update)

- R2 and XR1 are preconfigured as PE routers for the MPLS L3VPN customer routers R1 and XR2, respectively, but the core of the Service Provider network is not running LDP.
- Configure the core of the Service Provider network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for the IS-IS Level 2 core.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces running IS-IS in the core.
- Configure an MPLS TE tunnel from R2 to XR1 as follows:
  - Unnumber the tunnel to R2’s Loopback0 interface.
  - Set the tunnel destination as XR1’s Loopback0 interface.
  - Set the tunnel’s path option to explicitly follow the path from R2 to R3 to R4 to R5 to XR1.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from XR1 to R2 as follows:
  - Unnumber the tunnel to XR1’s Loopback0 interface.
  - Set the tunnel destination as R2’s Loopback0 interface.
  - Set the tunnel’s path option to explicitly follow the path from XR1 to R5 to R6 to R3 to R2.
  - Configure Autoroute Announce on the tunnel so that the IS-IS core can use it for dynamic routing.
- Configure an MPLS TE tunnel from R4 to R5 for FRR as follows:
  - Unnumber the tunnel to R4’s Loopback0 interface.
  - Set the tunnel destination as R5’s Loopback0 interface.
  - Set the tunnel’s path option to explicitly avoid the link between R4 and R5.
  - Configure BFD signaling between R4 and R5 to detect a link failure between them in less than one second.
  - R2’s TE tunnel to XR1 should be Fast Rerouted if the link between R4 and

R5 is down.

- Configure an MPLS TE tunnel from R6 to R3 for FRR as follows:
  - Unnumber the tunnel to R6’s Loopback0 interface.
  - Set the tunnel destination as R3’s Loopback0 interface.
  - Set the tunnel’s path option to explicitly avoid the link between R3 and R6.
  - Configure BFD signaling between R3 and R6 to detect a link failure between them in less than one second.
  - XR1’s TE tunnel to R2 should be Fast Rerouted if the link between R3 and R6 is down.
- When complete, you should be able to perform the following verifications:
  - Traceroutes from R1 to XR2 should follow the R2 to R3 to R4 to R5 to XR1 path.
  - Remove VLAN 45 from SW1 to simulate a failure of the link between R4 and R5; immediately following this the traceroutes from R1 to XR2 should be Fast Rerouted via R6.
  - Traceroutes from XR2 to R1 should follow the XR1 to R5 to R6 to R3 to R1 path.
  - Remove VLAN 36 from SW1 to simulate a failure of the link between R3 and R6; immediately following this the traceroutes from XR2 to R1 should be Fast Rerouted via R4.

Configuration

```
R2:
mpls traffic-eng tunnels
!
ip explicit-path name TO_XR1 enable
 next-address 3.3.3.3
 next-address 4.4.4.4
 next-address 5.5.5.5
 next-address 19.19.19.19
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 19.19.19.19
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name TO_XR1
 tunnel mpls traffic-eng fast-reroute
!
interface FastEthernet0/0.23
```

```
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 bfd interval 50 min_rx 50 multiplier 3
 ip rsvp bandwidth
 ip rsvp signalling hello bfd
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip rsvp signalling hello bfd

R4:
mpls traffic-eng tunnels
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 5.5.5.5
 tunnel mpls traffic-eng path-option 1 explicit name AVOID_R4_R5_LINK
!
interface FastEthernet0/0.24
```

```
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 bfd interval 50 min_rx 50 multiplier 3
 ip rsvp bandwidth
 ip rsvp signalling hello bfd
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip rsvp signalling hello bfd
!
ip explicit-path name AVOID_R4_R5_LINK enable
 exclude-address 20.4.5.4
 exclude-address 20.4.5.5

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 bfd interval 50 min_rx 50 multiplier 3
 ip rsvp bandwidth
 ip rsvp signalling hello bfd
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
```

```
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip rsvp signalling hello bfd

R6:
mpls traffic-eng tunnels
!
interface Tunnel1
 ip unnumbered Loopback0 tunnel mode
 mpls traffic-eng tunnel destination 3.3.3.3
 tunnel mpls traffic-eng path-option 1 explicit name AVOID_R3_R6_LINK
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng backup-path Tunnel1
 bfd interval 50 min_rx 50 multiplier 3
 ip rsvp signalling hello bfd
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip rsvp signalling hello bfd
!
ip explicit-path name AVOID_R3_R6_LINK enable
 exclude-address 20.3.6.6
 exclude-address 20.3.6.3

XR1:
```

```
explicit-path name TO_R2
 index 1 next-address strict ipv4 unicast 5.5.5.5
 index 2 next-address strict ipv4 unicast 6.6.6.6
 index 3 next-address strict ipv4 unicast 3.3.3.3
 index 4 next-address strict ipv4 unicast 2.2.2.2
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 explicit name TO_R2
 fast-reroute
!
router isis 1
 address-family ipv4 unicast
 metric-style wide
 mpls traffic-eng level-2-only
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
mpls ldp
```

Verification

Prior to any failures in the network, traffic from R1 to XR2 follows the explicit route of the TE tunnel from R2 to XR1.

```
R1#traceroute 20.20.20.20



Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 4 msec 0 msec 0 msec
  2 20.2.3.3 [MPLS: Labels 16/16013 Exp 0] 0 msec 0 msec 4 msec
```

```
  3 20.3.4.4 [MPLS: Labels 17/16013 Exp 0] 0 msec 4 msec 0 msec
  4 20.4.5.5 [MPLS: Labels 16/16013 Exp 0] 4 msec 0 msec 4 msec
  5 20.5.19.19 0 msec 4 msec 4 msec
  6 10.19.20.20 4 msec *    4 msec
```

R2 requests FRR protection for this tunnel.

```
R2#show mpls traffic-eng tunnels protection

P2P TUNNELS:
R2_t0
  LSP Head, Tunnel0, Admin: up, Oper: up
  Src 2.2.2.2, Dest 19.19.19.19, Instance 24 Fast Reroute Protection: Requested

    Outbound: Unprotected: no backup tunnel assigned
      LSP signalling info:
        Original: out i/f: Fa0/0.23, label: 16, nhop: 20.2.3.3
                  nnhop: 4.4.4.4; nnhop rtr id: 4.4.4.4
  Path Protection: None
```

R4 and R5 are BFD adjacent. Note that the “client” protocol of BFD is Fast Reroute (FRR).

```
R4#show ip rsvp hello bfd nbr detail
  Hello Client Neighbors

  Remote addr 20.4.5.5, Local addr  20.4.5.4
    Type: Active
    I/F: Fa0/0.45 State: Up
nah (for 00:09:02) Clients: FRR

    LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
    Communication with neighbor lost: 0
```

SW1 deletes VLAN 45, which causes a loss of communication on the link between R4 and R5.

```
SW1#config t
Enter configuration commands, one per line. End with CNTL/Z.SW1(config)#no vlan 45

SW1(config)#
```

R4 detects that the BFD neighbor R5 is down, which triggers the FRR protection.

```
R4#show bfd neighbor


NeighAddr                         LD/RD    RH/RS    State    Int
20.4.5.5                           1/0     Down     Down     Fa0/0.45
```

The traceroute from R1 to XR2 now indicates that the path is being rerouted from R4 to R5 to R6. Note the additional label in the stack, which is required to tunnel the R4 to R5 traffic over R6.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

  1 10.1.2.2 0 msec 0 msec 0 msec
  2 20.2.3.3 [MPLS: Labels 16/16013 Exp 0] 4 msec 0 msec 4 msec
  3 20.3.4.4 [MPLS: Labels 17/16013 Exp 0] 0 msec 4 msec 0 msec
4 20.4.6.6 [MPLS: Labels 16/16/16013 Exp 0] 4 msec 0 msec 4 msec

  5 20.5.6.5 [MPLS: Labels 16/16013 Exp 0] 0 msec 4 msec 0 msec
  6 20.5.19.19 4 msec 4 msec 4 msec
  7 10.19.20.20 4 msec *  4 msec
```

In the reverse direction, the same occurs. XR2’s traceroute to R1 follows XR1’s TE tunnel’s explicit path.

```
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Wed May 2 15:54:24.188 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 6 msec   28 msec 32 msec
 2 20.5.19.5 [MPLS: Labels 17/16 Exp 5] 11 msec  5 msec  3 msec
 3 20.5.6.6 [MPLS: Labels 17/16 Exp 5] 3 msec  3 msec  3 msec
 4 20.3.6.3 [MPLS: Labels 17/16 Exp 5] 4 msec  4 msec  3 msec
 5 10.1.2.2 [MPLS: Label 16 Exp 5] 3 msec  3 msec  2 msec
 6 10.1.2.1 3 msec  *  3 msec
```

XR1 has requested that this tunnel be FRR protected.

```
RP/0/0/CPU0:XR1#show mpls traffic-eng tunnels protection
Wed May 2 15:53:40.511 UTC
R2_t0 Tunnel Id: 0
  LSP Tail, signaled, connection up
  Src: 2.2.2.2, Dest: 19.19.19.19, Instance: 24
  Fast Reroute Protection: Requested
    Inbound: FRR Inactive
     LSP signalling info:
      Original: in i/f: GigabitEthernet0/1/0/0.519, label: 3, phop: 20.5.19.5

XR1_t0 Tunnel Id: 0
  LSP Head, Admin: up, Oper: up
  Src: 19.19.19.19, Dest: 2.2.2.2, Instance: 2 Fast Reroute Protection: Requested

    Outbound: FRR Inactive
     LSP signalling info:
      Original: out i/f: GigabitEthernet0/1/0/0.519, label: 17, nhop: 20.5.19.5
```

R3 and R6 are BFD adjacent, and R6 has registered this adjacency with the FRR process.

```
R6#show ip rsvp hello bfd nbr detail
  Hello Client Neighbors

  Remote addr 20.3.6.3, Local addr  20.3.6.6
    Type: Active
    I/F: Fa0/0.36
```

```
State: Up (for 00:06:38)
 Clients: FRR

    LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
    Communication with neighbor lost: 0
```

SW1 deletes VLAN 36, which causes communication to be lost between R3 and R6.

```
SW1#config t
Enter configuration commands, one per line. End with CNTL/Z.SW1(config)#no vlan 36

SW1(config)#
```

When R6 loses the BFD neighbor R3, the FRR process is triggered.

```
R6#show ip rsvp hello bfd nbr

  Client  Neighbor        I/F          State      LostCnt    LSPs
None    20.3.6.3        Fa0/0.36      Lost              1        0
```

The traceroute from XR2 to R1 now indicates that the tunnel is being rerouted via R4. Again, note the additional label in the stack that is needed for the FRR tunnel between R6 and R3.

```
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Wed May  2 15:55:13.438 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 1 10.19.20.19 5 msec  4 msec  3 msec
 2 20.5.19.5 [MPLS: Labels 17/16 Exp 5] 4 msec  5 msec  5 msec
 3 20.5.6.6 [MPLS: Labels 17/16 Exp 5] 4 msec  4 msec  3 msec
 4 20.4.6.4 [MPLS: Labels 16/17/16 Exp 5] 3 msec  4 msec  3 msec
 5 20.3.4.3 [MPLS: Labels 17/16 Exp 5] 4 msec  11 msec  29 msec
 6 10.1.2.2 [MPLS: Label 16 Exp 5] 31 msec  3 msec  3 msec
 7 10.1.2.1 4 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.9 Inter-Area MPLS TE with OSPF (pending update)

- Configure OSPFv2 routing in the network as follows:
  - Area 0 consists of links interconnecting R3 & R4, R3 & R6, R4 & R6, R4 & R5, and R5 & R6.
  - Area 1 consists of links interconnecting R1 & R1, R2 & R3, and R2 & R4.
  - Area 2 consists of links interconnecting XR1 & R5, XR1 & R6, and XR1 & XR2.
  - Advertise the Loopback interfaces of R3, R4, R5, and R6 into Area 0.
  - Advertise the Loopback interfaces of R1 and R2 into Area 1.
  - Advertise the Loopback interfaces of XR1 and XR2 into Area 2.
- Configure the network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for OSPF Area 0, Area 1, and Area 2.
  - Set the OSPF MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces.
- Configure an MPLS TE tunnel from R1 to XR2 as follows:
  - Unnumber the tunnel to R1’s Loopback0 interface.
  - Set the tunnel destination as XR2’s Loopback0 interface.
  - Configure the tunnel’s explicit path option to use loose next-hops as follows:
    - Traffic from Area 1 to Area 0 should use R3 as the ABR.
    - Traffic from Area 0 to Area 2 should use R5 as the ABR.
  - Configure Autoroute Destination so that R1 uses the tunnel to route toward XR2’s Loopback0.
- Configure an MPLS TE tunnel from XR2 to R1 as follows:
  - Unnumber the tunnel to XR2’s Loopback0 interface.
  - Set the tunnel destination as R1’s Loopback0 interface.
  - Configure the tunnel’s explicit path option to use loose next-hops as follows:
    - Traffic from Area 2 to Area 0 should use R6 as the ABR.
    - Traffic from Area 0 to Area 1 should use R4 as the ABR.
  - Configure static routing so that XR2 uses the tunnel to route toward R1’s Loopback0.

Configuration

```
R1:
mpls traffic-eng tunnels
!
ip explicit-path name INTER_AREA_TE enable
 next-address loose 3.3.3.3
 next-address loose 5.5.5.5
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 20.20.20.20
 tunnel mpls traffic-eng autoroute destination
 tunnel mpls traffic-eng path-option 10 explicit name INTER_AREA_TE
!
interface Loopback0
 ip ospf 1 area 1
!
interface FastEthernet0/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth ip ospf 1 area 1
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1

R2:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 1
!
interface FastEthernet1/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 1
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 1
!
```

```
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 1
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1

R3:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 1
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 1

R4:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 1
!
```

```
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 1

R5:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 2
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 2
```

```
R6:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 2
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 2

XR1:
router ospf 1
 area 2
  mpls traffic-eng
  interface Loopback0
  !
  interface GigabitEthernet0/1/0/0.519
  !
  interface GigabitEthernet0/1/0/0.619
  !
  interface POS0/6/0/0
  !
 !
 mpls traffic-eng router-id Loopback0
!
```

```
rsvp
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls ldp

XR2:
explicit-path name INTER_AREA_TE
 index 1 next-address loose ipv4 unicast 6.6.6.6
 index 2 next-address loose ipv4 unicast 4.4.4.4
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 1.1.1.1
 path-option 10 explicit name INTER_AREA_TE
!
router static
 address-family ipv4 unicast
  1.1.1.1/32 tunnel-te0
 !
!
router ospf 1
 area 2
  mpls traffic-eng
  interface Loopback0
  !
  interface POS0/7/0/0
  !
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
```

```
 interface POS0/7/0/0
  !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/7/0/0
  !
!
mpls ldp
```

Verification

In the previous MPLS Traffic Engineering examples, all nodes in the path from the Head End to the Tail End were in the same link state flooding domain. In the case of OSPF this is the area, and in the case of IS-IS it is the level. This means that each node along the path has full visibility of the entire link state topology end-to-end. MPLS TE then uses this topology information to calculate the Constrained Shortest Path First (cSPF), which can contain other attributes like the TE metric, affinity bits, bandwidth availability, etc. The key point though is that for the cSPF calculation to be successful, the source and destination nodes must be in the same link state flooding domain so a full shortest path tree can be built.

Running MPLS TE between areas or between ASes breaks this logic, because devices in different link state flooding domains (OSPF areas or IS-IS levels) cannot run a full SPF calculation on each other to build an SPT. Instead for Inter-Area routing, the Area Border Router for OSPF or Level-1/Level-2 router for IS-IS is used as a trusted exit point out toward the next area/level. Therefore, to configure MPLS TE between areas or levels, there must be a way to calculate the topology beyond the head end router's visibility into other link state areas or levels. Possible workarounds for this design problem of Inter-Area MPLS TE are explored in RFC 4105, Requirements for Inter-Area MPLS Traffic Engineering.

Specifically, the way that Cisco IOS and IOS XR implement Inter-Area MPLS TE is with the definition of an Explicit Route Object (ERO)—that is, an explicit-path—that contains the addresses of the Area Border Routers (or L1/L2 routers in the case of IS-IS) as loose hops in the path. The result of this is a pseudo-dynamic path calculation in which the Head End of the MPLS TE tunnel dynamically calculates the cSPF to their exit ABR, that ABR dynamically calculates the exit path to the next ABR, and so on until the final tail end of the tunnel is reached. This is accomplished through expansion of the loose hops into a fully defined explicit path, in which the tunnel Head End and ABRs explicitly define the hops that are only within their own local flooding domain.

From a configuration point of view, there are only two changes in this example, as compared to previous ones. The first is that the OSPF ABRs have MPLS Traffic Engineering enabled both for Area 0 and their non-transit Area (Areas 1 and 2 in this case), and the tunnel Head End has the explicit path defined with the loose hops, as seen below:

```
R1#show run | s explicit
 tunnel mpls traffic-eng path-option 10 explicit name hops ip explicit-path name INTER_AREA_TE enable
next-address loose 3.3.3.3
next-address loose 5.5.5.5
R3#sh run | s router ospf
router ospf 1
 log-adjacency-changes
 mpls traffic-eng router-id Loopback0 mpls traffic-eng area 0
mpls traffic-eng area 1
```

When the tunnels are initialized, path calculation to the first exit ABR occurs, intra-area signaling occurs to the first exit ABR, path calculation from the first ABR to the second ABR occurs, intra-area signaling occurs to the second ABR, and so on until the path is fully expanded. This process can be verified with the debug outputs shown below:

```
R1#debug mpls traffic-eng path lookup

MPLS traffic-eng path lookup events debugging is onR1#debug mpls traffic-eng tunnels signalling

MPLS traffic-eng tunnels signalling debugging is on
R3#debug mpls traffic-eng path lookup

MPLS traffic-eng path lookup events debugging is on
R2#R3#debug mpls traffic-eng tunnels signalling

MPLS traffic-eng tunnels signalling debugging is on
```

These debugs are enabled on all devices in the transit path. Next, R1 activates its tunnel, which causes path calculation and setup to occur.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int tunnel0R1(config-if)#no shut
R1(config-if)#TE-PCALC-API: 1.1.1.1_7->20.20.20.20_0 {7}: P2P LSP Path Lookup called
TE-PCALC: 1.1.1.1_7->20.20.20.20_0 {7}: Path Request Info
  Flags:  IP_EXPLICIT_PATH  METRIC_TE IP explicit-path: Supplied
   3.3.3.3 Loose
   5.5.5.5 Loose
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xFFFF
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: Area (ospf 1  area 1) Path Lookup
begin
TE-PCALC-PATH: Area (ospf 1 area 1): Dest ip addr 20.20.20.20 not found
TE-PCALC-PATH: lsr_exists:first Loose Hop is to addr 3.3.3.3
Path from 1.1.1.1 -> 3.3.3.3:
  20.2.3.3->0.0.0.0 (admin_weight=2):
  20.2.3.2->0.0.0.0 (admin_weight=2):
  10.1.2.2->0.0.0.0 (admin_weight=1):
  10.1.2.1->0.0.0.0 (admin_weight=1):
  num_hops 5, accumlated_aw 2, min_bw 75000
TE-PCALC: Verify Path Lookup: 1.1.1.1_7->20.20.20.20_0 {7}: (   area nil)
  Flags:  METRIC_TE
  Last Strict Router: 3.3.3.3
  sub-lsp weight:0 (Total LSP weight:2)  Hop List:
   10.1.2.1
   10.1.2.2
   20.2.3.2
```

```
  20.2.3.3

   3.3.3.3
  5.5.5.5 Loose
TE-PCALC-VERIFY: VERIFY to 3.3.3.3 BEGIN:
TE-PCALC-VERIFY: Verify:
TE-PCALC-VERIFY:  1.1.1.1, 10.1.2.1 points to
TE-PCALC-VERIFY:  2.2.2.2, 10.1.2.2
TE-PCALC-VERIFY: Verify:
TE-PCALC-VERIFY:  2.2.2.2, 20.2.3.2 points to
TE-PCALC-VERIFY:  3.3.3.3, 20.2.3.3
TE-PCALC-VERIFY: VERIFY to 3.3.3.3 PASSED
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: Area (ospf 1  area 1) Path Lookup end:
path found
TE-PCALC-API: 1.1.1.1_7->20.20.20.20_0 {7}: P2P LSP Path Lookup result: success
TE-SIG-HE: Tunnel0 [7]->20.20.20.20: RSVP head-end open
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: path next hop is 10.1.2.2 (Fa0/0)
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: sending ADD RESV reply
TE-SIG-HE: Tunnel0 [7]->20.20.20.20: received RESV CREATE
TE-SIG-HE: Tunnel0 [7]->20.20.20.20: notified of new label information
          FastEthernet0/0, nhop 10.1.2.2, frame, 16

TE-SIG-HE: Tunnel0 [7]->20.20.20.20: label information Changed
TE-SIG-HE: Tunnel0: route change: FastEthernet0/0:17->FastEthernet0/0:16
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
upR1(config-if)#
```

R1 exists in OSPF Area 1 with R2, R3, and R4. The ERO (explicit path) requests that 3.3.3.3 (R3) be the first exit ABR. R1 dynamically expands the loose route to 3.3.3.3 to the explicit path of 10.1.2.1 to 10.1.2.2 to 20.2.3.2 to 20.2.3.3 to 3.3.3.3. It knows that 5.5.5.5 is beyond R3, so it requests that R3 further expand the path toward the next ABR.

```
R3#
TE-PCALC-API: 1.1.1.1_7->5.5.5.5_0 {7}: LSP Path Expand called
TE-PCALC: 1.1.1.1_7->5.5.5.5_0 {7}: Path Request Info
  Flags:    END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 1.1.1.1_7->5.5.5.5_0 {7}: rrr_pcalc_lsr_expand:  Exclude node:
2.2.2.2 (intf: 20.2.3.2)
TE-PCALC-PATH: 1.1.1.1_7->5.5.5.5_0 {7}: rrr_pcalc_lsr_expand:  Exclude node:
```

```
1.1.1.1 (intf: 10.1.2.1)
TE-PCALC-PATH: 1.1.1.1_7->5.5.5.5_0 {7}: Area (ospf 1   area 0) Path Lookup begin
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known! Path from 3.3.3.3 -> 5.5.5.5:
  20.4.5.5->0.0.0.0 (admin_weight=2):
  20.4.5.4->0.0.0.0 (admin_weight=2):
  20.3.4.4->0.0.0.0 (admin_weight=1):
  20.3.4.3->0.0.0.0 (admin_weight=1):
  num_hops 5, accumlated_aw 2, min_bw 75000
TE-PCALC-PATH: 3.3.3.3_7->5.5.5.5_0 {7}: Area (ospf 1 area 0) Path Lookup end:
path found
5.5.5.5 expands to:
20.3.4.3
20.3.4.4
20.4.5.4
20.4.5.5
5.5.5.5
TE-PCALC-API: 3.3.3.3_7->5.5.5.5_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: path previous hop is 20.2.3.2 (Fa0/0.23)
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: path next hop is 20.3.4.4 (Fa0/0.34)
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: sending ADD RESV reply
```

R3 received the request from R1 to expand the path to 5.5.5.5. Because R3 is in OSPF Area 0 with 5.5.5.5 (R5), a cSPF calculation can be performed, and the SPT expands to 20.3.4.3 to 20.3.4.4 to 20.4.5.4 to 20.4.5.5 to 5.5.5.5. R3 then asks 5.5.5.5 (R5) to further expand the path to the final destination.

```
R5#
TE-PCALC-API: 1.1.1.1_7->20.20.20.20_0 {7}: LSP Path Expand called

TE-PCALC: 1.1.1.1_7->20.20.20.20_0 {7}: Path Request Info
  Flags:    END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand:  Exclude node: 4.4.4.4 (intf: 20.4.5.4)
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand:  Exclude node: 3.3.3.3 (intf: 20.3.4.3)
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand: Can't get router ID addr for 20.2.3.2
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand: Can't get router ID addr for 10.1.2.1
TE-PCALC-PATH: 1.1.1.1_7->20.20.20.20_0 {7}: Area (ospf 1 area 2) Path Lookup
begin
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
```

```
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known! Path from 5.5.5.5 -> 20.20.20.20:
  10.19.20.19->10.19.20.20 (admin_weight=2):
  20.5.19.19->0.0.0.0 (admin_weight=1):
  20.5.19.5->0.0.0.0 (admin_weight=1):
  num_hops 4, accumlated_aw 2, min_bw 0
TE-PCALC-PATH: 5.5.5.5_7->20.20.20.20_0 {7}: Area (ospf 1 area 2) Path Lookup end:
path found
20.20.20.20 expands to:
20.5.19.5
20.5.19.19
10.19.20.20
20.20.20.20
TE-PCALC-API: 5.5.5.5_7->20.20.20.20_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: path previous hop is 20.4.5.4 (Fa0/0.45)
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: path next hop is 20.5.19.19 (Fa0/0.519)
TE-SIG-LM: 1.1.1.1_7->20.20.20.20_0 {7}: sending ADD RESV reply
```

R5 receives the request from 3.3.3.3 (R3) to expand the path to 20.20.20.20 (XR2, the tunnel Tail End). Because R5 is in the same Area as XR2, the expansion succeeds and the path is expanded to 20.5.19.5 to 20.5.19.19 to 10.19.20.20 to 20.20.20.20. The end result is that the tunnel is properly signaled end to end, and traffic routes over the TE tunnel as seen below:

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
  1 10.1.2.2 [MPLS: Label 16 Exp 0]
 0 msec 4 msec 0 msec   2 20.2.3.3 [MPLS: Label 17 Exp 0]
 4 msec 0 msec 0 msec   3 20.3.4.4 [MPLS: Label 31 Exp 0]
 0 msec 0 msec 4 msec   4 20.4.5.5 [MPLS: Label 17 Exp 0]
 0 msec 4 msec 0 msec   5 20.5.19.19 [MPLS: Label 16015 Exp 0]
 4 msec 0 msec 0 msec
  6 10.19.20.20 4 msec *  4 msec
```

One additional option that is used on the tunnel on R1 in this case is the `autoroute destination` command. This command simply takes the place of configuring a static route to the tunnel destination out the tunnel. The output in the routing table shows the destination as reachable via static, but there is no static `ip route` statement manually configured on R1.

```
R1#show run | include ip route R1#show ip route 20.20.20.20
Routing entry for 20.20.20.20/32 Known via "static"
, distance 1, metric 0 (connected)
  Routing Descriptor Blocks:   * directly connected, via Tunnel0

      Route metric is 0, traffic share count is 1
```

The tunnel from XR2 back to R1 will have the same logical result. XR2 dynamically calculates the path to the first ABR R6 and asks R6 to expand the path.

```
RP/0/3/CPU0:XR2#config t
Thu Jun 28 18:13:24.389 UTC
RP/0/3/CPU0:XR2(config)#int tunnel-te0 RP/0/3/CPU0:XR2(config-if)#no shut

RP/0/3/CPU0:XR2(config-if)#commit
R6#

TE-PCALC-API: 20.20.20.20_4->4.4.4.4_0 {7}: LSP Path Expand called TE-
PCALC: 20.20.20.20_4->4.4.4.4_0 {7}: Path Request Info
  Flags:  END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0

TE-PCALC-PATH: 20.20.20.20_4->4.4.4.4_0 {7}: Area (ospf 1   area 0) Path Lookup
begin
Path from 6.6.6.6 -> 4.4.4.4:
  20.4.6.4->0.0.0.0 (admin_weight=1):
  20.4.6.6->0.0.0.0 (admin_weight=1):
  num_hops 3, accumlated_aw 1, min_bw 75000
TE-PCALC-PATH: 6.6.6.6_4->4.4.4.4_0 {7}: Area (ospf 1 area 0) Path Lookup end:
path found
4.4.4.4 expands to:
20.4.6.6
20.4.6.4
4.4.4.4
TE-PCALC-API: 6.6.6.6_4->4.4.4.4_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: received ADD RESV request
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path previous hop is 20.6.19.19
(Fa0/0.619)
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path next hop is 20.4.6.4 (Fa0/0.46)
```

```
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: sending ADD RESV reply
```

R6 expands the path and asks the next ABR (R4) to continue to expand the path.

```
R4#
TE-PCALC-API: 20.20.20.20_4->1.1.1.1_0 {7}: LSP Path Expand called TE-
PCALC: 20.20.20.20_4->1.1.1.1_0 {7}: Path Request Info
  Flags:  END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 20.20.20.20_4->1.1.1.1_0 {7}: Area (ospf 1   area 1) Path Lookup
begin
Path from 4.4.4.4 -> 1.1.1.1:
  10.1.2.1 ->0.0.0.0 (admin_weight=2):
  10.1.2.2 ->0.0.0.0 (admin_weight=2):
  20.2.4.2->0.0.0.0 (admin_weight=1):
  20.2.4.4->0.0.0.0 (admin_weight=1):
  num_hops 5, accumlated_aw 2, min_bw 75000
TE-PCALC-PATH: 4.4.4.4_4->1.1.1.1_0 {7}: Area (ospf 1 area 1) Path Lookup end:
path found
1.1.1.1 expands to:
20.2.4.4
20.2.4.2
10.1.2.2
10.1.2.1
1.1.1.1
TE-PCALC-API: 4.4.4.4_4->1.1.1.1_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: received ADD RESV request
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path previous hop is 20.4.6.6 (Fa0/0.46)
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path next hop is 20.2.4.2 (Fa0/0.24)
TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: sending ADD RESV reply
```

R4 expands the path to the final destination, and now the tunnel is signaled end to end. Traffic from XR2 to R1 must now follow R6 and R4 in the path, but the individual calculations up to these routers are dynamic.

```
RP/0/3/CPU0:XR2#traceroute 1.1.1.1

Thu Jun 28 18:16:07.659 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1
```

```
1 10.19.20.19 [MPLS: Label 16016 Exp 0] 8 msec  6 msec  4 msec
2 20.6.19.6 [MPLS: Label 16 Exp 0] 3 msec  4 msec  2 msec
3 20.4.6.4 [MPLS: Label 30 Exp 0] 3 msec  3 msec  2 msec
4 20.2.4.2 [MPLS: Label 17 Exp 0] 3 msec  3 msec  2 msec
5 10.1.2.1 2 msec *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.10 Inter-Area MPLS TE with IS-IS (pending update)

- Configure IS-IS routing in the network as follows:
  - R1, R2, R3, and R4 should use NET address 00.0000.0000.000Y.00, where Y is the router number.
  - R5, R6, XR1, and XR2 should use NET address 01.0000.0000.000Y.00, where Y is the router number; for XR1 use 19, and for XR2 use 20.
  - Level-2 consists of links interconnecting R3 & R4, R3 & R6, R4 & R6, R4 & R5, R5 & R6, and all their Loopback0 interfaces.
  - Level-1 consists of all other links and Loopbacks.
- Configure the network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for IS-IS Level-1 and Level-2.
  - Set the IS-IS MPLS TE Router-ID to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces.
- Configure an MPLS TE tunnel from R1 to XR2 as follows:
  - Unnumber the tunnel to R1’s Loopback0 interface.
  - Set the tunnel destination as XR2’s Loopback0 interface.
  - Configure the tunnel’s explicit path option to use loose next-hops as follows:
    - R1 should use R3 as the L1/L2 router.
    - R3 should use R6 as the next L1/L2 router.
  - Configure Autoroute Destination so that R1 uses the tunnel to route toward XR2’s Loopback0.
- Configure an MPLS TE tunnel from XR2 to R1 as follows:
  - Unnumber the tunnel to XR2’s Loopback0 interface.
  - Set the tunnel destination as R1’s Loopback0 interface.
  - Configure the tunnel’s explicit path option to use loose next-hops as follows:
    - XR2 should use R5 as the L1/L2 router.
    - R5 should use R4 as the next L1/L2 router.
  - Configure static routing so that XR2 uses the tunnel to route toward R1’s Loopback0.

Configuration

```
R1:
mpls traffic-eng tunnels
!
ip explicit-path name INTER_AREA_TE enable
 next-address loose 3.3.3.3
 next-address loose 6.6.6.6
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 20.20.20.20
 tunnel mpls traffic-eng autoroute destination
 tunnel mpls traffic-eng path-option 10 explicit name INTER_AREA_TE
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-1
!
interface FastEthernet0/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
router isis 1
 net 00.0000.0000.0001.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

R2:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-1
!
interface FastEthernet1/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
```

```
 isis circuit-type level-1
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
router isis 1
 net 00.0000.0000.0002.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

R3:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
router isis 1
```

```
 net 00.0000.0000.0003.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 mpls traffic-eng level-1

R4:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
router isis 1
 net 00.0000.0000.0004.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 mpls traffic-eng level-1

R5:
mpls traffic-eng tunnels
```

```
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
router isis 1
 net 01.0000.0000.0005.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 mpls traffic-eng level-1

R6:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
```

```
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-2
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
 isis circuit-type level-1
!
router isis 1
 net 01.0000.0000.0006.00
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 mpls traffic-eng level-1

XR1:
router isis 1
 net 01.0000.0000.0019.00
 is-type level-1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-1
 !
 interface Loopback0
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/1/0/0.519
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/1/0/0.619
  address-family ipv4 unicast
  !
 !
 interface POS0/6/0/0
  address-family ipv4 unicast
  !
 !
```

```
!
rsvp
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls ldp

XR2:
explicit-path name INTER_AREA_TE
 index 1 next-address loose ipv4 unicast 5.5.5.5
 index 2 next-address loose ipv4 unicast 4.4.4.4
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 1.1.1.1
 path-option 10 explicit name INTER_AREA_TE
!
router static
 address-family ipv4 unicast
  1.1.1.1/32 tunnel-te0
 !
!
router isis 1
 net 01.0000.0000.0020.00
 is-type level-1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-1
 !
 interface Loopback0
  address-family ipv4 unicast
  !
```

```
 !
 interface POS0/7/0/0
  address-family ipv4 unicast
  !
 !
!
rsvp
 interface POS0/7/0/0
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/7/0/0
!
mpls ldp
```

Verification

This section is very similar to the previous Inter-Area MPLS TE example, except that the IGP used is IS-IS instead of OSPF. As with OSPF, IS-IS MPLS TE normally requires that the Head End and Tail End of the TE tunnel be in the same flooding domain (same IS-IS level); otherwise a full cSPF run cannot be completed and the cSPT cannot be formed. The workaround is to specify the L1/L2 routers (like the OSPF ABRs) as loose hops in an explicit path. When the signaling is sent to the L1/L2 routes, they will calculate a dynamic path to the next L1/L2 router and expand the path into a full explicit path to be used for the purposes of TE.

As in the previous example, the best verification for this is the output of `debug mpls traffic- eng path lookup` and `debug mpls traffic-eng tunnel signalling`, as seen below.

```
R1#debug mpls traffic-eng tunnels signalling
MPLS traffic-eng tunnels signalling debugging is onR1#debug mpls traffic-eng path lookup
MPLS traffic-eng path lookup events debugging is on
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int tun0R1(config-if)#no shut
R1(config-if)#TE-PCALC-API: 1.1.1.1_56->20.20.20.20_0 {7}: P2P LSP Path Lookup called
TE-PCALC: 1.1.1.1_56->20.20.20.20_0 {7}: Path Request Info
  Flags:  IP_EXPLICIT_PATH  METRIC_TE
  IP explicit-path: Supplied
    3.3.3.3 Loose
    6.6.6.6 Loose
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
```

```
  affinity_bits 0x0, affinity_mask 0xFFFF
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: Area (isis    level-1) Path Lookup
begin
TE-PCALC-PATH: Area (isis  level-1): Dest ip addr 20.20.20.20 not found
TE-PCALC-PATH: lsr_exists:first Loose Hop is to addr 3.3.3.3
Path from 0000.0000.0001.00 -> 0000.0000.0003.00:
  20.2.3.3->0.0.0.0 (admin_weight=20):
  20.2.3.2->0.0.0.0 (admin_weight=20):
  10.1.2.2->0.0.0.0 (admin_weight=10):
  10.1.2.1->0.0.0.0 (admin_weight=10):
  num_hops 5, accumlated_aw 20, min_bw 75000
TE-PCALC: Verify Path Lookup: 1.1.1.1_56->20.20.20.20_0 {7}: ( area nil)

  Flags:    METRIC_TE
  Last Strict Router: 3.3.3.3
  sub-lsp weight:0 (Total LSP weight:20) Hop List:
   10.1.2.1
   10.1.2.2
   20.2.3.2
   20.2.3.3
   3.3.3.3
   6.6.6.6 Loose
TE-PCALC-VERIFY: VERIFY to 3.3.3.3 BEGIN:
TE-PCALC-VERIFY: Verify:
TE-PCALC-VERIFY:  0000.0000.0001.00, 10.1.2.1 points to
TE-PCALC-VERIFY:  0000.0000.0002.00, 10.1.2.2
TE-PCALC-VERIFY: Verify:
TE-PCALC-VERIFY:  0000.0000.0002.00, 20.2.3.2 points to
TE-PCALC-VERIFY:  0000.0000.0003.00, 20.2.3.3
TE-PCALC-VERIFY: VERIFY to 3.3.3.3 PASSED
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: Area (isis  level-1) Path Lookup end:
path found
TE-PCALC-API: 1.1.1.1_56->20.20.20.20_0 {7}: P2P LSP Path Lookup result: success
TE-SIG-HE: Tunnel0 [56]->20.20.20.20: RSVP head-end open
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: path next hop is 10.1.2.2 (Fa0/0)
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: sending ADD RESV reply
TE-SIG-HE: Tunnel0 [56]->20.20.20.20: received RESV CREATE
TE-SIG-HE: Tunnel0 [56]->20.20.20.20: notified of new label information
        FastEthernet0/0, nhop 10.1.2.2, frame, 17

TE-SIG-HE: Tunnel0 [56]->20.20.20.20: label information Changed
TE-SIG-HE: Tunnel0: route change: FastEthernet0/0:18->FastEthernet0/0:17
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

R1 initializes its tunnel and calculates a dynamic path to the first loose hop, 3.3.3.3 (R3). The expansion of this path is from R1 to R2 to R3. R1 then asks R3 to further expand the path to the next loose hop, 6.6.6.6 (R6).

```
R3#
TE-PCALC-API: 1.1.1.1_56->6.6.6.6_0 {7}: LSP Path Expand called

TE-PCALC: 1.1.1.1_56->6.6.6.6_0 {7}: Path Request Info
  Flags:  END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 1.1.1.1_56->6.6.6.6_0 {7}: rrr_pcalc_lsr_expand:  Exclude node:
2.2.2.2 (intf: 20.2.3.2)
TE-PCALC-PATH: 1.1.1.1_56->6.6.6.6_0 {7}: rrr_pcalc_lsr_expand:  Exclude node:
1.1.1.1 (intf: 10.1.2.1)
TE-PCALC-PATH: 1.1.1.1_56->6.6.6.6_0 {7}: Area (isis  level-2) Path Lookup begin

TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
Path from 0000.0000.0003.00 -> 0000.0000.0006.00:
  20.3.6.6->0.0.0.0 (admin_weight=10):
  20.3.6.3->0.0.0.0 (admin_weight=10):
  num_hops 3, accumlated_aw 10, min_bw 75000
TE-PCALC-PATH: 3.3.3.3_56->6.6.6.6_0 {7}: Area (isis  level-2) Path Lookup end:
path found
6.6.6.6 expands to:
20.3.6.3
20.3.6.6
6.6.6.6
TE-PCALC-API: 3.3.3.3_56->6.6.6.6_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: path previous hop is 20.2.3.2 (Fa0/0.23)
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: path next hop is 20.3.6.6 (Fa0/0.36)
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: sending ADD RESV reply
```

R3 can successfully expand the path toward R6, because both are in the same flooding domain (IS-IS Level-2). R3 expands the path as R3 to R6, and then asks R6 to expand the path to the final destination, 20.20.20.20 (XR2).

```
R6#
TE-PCALC-API: 1.1.1.1_56->20.20.20.20_0 {7}: LSP Path Expand called


TE-PCALC: 1.1.1.1_56->20.20.20.20_0 {7}: Path Request Info
  Flags:  END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand: Exclude node:
3.3.3.3 (intf: 20.3.6.3)
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand: Can't get router ID addr for 20.2.3.2
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: rrr_pcalc_lsr_expand: Can't get router ID addr for 10.1.2.1
TE-PCALC-PATH: 1.1.1.1_56->20.20.20.20_0 {7}: Area (isis  level-1) Path Lookup
begin
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
TE-PCALC-PATH: exclude_path: system_id 0-0-0-0-0-0-0 not known!
Path from 0000.0000.0006.00 -> 0000.0000.0020.00:
  10.19.20.19->10.19.20.20 (admin_weight=20):
  20.6.19.19->20.6.19.19 (admin_weight=10):
  20.6.19.6->0.0.0.0 (admin_weight=10):
  num_hops 4, accumlated_aw 20, min_bw 0
TE-PCALC-PATH: 6.6.6.6_56->20.20.20.20_0 {7}: Area (isis  level-1) Path Lookup end:
path found
20.20.20.20 expands to:
20.6.19.6
20.6.19.19
10.19.20.20
20.20.20.20
TE-PCALC-API: 6.6.6.6_56->20.20.20.20_0 {7}: LSP Path Expand result: success


TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: received ADD RESV request
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: path previous hop is 20.3.6.3 (Fa0/0.36)
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: path next hop is 20.6.19.19 (Fa0/0.619)
TE-SIG-LM: 1.1.1.1_56->20.20.20.20_0 {7}: sending ADD RESV reply
```

R6 receives the expansion request from R3 and is able to fulfill it, because R6 and XR2 are in the same flooding domain (IS-IS Level-1). R6 then expands the path as R6 to XR1 to XR2, and sends the RSVP messages to request the reservation of

XR2. The final result is that the tunnel is signaled end to end, and traffic flows from R1 to XR2 via R3 and via R6.

```
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20
 1 10.1.2.2 [MPLS: Label 17 Exp 0]
 0 msec 4 msec 0 msec 2 20.2.3.3 [MPLS: Label 16 Exp 0]
 0 msec 0 msec 0 msec 3 20.3.6.6 [MPLS: Label 17 Exp 0]
 4 msec 0 msec 4 msec 4 20.6.19.19 [MPLS: Label 16000 Exp 0]
 0 msec 4 msec 4 msec
  5 10.19.20.20 4 msec *  4 msec
```

The logic is identical in the reverse path. XR2 requests a tunnel to R1 that will loosely route via R5 and R4. So the first step is to calculate the path to R5, and then ask R5 to expand the path to R4.

```
RP/0/3/CPU0:XR2#config t
Thu Jun 28 19:59:13.242 UTC
RP/0/3/CPU0:XR2(config)#int tunnel-te0 RP/0/3/CPU0:XR2(config-if)#no shut

RP/0/3/CPU0:XR2(config-if)#commit
R5#
TE-PCALC-API: 20.20.20.20_11->4.4.4.4_0 {7}: LSP Path Expand called

TE-PCALC: 20.20.20.20_11->4.4.4.4_0 {7}: Path Request Info
  Flags:    END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 20.20.20.20_11->4.4.4.4_0 {7}: Area (isis  level-2) Path Lookup
begin
Path from 0000.0000.0005.00 -> 0000.0000.0004.00:
  20.4.5.4 ->0.0.0.0 (admin_weight=10):
  20.4.5.5 ->0.0.0.0 (admin_weight=10):
  num_hops 3, accumlated_aw 10, min_bw 75000
TE-PCALC-PATH: 5.5.5.5_11->4.4.4.4_0 {7}: Area (isis  level-2) Path Lookup end:
 path found
4.4.4.4 expands to:
20.4.5.5
20.4.5.4
4.4.4.4
TE-PCALC-API: 5.5.5.5_11->4.4.4.4_0 {7}: LSP Path Expand result: success
```

```
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: received ADD RESV request
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: path previous hop is 20.5.19.19
(Fa0/0.519)
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: path next hop is 20.4.5.4 (Fa0/0.45)
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: sending ADD RESV reply
```

R5 sees that 4.4.4.4 (R4) is in the same link state flooding domain as itself (IS-IS Level-2), so it can expand the path. R5 then asks R4 to expand the path to 1.1.1.1 (R1).

```
R4#
TE-PCALC-API: 20.20.20.20_11->1.1.1.1_0 {7}: LSP Path Expand called

TE-PCALC: 20.20.20.20_11->1.1.1.1_0 {7}: Path Request Info
  Flags:    END_SWCAP_UNKNOWN
  IP explicit-path: None (dynamic)
  bw 0, min_bw 0, metric: 0
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0x0
TE-PCALC-PATH: 20.20.20.20_11->1.1.1.1_0 {7}: Area (isis  level-1) Path Lookup
begin
Path from 0000.0000.0004.00 -> 0000.0000.0001.00:
  10.1.2.1 ->0.0.0.0 (admin_weight=20):
  10.1.2.2 ->0.0.0.0 (admin_weight=20):
  20.2.4.2->0.0.0.0 (admin_weight=10):
  20.2.4.4->0.0.0.0 (admin_weight=10):
  num_hops 5, accumlated_aw 20, min_bw 75000
TE-PCALC-PATH: 4.4.4.4_11->1.1.1.1_0 {7}: Area (isis level-1) Path Lookup end: path found
1.1.1.1 expands to:
20.2.4.4
20.2.4.2
10.1.2.2
10.1.2.1
1.1.1.1
TE-PCALC-API: 4.4.4.4_11->1.1.1.1_0 {7}: LSP Path Expand result: success

TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: received ADD RESV request
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: path previous hop is 20.4.5.5 (Fa0/0.45)
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: path next hop is 20.2.4.2 (Fa0/0.24)
TE-SIG-LM: 20.20.20.20_11->1.1.1.1_0 {7}: sending ADD RESV reply
```

Because R4 knows about R1 via the Level-1 flooding domain, the path can be expanded. The result is that signaling is end to end between XR2 and R1, and the label bindings occur via the RSVP messages.

```
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
 Thu Jun 28 20:01:49.035 UTC

 Type escape sequence to abort.
 Tracing the route to 1.1.1.1
  1 10.19.20.19 [MPLS: Label 16001 Exp 0]
  7 msec  5 msec  4 msec 2 20.5.19.5 [MPLS: Label 16 Exp 0]
  3 msec  4 msec  2 msec 3 20.4.5.4   [MPLS: Label 29 Exp 0] 3 msec
   3 msec  2 msec 4 20.2.4.2   [MPLS: Label 16 Exp 0] 2 msec
   4 msec  2 msec
  5 10.1.2.1 2 msec  *   3  msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 5: MPLS TE v4

5.11 Inter-AS MPLS TE (pending update)

- Configure IS-IS routing in the network as follows:
  - R1, R2, R3, and R4 should run IS-IS and use NET address 00.0000.0000.000Y.00, where Y is the router number.
  - Level-2 consists of links interconnecting R1 & R2, R2 & R3, R2 & R4, R3 & R4, and all their Loopback0 interfaces.
- Configure OSPF routing in the network as follows:
  - R5, R6, XR1, and XR2 should run OSPF.
  - Area 0 consists of links interconnecting R5 & R6, R5 & XR1, R6 & XR1, XR1 & XR2, and all their Loopback0 interfaces.
- Configure the network to support MPLS TE tunnels as follows:
  - Enable MPLS TE support for IS-IS Level-2 on R1, R2, R3, and R4.
  - Enable MPLS TE support for OSPF Area 0 on R5, R6, XR1, and XR2.
  - Set the MPLS TE Router-IDs to be the Loopback0 interfaces.
  - Enable support for RSVP and MPLS TE on all transit interfaces.
- Configure Inter-AS MPLS TE support as follows:
  - Do not advertise the Inter-AS links (R3 & R6, R4 & R5, and R4 & R6) into IGP.
  - Instead, configure these links as passive interfaces for the MPLS TE process.
  - Use the routers' Loopback0 interfaces as the neighbor TE ID.
- Configure an MPLS TE tunnel from R1 to XR2 as follows:
  - Unnumber the tunnel to R1's Loopback0 interface.
  - Set the tunnel destination as XR2's Loopback0 interface.
  - Configure the tunnel's explicit path option to use loose next-hops as follows:
    - R1 should use R3 as the first ASBR.
    - R3 should use R6 as the next ASBR.
  - Configure Autoroute Destination so that R1 uses the tunnel to route toward XR2's Loopback0.
- Configure an MPLS TE tunnel from XR2 to R1 as follows:
  - Unnumber the tunnel to XR2's Loopback0 interface.

- Set the tunnel destination as R1's Loopback0 interface.
  - Configure the tunnel's explicit path option to use loose next-hops as follows:
    - XR2 should use R6 as the first ASBR.
    - R6 should use R4 as the next ASBR.
  - Configure static routing so that XR2 uses the tunnel to route toward R1's Loopback0.
- When complete, you should be able to ping and traceroute between the Loopback0 networks of R1 and XR2.

Configuration

```
R1:
mpls traffic-eng tunnels
!
ip explicit-path name INTER_AS_TE enable
 next-address loose 3.3.3.3
 next-address loose 6.6.6.6
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 20.20.20.20
 tunnel mpls traffic-eng autoroute destination
 tunnel mpls traffic-eng path-option 10 explicit name INTER_AS_TE
!
interface Loopback0
 ip router isis 1
!
interface FastEthernet0/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
router isis 1
 net 00.0000.0000.0001.00
 is-type level-2
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R2:
mpls traffic-eng tunnels
!
```

```
interface Loopback0
 ip router isis 1
!
interface FastEthernet1/0
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
router isis 1
 net 00.0000.0000.0002.00
 is-type level-2
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
!
interface FastEthernet0/0.23
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 6.6.6.6 nbr-if-addr 20.3.6.6
!
```

```
router isis 1
 net 00.0000.0000.0003.00
 is-type level-2
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface Loopback0
 ip router isis 1
!
interface FastEthernet0/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip router isis 1
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 5.5.5.5 nbr-if-addr 20.4.5.5
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 6.6.6.6 nbr-if-addr 20.4.6.6
!
router isis 1
 net 00.0000.0000.0004.00
 metric-style wide is-type level-2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.45
```

```
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 4.4.4.4 nbr-if-addr 20.4.5.4
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.519
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R6:
mpls traffic-eng tunnels
!
interface Loopback0
 ip ospf 1 area 0
!
interface FastEthernet0/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 3.3.3.3 nbr-if-addr 20.3.6.3
!
interface FastEthernet0/0.46
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng passive-interface nbr-te-id 4.4.4.4 nbr-if-addr 20.4.6.4
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 ip ospf 1 area 0
!
router ospf 1
 mpls traffic-eng router-id Loopback0
```

```
 mpls traffic-eng area 0

XR1:
router ospf 1
 area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface GigabitEthernet0/1/0/0.519
  !
  interface GigabitEthernet0/1/0/0.619
  !
  interface POS0/6/0/0
  !
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.519
 !
 interface GigabitEthernet0/1/0/0.619
 !
!
mpls ldp

XR2:
explicit-path name INTER_AS_TE
 index 1 next-address loose ipv4 unicast 6.6.6.6
 index 2 next-address loose ipv4 unicast 4.4.4.4
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 1.1.1.1
 path-option 10 explicit name INTER_AS_TE
```

```
!
router static
 address-family ipv4 unicast
  1.1.1.1/32 tunnel-te0
 !
!
router ospf 1
 area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface POS0/7/0/0
  !
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface POS0/7/0/0
 !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/7/0/0
 !
!
mpls ldp
```

Verification

Inter-AS MPLS TE has design problems similar to Inter-Area MPLS TE, where the Head End of the TE tunnel is not in the same link state flooding domain as the Tail End. To overcome this, as in Inter-Area MPLS TE, the Head End specifies loose hops in the explicit path, which list the ASBRs that should be used as transit between the ASes. Because the Inter-AS links would not typically run IGP, the command `mpls traffic-eng passive-interface` is used to populate the MPLS TE topology database with the TE router-id and interface IP address of the remote ASBRs, and specify the exit links by which they are reachable.

For example, in the below output we see that in the OSPF TE topology of XR2, it knows that the remote ASBRs R3 and R4 are reachable via the OSPF router R6, because R6 has specific links to R3 and R4 as an MPLS TE passive interface.

```
RP/0/3/CPU0:XR2#show mpls traffic-eng topology 6.6.6.6

Thu Jun 28 21:00:04.325 UTC


IGP Id: 6.6.6.6, MPLS TE Id: 6.6.6.6 Router Node    (OSPF 1 area 0)

 <snip>
 Link[2]:Unknown subnet type, Nbr IGP Id:3.3.3.3, Nbr Node Id:-1, gen:17538

      Frag Id:5, Intf Address:20.3.6.6, Intf Id:0
      Nbr Intf Address:3.3.3.3, Nbr Intf Id:0
      TE Metric:10, IGP Metric:4294967295, Attribute Flags:0x0
      Attribute Names:
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
      Max Reservable BW Sub:0 (kbps)
                               Global Pool       Sub Pool
               Total Allocated Reservable        Reservable
               BW (kbps)       BW (kbps)         BW (kbps)
               --------------- -----------       ----------
        bw[0]:           0         75000                0
        bw[1]:           0         75000                0
        bw[2]:           0         75000                0
        bw[3]:           0         75000                0
        bw[4]:           0         75000                0
        bw[5]:           0         75000                0
        bw[6]:           0         75000                0
        bw[7]:           0         75000                0
 Link[3]:Point-to-Point, Nbr IGP Id:4.4.4.4, Nbr Node Id:-1, gen:17539

      Frag Id:6, Intf Address:20.4.6.6, Intf Id:0
      Nbr Intf Address:4.4.4.4, Nbr Intf Id:0
      TE Metric:10, IGP Metric:4294967295, Attribute Flags:0x0 Attribute Names:
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
      Max Reservable BW Sub:0 (kbps)


                               Global Pool       Sub Pool
               Total Allocated Reservable        Reservable
               BW (kbps)       BW (kbps)         BW (kbps)
               --------------- -----------       ----------
        bw[0]:           0         75000                0
```

```
        bw[1]:          0       75000           0
        bw[2]:          0       75000           0
        bw[3]:          0       75000           0
        bw[4]:          0       75000           0
        bw[5]:          0       75000           0
        bw[6]:          0       75000           0
        bw[7]:          0       75000           0
```

When the MPLS TE topology calculation is performed, XR2 runs cSPF to reach its local ASBR 6.6.6.6 (R6). XR2 then asks R6 to expand the path to the next ASBR, 4.4.4.4 (R4).

```
RP/0/3/CPU0:XR2#config t

Thu Jun 28 21:04:34.790 UTC

RP/0/3/CPU0:XR2(config)#int tunnel-te0 RP/0/3/CPU0:XR2(config-if)#no shut


RP/0/3/CPU0:XR2(config-if)#commit

R6#debug mpls traffic-eng tunnels signalling


MPLS traffic-eng tunnels signalling debugging is onR6#debug mpls traffic-eng path lookup


MPLS traffic-eng path lookup events debugging is on

R6# TE-PCALC-API: 20.20.20.20_4->4.4.4.4_0 {7}: LSP Path Expand called


  TE-PCALC: 20.20.20.20_4->4.4.4.4_0 {7}: Path Request Info

  Flags:  END_SWCAP_UNKNOWN

  IP explicit-path: None (dynamic)

  bw 0, min_bw 0, metric: 0

  setup_pri 7, hold_pri 7

  affinity_bits 0x0, affinity_mask 0x0

TE-PCALC-PATH: 20.20.20.20_4->4.4.4.4_0 {7}: Area (ospf 1  area 0) Path Lookup

begin TE-PCALC-PATH: expand_lsr: Dst addr 4.4.4.4 not found in area (ospf 1 area 0)


Path from 6.6.6.6 -> 4.4.4.4:

20.4.6.6->4.4.4.4 (admin_weight=10): TE-PCALC-PATH: Reached static node


num_hops 2, accumlated_aw 10, min_bw 75000 TE-PCALC-PATH:    Path to a non-igp destination 4.4.4.4

 TE-PCALC-PATH: 6.6.6.6_4->4.4.4.4_0 {7}: Area (ospf 1  area 0) Path Lookup end:

 path found

 4.4.4.4 expands to:

 20.4.6.6

 4.4.4.4

 TE-PCALC-API: 6.6.6.6_4->4.4.4.4_0 {7}: LSP Path Expand result: success


TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: received ADD RESV request

TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path previous hop is 20.6.19.19

(Fa0/0.619)

TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path next hop is 20.4.6.4 (Fa0/0.46)

TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: sending ADD RESV reply
```

In the above output, we see that R6 receives the request to expand the path toward R4. First it looks to see if R4 is part of the IGP domain, which it is not. R6 then checks the statically defined neighbors via the `mpls traffic-eng passive-interface` command and is able to expand the path to that directly connected neighbor. R6 then asks R4 to expand the path to the final destination.

```
R4#
TE-PCALC-API: 20.20.20.20_4->1.1.1.1_0 {7}: LSP Path Expand called

 TE-PCALC: 20.20.20.20_4->1.1.1.1_0 {7}: Path Request Info
   Flags:  END_SWCAP_UNKNOWN
   IP explicit-path: None (dynamic)
   bw 0, min_bw 0, metric: 0
   setup_pri 7, hold_pri 7
   affinity_bits 0x0, affinity_mask 0x0
 TE-PCALC-PATH: 20.20.20.20_4->1.1.1.1_0 {7}: Area (isis  level-2) Path Lookup begin
 Path from 0000.0000.0004.00 -> 0000.0000.0001.00:
   10.1.2.1 ->0.0.0.0 (admin_weight=20):
   10.1.2.2 ->0.0.0.0 (admin_weight=20):
   20.2.4.2->0.0.0.0 (admin_weight=10):
   20.2.4.4->0.0.0.0 (admin_weight=10):
   num_hops 5, accumlated_aw 20, min_bw 75000
 TE-PCALC-PATH: 4.4.4.4_4->1.1.1.1_0 {7}: Area (isis  level-2) Path Lookup end: path found
1.1.1.1 expands to:
20.2.4.4
20.2.4.2
10.1.2.2
10.1.2.1
1.1.1.1
TE-PCALC-API: 4.4.4.4_4->1.1.1.1_0 {7}: LSP Path Expand result: success

 TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: received ADD RESV request
 TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path previous hop is 20.4.6.6 (Fa0/0.46)
 TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: path next hop is 20.2.4.2 (Fa0/0.24)
 TE-SIG-LM: 20.20.20.20_4->1.1.1.1_0 {7}: sending ADD RESV reply
```

Because R4 is in the same IGP flooding domain as the final destination, it can use the normal TE topology to calculate the cSPF toward the tunnel Tail End. The final result is that R4 expands the path to R1 via R2. The same process happens in the reverse direction from R1 to XR1 via ASBRs R3 and R6. The final verification is then the traceroute between the tunnel endpoints, which indicates which ASBRs are used for forwarding.

```
R1#traceroute 20.20.20.20
```

```
Type escape sequence to abort.
Tracing the route to 20.20.20.20
 1 10.1.2.2 [MPLS: Label 17 Exp 0]
 0 msec 4 msec 4 msec 2 20.2.3.3 [MPLS: Label 16 Exp 0]
 0 msec 0 msec 4 msec 3 20.3.6.6 [MPLS: Label 17 Exp 0]
 0 msec 4 msec 0 msec 4 20.6.19.19 [MPLS: Label 16000 Exp 0]
 4 msec 4 msec 0 msec
  5 10.19.20.20 8 msec *  4 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1 source 20.20.20.20
Thu Jun 28 21:10:29.215 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1
 1 10.19.20.19 [MPLS: Label 16001 Exp 0
] 7 msec   7 msec  4 msec 2 20.6.19.6 [MPLS: Label 16 Exp 0]
 3 msec  4 msec  2 msec 3 20.4.6.4 [MPLS: Label 26 Exp 0]
 3 msec  4 msec  2 msec 4 20.2.4.2 [MPLS: Label 16 Exp 0]
 3 msec  4 msec  2 msec
 5 10.1.2.1 3 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - Advanced Technology Lab 6: Services v4

6.1 Multicast VPNs (pending update)

- R2 and XR1 are preconfigured as PE routers for Unicast MPLS L3VPN service to VRF VPN_A. Configure the network as defined below to also provide Multicast transport services to this customer.
- Configure Multicast Routing in the Service Provider Core as follows:
  - Enable PIM in Sparse Mode on all transit interfaces running IGP in the core, along with the Loopback0 interfaces of R2 and XR1.
  - Enable support for Source Specific Multicast using the group range 232.0.0.0/8 in the core.
  - Activate the MDT address-family for the BGP peering between the PE routers R2 and XR1.
  - Configure VRF VPN_A on R2 and XR1 to use the default Multicast Distribution Tree (MDT) address 232.0.0.1, and the data MDT address 232.0.1.0/24.
- Configure the Multicast Routing in the Customer sites as follows:
  - Enable PIM in Sparse Mode on all transit interfaces of R1 & XR2, and on the CE facings links of R2 and XR1.
  - Enable PIM in Sparse Mode on the Loopback0 interface of XR2.
  - Configure XR2 to announce itself as the BSR and RP Candidate for all groups in the range 224.0.0.0/4.
  - Configure R7's link to R1 to generate an IGMP Report message for the group 227.7.7.7.
  - Configure R8's link to XR2 to generate an IGMP Report message for the group 228.8.8.8.
- When complete, you should be able to perform the following verifications:
  - R1 should have built a (*,G) tree for the group (*,227.7.7.7) back to the Rendezvous Point XR2.
  - XR2 should have a (*,G) tree built for the group (*,228.8.8.8) to its attached receiver, R8.
  - R7 should be able to ping the multicast group address 228.8.8.8, and have packets forwarded out to the receiver R8.

- R8 should be able to ping the multicast group address 227.7.7.7, and have packets forwarded out to the receiver R7.
- High volumes of multicast traffic generated by R7 or R8 for these group addresses should cause new MDT data tunnels to form between R2 and XR1.

Configuration

```
R1:
ip multicast-routing
!
interface FastEthernet0/0
 ip pim sparse-mode
!
interface FastEthernet1/0
 ip pim sparse-mode

R2:
ip multicast-routing
ip pim ssm default
!
ip multicast-routing vrf VPN_A
!
vrf definition VPN_A
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet1/0
 ip pim sparse-mode
!
interface FastEthernet0/0.23
 ip pim sparse-mode
!
interface FastEthernet0/0.24
 ip pim sparse-mode
!
router bgp 100
 address-family ipv4 mdt
  neighbor 19.19.19.19 activate
```

```
  neighbor 19.19.19.19 send-community extended
 exit-address-family

R3:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet0/0.23
 ip pim sparse-mode
!
interface FastEthernet0/0.34
 ip pim sparse-mode
!
interface FastEthernet0/0.36
 ip pim sparse-mode

R4:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet0/0.24
 ip pim sparse-mode
!
interface FastEthernet0/0.34
 ip pim sparse-mode
!
interface FastEthernet0/0.45
 ip pim sparse-mode
!
interface FastEthernet0/0.46
 ip pim sparse-mode

R5:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet0/0.45
 ip pim sparse-mode
!
interface FastEthernet0/0.56
 ip pim sparse-mode
!
interface FastEthernet0/0.519
 ip pim sparse-mode

R6:
```

```
ip multicast-routing
ip pim ssm default
!
interface FastEthernet0/0.36
 ip pim sparse-mode
!
interface FastEthernet0/0.46
 ip pim sparse-mode
!
interface FastEthernet0/0.56
 ip pim sparse-mode
!
interface FastEthernet0/0.619
 ip pim sparse-mode

R7:
interface FastEthernet0/0
 ip igmp join-group 227.7.7.7

R8:
interface FastEthernet0/0
 ip igmp join-group 228.8.8.8

XR1:
router bgp 100
 address-family ipv4 mdt
 !
 neighbor 2.2.2.2
  address-family ipv4 mdt
!
multicast-routing
 address-family ipv4
  mdt source Loopback0
  interface all enable
!
vrf VPN_A
 address-family
  ipv4 mdt data 232.0.1.0/24
  mdt default ipv4 232.0.0.1
  interface all enable
!
end

XR2:
multicast-routing
 address-family ipv4
```

```
  interface all enable
 !
!
router pim
 address-family ipv4
  bsr candidate-bsr 20.20.20.20 hash-mask-len 30 priority 1
  bsr candidate-rp 20.20.20.20 group-list 224/4 priority 192 interval 60
```

Verification

Verification of Multicast over MPLS L3VPN service consists of two separate portions: verification of the SP core, and verification of the customer networks. In the SP core we must ensure that the PE routers can form an MDT tunnel for their VRF, which is essentially a GRE tunnel that uses a multicast destination address. Because in this case the MDT addresses are Source Specific Multicast addresses, the core of the SP network does not need a Rendezvous Point. Instead, PIM Sparse Mode simply needs to be on the transit interfaces running IGP, and the regular IOS routers need the command `ip pim ssm default` to know which PIM Join/Prune message should belong to SSM groups vs. regular Sparse Mode groups.

If the Multicast Tree for the MDT tunnel is properly formed, the PE routers should have (S,G) entries for each other's BGP loopback addresses and the MDT default address, as seen below.

```
R2#show ip mroute 232.0.0.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(2.2.2.2, 232.0.0.1), 00:13:14/00:03:01, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0.24, Forward/Sparse, 00:13:14/00:03:01
(19.19.19.19, 232.0.0.1), 00:13:33/stopped, flags: sTIZ

  Incoming interface: FastEthernet0/0.24, RPF nbr 20.2.4.4
```

```
  Outgoing interface list: MVRF VPN_A, Forward/Sparse
, 00:13:33/00:01:26

RP/0/0/CPU0:XR1#show pim topology 232.0.0.1
Wed May  2 21:48:12.758 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
(2.2.2.2,232.0.0.1)SPT SSM Up: 01:01:57
JP: Join(now) RPF: GigabitEthernet0/1/0/0.619,20.6.19.6 Flags:
  Loopback0                   01:01:57  fwd LI LH
(19.19.19.19,232.0.0.1)SPT SSM Up: 01:02:11

JP: Join(never) RPF: Loopback0,19.19.19.19* Flags:
  GigabitEthernet0/1/0/0.619  00:52:16  fwd Join(00:03:17)
  Loopback0                   01:02:11  fwd LI LH
```

In regular IOS, the lowercase “s” flag means SSM, and the Outgoing Interface List for the (19.19.19.19, 232.0.0.1) entry points to the VRF. This essentially means that the outer GRE header gets decapsulated when the packet is received in, and then it is forwarded to the VRF VPN_A Multicast Routing Table for further forwarding. XR1 shows similar output for the (2.2.2.2, 232.0.0.1) group, but the OIL doesn’t explicitly list the MVPN. The MDT tunnel can also be verified working as seen below.

```
R2#show bgp ipv4 mdt all
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_A)
*> 2.2.2.2/32       0.0.0.0                                0 ?
*>i19.19.19.19/32   19.19.19.19                   100      0 i
```

```
R2#show bgp ipv4 mdt all 19.19.19.19

BGP routing table entry for 100:1:19.19.19.19/32     version 3
Paths: (1 available, best #1, table IPv4-MDT-BGP-Table)
  Not advertised to any peer
  Local
    19.19.19.19 from 19.19.19.19 (19.19.19.19)
      Origin IGP, localpref 100, valid, internal, best, MDT group address: 232.0.0.1
RP/0/0/CPU0:XR1#show bgp ipv4 mdt
Wed May  2 22:09:06.891 UTC
BGP router identifier 19.19.19.19, local AS number 100
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 3
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1  *>i2.2.2.2/96         2.2.2.2                  0    100      0 ?
*> 19.19.19.19/96      0.0.0.0                                0 i

Processed 2 prefixes, 2 paths
RP/0/0/CPU0:XR1#show bgp ipv4 mdt vrf VPN_A 2.2.2.2
Wed May  2 22:12:53.749 UTC
BGP routing table entry for 2.2.2.2/96, Route Distinguisher: 100:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                  3           3
Last Modified: May  2 20:46:15.546 for 01:26:38
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Local
    2.2.2.2 (metric 4) from 2.2.2.2 (2.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, best MDT group address: 232.0.0.1
```

The above output shows that R2 and XR1 are learning that each other’s BGP Loopback addresses are possible endpoints for MDT tunnels, specifically using the group address 232.0.0.1. Without learning these addresses through the MDT extensions of BGP, they would not know where to send their PIM SPT Join messages for the (S,G) pair of the MDT tunnel. Another more concise variation of this is shown below:

```
R2#show ip pim mdt bgp
MDT (Route Distinguisher + IPv4)              Router ID        Next Hop
  MDT group 232.0.0.1
    100:1:19.19.19.19                         19.19.19.19      19.19.19.19
RP/0/0/CPU0:XR1#show pim bgp-safi

Wed May 2 22:11:47.371 UTC
 Grp 232.0.0.1       Src 2.2.2.2         RD 100:1    Nexthop 2.2.2.2 Ext 0, BGP
```

If the tunnel is properly formed bi-directionally, the PE routers should form a PIM adjacency over the tunnel, but inside the VRF table, not the global table. This can be seen below:

```
R2#show ip pim vrf VPN_A neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
19.19.19.19       Tunnel0                  01:20:01/00:01:30 v2    1 / DR G
10.1.2.1          FastEthernet1/0          01:31:50/00:01:21 v2    1 / S P G
RP/0/0/CPU0:XR1#show pim vrf VPN_A neighbor
Wed May  2 22:17:17.148 UTC

PIM neighbors in VRF VPN_A

Neighbor Address                Interface           Uptime    Expires  DR pri
Flags
 2.2.2.2                        mdtVPN/A            01:30:56  00:01:43 1      P

19.19.19.19*                    mdtVPN/A            01:31:11  00:01:19 1 (DR) B
10.19.20.19*                    POS0/6/0/0          01:31:15  00:01:29 1      B P
10.19.20.20                     POS0/6/0/0          01:28:07  00:01:16 1 (DR) B
```

Regular IOS expresses this as Tunnel0, whereas IOS XR expresses it as mdtVPN/A. Both essentially mean the same thing, that the routers have formed a PIM adjacency over the multicast GRE tunnels. If there are any problems in the design up to this point, such as RPF failure in the core, PIM adjacencies not being established, etc., none of the customer's traffic will get properly encapsulated inside GRE after it enters the provider network.

The next set of verifications are then on the customer side. From the CE's point of view, the PE routers are simply normal PIM neighbors in the global routing table, as seen below on R1 and XR2.

```
R1#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.1.2.2          FastEthernet0/0          01:34:11/00:01:33 v2    1 / DR S P G
RP/0/3/CPU0:XR2#show pim neighbor
Wed May 2 22:19:38.152 UTC

PIM neighbors in VRF default

Neighbor Address             Interface              Uptime    Expires  DR pri
Flags

20.20.20.20*                 Loopback0             01:30:29  00:01:34 1 (DR) B P
10.8.20.20*                  GigabitEthernet0/4/0/0 01:30:29  00:01:30 1 (DR) B P
10.19.20.19                  POS0/7/0/0            01:30:26  00:01:39 1      B


10.19.20.20*                 POS0/7/0/0            01:30:29  00:01:26 1 (DR) B P
```

XR2 has configured itself as a BSR and an RP Candidate. The XR command `show pim range-list` is the equivalent of the IOS command `show ip pim rp mapping`.

```
RP/0/3/CPU0:XR2#show pim bsr election
Wed May  2 22:20:42.854 UTC
PIM BSR Election State
 Cand/Elect-State      Uptime    BS-Timer BSR
                C-BSR
 Elected/Accept-Pref   01:31:19  00:00:55 20.20.20.20
  [1, 30]   20.20.20.20 [1, 30]
RP/0/3/CPU0:XR2#show pim bsr candidate-rp
Wed May  2 22:20:48.229 UTC
PIM BSR Candidate RP Info
```

```
 Cand-RP
mode     scope     priority    uptime   group-list 20.20.20.20
   SM    16          192        01:31:24
RP/0/3/CPU0:XR2#show pim range-list
Wed May  2 22:20:55.410 UTC

config SSM Exp: never Learnt from : 0.0.0.0
  232.0.0.0/8 Up: 01:31:46 bsr SM RP: 20.20.20.20
 Exp: never Learnt from : 0.0.0.0  224.0.0.0/4
 Up: 01:30:31
```

If the MDT tunnel is working end to end, R1 should learn that XR2 is the RP via BSR.

```
R1#show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4 RP 20.20.20.20
 (?), v2 Info source: 20.20.20.20  (?), via bootstrap
, priority 192, holdtime 150
         Uptime: 01:24:40, expires: 00:01:49
```

Now the entire control plane for multicast is verified as working. The next step is to verify the data plane. When a multicast sender comes onto the network, the PIM DR on the attached segment should notify the RP though a PIM Register message. This can be verified by pinging a multicast group address on R7 (behind R1), and seeing if the (S,G) entry is learned on the RP, XR2.

```
RP/0/3/CPU0:XR2#show pim topology 224.1.1.1
Wed May  2 22:23:53.871 UTC No PIM topology table entries found.
R7#ping 224.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.1.1.1, timeout is 2 seconds:
.
RP/0/3/CPU0:XR2#show pim topology 224.1.1.1
Wed May  2 22:24:12.607 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
```

```
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
(10.1.7.7,224.1.1.1
) SM Up: 00:00:09
JP: Null(never) RPF: POS0/7/0/0,10.19.20.19 Flags: KAT(00:03:23) RA RR (00:04:25)
  No interfaces in immediate olist
```

The RP has installed the (S,G) entry, which means that the Register message was successfully processed. Further verification of this could be performed with the debug ip pim in regular IOS or the debug pim protocol register in IOS XR. The next verification would be to see if a (*,G) PIM Join can be properly processed over the MDT tunnel. This is accomplished as follows:

```
RP/0/3/CPU0:XR2#show pim topology 227.7.7.7

 Wed May  2 22:28:01.403 UTC
 No PIM topology table entries found.
 R7#config t

 Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#int f0/0R7(config-if)#ip igmp join 227.7.7.7

 R7(config-if)#end
 RP/0/3/CPU0:XR2#show pim topology 227.7.7.7

 Wed May 2 22:28:36.873 UTC

 IP PIM Multicast Topology Table
 Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
 Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
     RA - Really Alive, IA - Inherit Alive, LH - Last Hop
     DSS - Don't Signal Sources, RR - Register Received
     SR - Sending Registers, E - MSDP External, EX - Extranet
     DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
     MT - Crossed Data MDT threshold, MA - Data MDT group assigned
 Interface state: Name, Uptime, Fwd, Info
 Interface flags: LI - Local Interest, LD - Local Dissinterest,
     II - Internal Interest, ID - Internal Dissinterest,
     LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
  (\*,227.7.7.7) SM Up: 00:00:07 RP: 20.20.20.20*

 JP: Join(never) RPF: Decapstunnel0,20.20.20.20 Flags:
   POS0/7/0/0                  00:00:07  fwd Join(00:03:22)
```

The RP knows about the (*,G) tree, for which it is the root. This means that the PIM Join message was properly sent all the way across the MDT tunnel in the SP core.

The next verification would be to ensure that traffic can actually flow. This is done bidirectionally with a sender on R7 and a receiver on R8, and vice versa.

```
R7#ping 228.8.8.8 repeat 10

 Type escape sequence to abort.
 Sending 10, 100-byte ICMP Echos to 228.8.8.8, timeout is 2 seconds:
 . Reply to request 1 from 10.8.20.8
, 12 ms
 Reply to request 2 from 10.8.20.8, 1 ms
```

```
Reply to request 3 from 10.8.20.8, 4 ms
Reply to request 4 from 10.8.20.8, 1 ms
<snip>
R8#ping 227.7.7.7 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 227.7.7.7, timeout is 2 seconds:
Reply to request 0 from 10.1.7.7
, 12 ms
Reply to request 1 from 10.1.7.7, 1 ms
Reply to request 2 from 10.1.7.7, 1 ms
Reply to request 3 from 10.1.7.7, 1 ms
Reply to request 4 from 10.1.7.7, 1 ms
<snip>
```

The PE routers should now have both of these (S,G) states in the VRF specific Multicast Routing Tables.

```
R2#show ip mroute vrf VPN_A
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(\*, 228.8.8.8), 00:01:23/stopped, RP 20.20.20.20, flags: SP
  Incoming interface: Tunnel0, RPF nbr 19.19.19.19
  Outgoing interface list: Null
(10.1.7.7, 228.8.8.8)
, 00:01:23/00:02:06, flags: T Incoming interface: FastEthernet1/0
, RPF nbr 10.1.2.1 Outgoing interface list
: Tunnel0
, Forward/Sparse, 00:01:23/00:03:09

(\*, 227.7.7.7), 01:32:51/00:03:15, RP 20.20.20.20, flags: S
  Incoming interface: Tunnel0, RPF nbr 19.19.19.19
  Outgoing interface list:
    FastEthernet1/0, Forward/Sparse, 00:04:11/00:03:15
```

```
(10.8.20.8, 227.7.7.7)
, 00:02:29/00:01:00, flags: T Incoming interface: Tunnel0
, RPF nbr 19.19.19.19 Outgoing interface list
: FastEthernet1/0
, Forward/Sparse, 00:02:29/00:03:15

(\*, 224.0.1.40), 01:47:24/00:02:39, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet1/0, Forward/Sparse, 01:47:22/00:02:35



RP/0/0/CPU0:XR1#show pim vrf VPN_A topology
Wed May  2 22:32:59.149 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(\*,224.0.1.40) DM Up: 01:46:53 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags:
  POS0/6/0/0                  01:46:53  off LI II

(\*,227.7.7.7) SM Up: 00:04:30 RP: 20.20.20.20
JP: Join(00:00:20) RPF: POS0/6/0/0,10.19.20.20 Flags:
  mdtVPN/A                    00:04:30  fwd Join(00:02:54)
(10.8.20.8,227.7.7.7)
SPT SM Up: 00:02:48 JP: Join(now) RPF: POS0/6/0/0
,10.19.20.20 Flags:
  mdtVPN/A                    00:02:48  fwd Join(00:02:40)

(10.1.7.7,228.8.8.8)SPT SM Up: 00:01:42 JP: Join(00:00:10) RPF: mdtVPN/A
,2.2.2.2 Flags: POS0/6/0/0
                  00:01:42  fwd Join(00:02:47)
```

The final verification is to see if new MDT tunnels are formed after higher volumes of multicast feeds are generated. This can be tested by varying the source and destination addresses of the feeds, as shown below.

```
R7#config t
Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#int f0/0R7(config-if)#ip address 10.1.7.100 255.255.255.0
R7(config-if)#end
R7#

R8#config t
Enter configuration commands, one per line. End with CNTL/Z.
R8(config)#int f0/0R8(config-if)#ip igmp join 228.88.88.88
R7#ping 228.88.88.88 repeat 100000 timeout 0 size 1400

Type escape sequence to abort.
Sending 100000, 1400-byte ICMP Echos to 228.88.88.88, timeout is 0 seconds:
......................................................................
......................................................................
......................................................................
<snip>
R2#show ip pim vrf VPN_A mdt send
MDT-data send list for VRF: VPN_A
  (source, group)                     MDT-data group/num  ref_count (10.1.7.100, 228.88.88.88) 232.0.1.0
          1
```

This new feed has caused a new MDT to form with the MDT Data address of 232.0.1.0. R2 should be the root of this tree, with XR1 as a receiver.

```
R2#show ip mroute 232.0.1.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
 (2.2.2.2, 232.0.1.0)
, 00:03:39/00:03:11, flags: sT Incoming interface: Loopback0
, RPF nbr 0.0.0.0 Outgoing interface list
:
```

```
FastEthernet0/0.24
, Forward/Sparse, 00:03:39/00:03:11

R4#show ip mroute 232.0.1.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(2.2.2.2, 232.0.1.0)
, 00:08:31/00:02:52, flags: sT Incoming interface: FastEthernet0/0.24
, RPF nbr 20.2.4.2 Outgoing interface list
: FastEthernet0/0.46
, Forward/Sparse, 00:03:59/00:02:52
R6#show ip mroute 232.0.1.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(2.2.2.2, 232.0.1.0)
, 00:08:43/00:03:22, flags: sT Incoming interface: FastEthernet0/0.46
, RPF nbr 20.4.6.4 Outgoing interface list
: FastEthernet0/0.619
, Forward/Sparse, 00:04:11/00:03:22
RP/0/0/CPU0:XR1#show pim topology 232.0.1.0
Wed May  2 22:40:20.444 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
```

```
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
        ,232.0.1.0)
SPT SSM Up: 00:04:24 JP: Join(00:00:29) RPF: GigabitEthernet0/1/0/0.619
,20.6.19.6 Flags: Loopback0
                     00:04:24  fwd LI LH
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Tasks (pending update)

Difficulty Rating (10 highest): 6

Lab Overview

The following scenario is a practice lab exam designed to test your skills at configuring Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco's CCIE Service Provider Version 3.0 Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab to complete all the configuration steps, take the time to research each networking technology and gain a deeper understanding of the principles behind its operation.

Lab Instructions

Before starting, ensure that the initial configuration scripts for this lab have been applied. If you have any questions related to the scenario solutions, visit our Online Community.

Refer to the attached diagrams for interface and protocol assignments. Upon completion, all devices in the Service Provider core should have full IP reachability to all networks in the core, and all customer devices should have full IP reachability to other sites belonging to the same customer, unless otherwise explicitly specified.

Lab Do’s and Don’ts

- Do not change or add any IP addresses from the initial configuration unless otherwise specified or required for troubleshooting.
- If additional IP addresses are needed but not specifically permitted by the task, use IP unnumbered.
- Do not change any interface encapsulations unless otherwise specified.
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified.
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified.
- Save your configurations often.

Grading

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to pass the exam. A section must work 100% with the requirements given to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Point Values

This lab is broken into 6 main technology sections, with point values for each section distributed as follows:

Section	Point Value
Bridging & Switching	5
IGP	11
MPLS	16

Section	Point Value
VPN	31
MPLS TE	17
Services	20

GOOD LUCK!

---

1. Bridging & Switching

1.1 VLANs & Trunking

- Configure VLANs and VLAN assignments on SW1 according to the diagram.
- Links on SW1 connecting to R1 – R6 and XR2 should be Network Node Interfaces that are 802.1q trunks.
- Links Fa0/20 and Fa0/21 on SW1 that connect to SW2 should be in an EtherChannel, and be Network Node Interfaces that are 802.1q trunks.

Score: 5 Points

---

2. IGP

2.1 OSPF

- Configure OSPF area 0 on all links in the Service Provider core.
- Advertise the Loopbacks of these routers into OSPF, but do not send hello packets out these interfaces.
- Do not generate Type 2 LSAs for any transit links in the SP core.

Score: 6 Points

2.2 OSPF Security

- Authenticate all OSPF area 0 adjacencies with an MD5 hash of the password **CCIE**.

Score: 5 Points

---

3. MPLS

3.1 LDP

- Configure LDP on all interfaces in the Service Provider core.
- Use the minimum number of commands to accomplish this.

Score: 5 Points

3.2 LDP Security

- Authenticate all LDP adjacencies with an MD5 hash of the password **CCIE**.
- New routers added to the topology at a later time should be authenticated with the default password **DEFAULTMD5**.
- R1 – R6 should not allow new unauthenticated LDP sessions to form.

Score: 5 Points

3.3 LDP Blackhole Prevention

- Additional routers with 10-Gigabit Ethernet links will be added to the core of the IGP network in the near future. Configure the core of the network to avoid using these new routers as transit for MPLS LSPs until it is verified that LDP has converged with them.

Score: 6 Points

---

4. VPN

The Service Provider AS 1284 has been contracted to provide both MPLS L2VPN and MPLS L3VPN to its customers Acme Inc. and ENT LLC via various POPs. Acme has multiple connections to the SP, with the L3VPN terminating at XR1 and R2 being primary, and the L3VPN terminating at R1 and XR2 being secondary. ENT only has single L3VPN connectivity via connections terminating at XR1 and XR2. Customer Edge routers SW1 and SW2 are preconfigured with VRF Lite routing to appear as if they are separate physical customer routers at different attachment points.

Configure the network as follows to provide connectivity between these customer sites.

4.1 VPNv4 BGP

- Configure R5 to peer VPNv4 BGP with PE routers R2, XR1, and XR2.
- Do not negotiate the IPv4 Unicast BGP AF between these peers.

Score: 6 Points

4.2 MPLS L3VPN

- Configure VRF "Acme" on XR1 and R2 for their SW1 and SW2 connections.
- Use Route Distinguishers and Route Targets in the format *Y.Y.Y.Y*:10 on XR1 and R2, where *Y.Y.Y.Y* is their BGP Router-ID.
- Use OSPF as the PE to CE routing protocol for this VPN.
- When complete, Acme Site 1 and Acme Site 2 should have full IP reachability to each other over the L3VPN connection.

Score: 6 Points

4.3 MPLS L2VPN

- Configure an MPLS L2VPN between R1 and XR2 for their R7 and R8 connections.
- Use Frame Relay on the attachment circuit from R1 to R7.
- When complete, R7 and R8 should form an OSPF area 0 adjacency.

Score: 6 Points

4.4 MPLS Path Selection

- Configure the network so that traffic between Acme Site 1 and Acme Site 2 uses the L3VPN as primary, and the L2VPN as secondary.

Score: 7 Points

4.5 MPLS L3VPN

- Configure VRF “ENT” on XR1 and XR2 for their SW2 and SW1 connections.
- Use Route Distinguishers and Route Targets in the format *Y.Y.Y.Y*:20 on XR1 and XR2, where *Y.Y.Y.Y* is their BGP Router-ID.
- Configure EIGRP AS 1 as the PE to CE routing protocol. When complete, ensure that SW1 and SW2 have reachability to each other’s Loopback networks advertised into the VRF.

Score: 6 Points

---

5. MPLS TE

5.1 MPLS TE

- Configure the Service Provider network to support MPLS Traffic Engineering on all links in the core.
- Allow for 90% of the link bandwidths to be reserved by MPLS TE tunnels.

Score: 5 Points

5.2 MPLS TE

- Configure an MPLS TE tunnel from R1 to XR2 and back that is used to route their L2VPN traffic.
- This tunnel should have a 45Mbps bandwidth reservation, and prefer to use the link between R3 and R4 in the transit path.

Score: 6 Points

5.3 MPLS TE Path Protection

- Configure the tunnels between R1 and XR2 so that they are protected against a link failure between R3 and R4.
- The label values for the backup path should be pre-calculated, and should not rely on IGP hold timers expiring before rerouting the path.

Score: 6 Points

---

6. Services

6.1 Multicast L3VPN

- Configure XR1 and R2 to support multicast forwarding between the Acme L3VPN sites.
- XR1 and R2 should use the group address 232.100.100.100 to tunnel multicast traffic over the SP core.
- When complete, you should be able to perform the following verification and receive the highlighted output below:

```
SW2#ping vrf MULTICAST 224.1.2.3

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.1.2.3, timeout is 2 seconds:
.
R8#show ip mroute 224.1.2.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
```

```
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.2.3), 00:00:31/stopped, RP 192.168.0.10, flags: SJCL
  Incoming interface: FastEthernet0/1, RPF nbr 192.168.108.10
  Outgoing interface list:
    Loopback0, Forward/Sparse, 00:00:31/00:02:44
(192.168.7.100, 224.1.2.3), 00:00:11/00:02:50,
flags: LJT
  Incoming interface: FastEthernet0/1, RPF nbr 192.168.108.10
  Outgoing interface list:     Loopback0, Forward/Sparse
, 00:00:12/00:02:47
```

Score: 7 Points

6.2 Multicast Traffic Engineering

- Multicast traffic sourced from servers on the network 192.168.7.0/24 at Acme Site 1 should use the L2VPN link to deliver their traffic to Acme Site 2.
- If the L2VPN link is down, multicast traffic should revert back to using the L3VPN links.
- Do not use static multicast routing to accomplish this.
- When complete, you should be able to perform the following verification and receive the highlighted output below:

```
SW2#ping vrf MULTICAST 224.4.5.6


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.4.5.6, timeout is 2 seconds:
.
R8#show ip mroute 224.4.5.6
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
 (*, 224.4.5.6)
, 00:06:42/00:02:56, RP 192.168.0.10, flags: SJCL Incoming interface: FastEthernet0/1,
RPF nbr 192.168.108.10
  Outgoing interface list:
    Loopback0, Forward/Sparse, 00:06:42/00:02:17
 (192.168.7.100, 224.4.5.6)
, 00:00:03/00:02:56, flags: LJ
Incoming interface: FastEthernet0/0, RPF nbr 192.168.78.7, Mbgp
  Outgoing interface list:     Loopback0
, Forward/Sparse, 00:00:04/00:02:55
```

Score: 7 Points

6.3 QoS

- Configure R1 and XR2 so that traffic coming from the L2VPN customer is rate limited to 45 Mbps.
- Traffic from the L2VPN should be assigned MPLS EXP 3.
- MPLS EXP 3 packets should be guaranteed 45 Mbps of transit in the core.
- Make sure to account for the case when fast reroute is in effect.

Score: 6 Points

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solution 1.1 (pending update)

Task 1.1 Solution

```
SW1:
vlan 13,26,34-35,45,56,78,420,619,920,1019
!
interface FastEthernet0/1
 port-type nni
 switchport mode trunk
 duplex full
 no shutdown
!
interface FastEthernet0/2
 port-type nni
 switchport mode trunk
 duplex full
 no shutdown
!
interface FastEthernet0/3
 port-type nni
 switchport mode trunk
 duplex full
 no shutdown
!
interface FastEthernet0/4
 port-type nni
 switchport mode trunk
 duplex full
 no shutdown
!
interface FastEthernet0/5
 port-type nni
 switchport mode trunk
 duplex full
```

```
 no shutdown
!
interface FastEthernet0/6
 port-type nni
 switchport mode trunk
 duplex full
 no shutdown
!
interface FastEthernet0/8
 switchport access vlan 78
 no shutdown
!
interface Port-channel1
 port-type nni
 switchport mode trunk
!
interface FastEthernet0/20
 port-type nni
 switchport mode trunk
 channel-group 1 mode on
 no shutdown
!
interface FastEthernet0/21
 port-type nni
 switchport mode trunk
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 speed nonegotiate
!
interface GigabitEthernet0/2
 port-type nni
 switchport mode trunk
 speed nonegotiate
```

Task 1.1 Verification

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/22
                                                 Fa0/23, Fa0/24 13    VLAN0013
                        active 26    VLAN0026
                         active 34    VLAN0034
                         active 35    VLAN0035
                         active 45    VLAN0045
                         active 56    VLAN0056
                         active 78    VLAN0078
                         active     Fa0/8 420    VLAN0420
                        active 619    VLAN0619
                        active 920    VLAN0920
                        active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
1019 VLAN1019                         active
```

SW1#show port-type

```
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Fa0/1                        trunk Network   Node Interface
        (nni) Fa0/2                       trunk Network   Node Interface
        (nni) Fa0/3                       trunk Network   Node Interface
        (nni)    Fa0/4                       trunk Network   Node Interface
        (nni)    Fa0/5                       trunk Network   Node Interface
        (nni)    Fa0/6                       trunk Network   Node Interface
        (nni)
Fa0/7                        routed     User Network Interface          (uni)
Fa0/8                        78 User    Network Interface               (uni)
Fa0/9                        1          User Network Interface          (uni)
Fa0/10                       1          User Network Interface          (uni)
Fa0/11                       1          User Network Interface          (uni)
Fa0/12                       1          User Network Interface          (uni)
Fa0/13                       1          User Network Interface          (uni)
Fa0/14                       1          User Network Interface          (uni)
Fa0/15                       1          User Network Interface          (uni)
Fa0/16                       1          User Network Interface          (uni)
Fa0/17                       1          User Network Interface          (uni)
Fa0/18                       1          User Network Interface          (uni)
Fa0/19                       1          User Network Interface          (uni)
Fa0/20                       trunk      Network Node Interface          (nni)
Fa0/21                       trunk      Network Node Interface          (nni)
Fa0/22                       1          User Network Interface          (uni)
Fa0/23                       1          User Network Interface          (uni)
Fa0/24                       1          User Network Interface          (uni)
Gi0/1                        routed     Network Node Interface          (nni)
```

```
Gi0/2                        trunk      Network Node Interface          (nni)
Po1 1                        trunk      Network Node Interface          (nni)
```

```
SW1#show interface trunk
Port           Mode                 Encapsulation  Status        Native vlan
Fa0/1          on                   802.1q         trunking
      1
Fa0/2          on                   802.1q         trunking      1
Fa0/3          on                   802.1q         trunking      1
Fa0/4          on                   802.1q         trunking      1
Fa0/5          on                   802.1q         trunking      1
Fa0/6          on                   802.1q         trunking      1
Gi0/2          on                   802.1q         trunking      1
Po1            on                   802.1q         trunking      1

Port           Vlans allowed on trunk
Fa0/1          1-4094
Fa0/2          1-4094
Fa0/3          1-4094
Fa0/4          1-4094
Fa0/5          1-4094
Fa0/6          1-4094
Gi0/2          1-4094
Po1            1-4094

Port           Vlans allowed and active in management domain
Fa0/1          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/2          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/3          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/4          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/5          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/6          1,13,26,34-35,45,56,78,420,619,920,1019
Gi0/2          1,13,26,34-35,45,56,78,420,619,920,1019
Po1            1,13,26,34-35,45,56,78,420,619,920,1019

Port           Vlans in spanning tree forwarding state and not pruned
Fa0/1          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/2          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/3          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/4          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/5          1,13,26,34-35,45,56,78,420,619,920,1019
Fa0/6          1,13,26,34-35,45,56,78,420,619,920,1019
Gi0/2          1,13,26,34-35,45,56,78,420,619,920,1019
Po1            1,13,26,34-35,45,56,78,420,619,920,1019
```

```
SW1#show etherchannel summary

Flags:  D - down     P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3  S - Layer2
        U - in use  f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:  1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Fa0/20(P)    Fa0/21(P)
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solutions 2.1 - 2.2 (pending update)

Task 2.1 Solution

```
R1:
interface FastEthernet0/0.13
 ip ospf network point-to-point
!
router ospf 1
 network 12.1.3.1 0.0.0.0 area 0
 network 1.1.1.1 0.0.0.0 area 0
 passive-interface Loopback0

R2:
interface FastEthernet0/0.26
 ip ospf network point-to-point
!
router ospf 1
 network 12.2.6.2 0.0.0.0 area 0
 network 2.2.2.2 0.0.0.0 area 0
 passive-interface Loopback0

R3:
interface FastEthernet0/0.13
 ip ospf network point-to-point
!
interface FastEthernet0/0.34
 ip ospf network point-to-point
!
interface FastEthernet0/0.35
 ip ospf network point-to-point
!
```

```
router ospf 1
 network 12.1.3.3 0.0.0.0 area 0
 network 12.3.4.3 0.0.0.0 area 0
 network 12.3.5.3 0.0.0.0 area 0
 network 3.3.3.3 0.0.0.0 area 0
 passive-interface Loopback0

R4:
interface FastEthernet0/0.34
 ip ospf network point-to-point
!
interface FastEthernet0/0.45
 ip ospf network point-to-point
!
interface FastEthernet0/0.420
 ip ospf network point-to-point
!
router ospf 1
 network 12.3.4.4 0.0.0.0 area 0
 network 12.4.5.4 0.0.0.0 area 0
 network 12.4.20.4 0.0.0.0 area 0
 network 4.4.4.4 0.0.0.0 area 0
 passive-interface Loopback0


R5:
interface FastEthernet0/0.35
 ip ospf network point-to-point
!
interface FastEthernet0/0.45
 ip ospf network point-to-point
!
interface FastEthernet0/0.56
 ip ospf network point-to-point
!
router ospf 1
 network 12.3.5.5 0.0.0.0 area 0
 network 12.4.5.5 0.0.0.0 area 0
 network 12.5.6.5 0.0.0.0 area 0
 network 5.5.5.5 0.0.0.0 area 0
 passive-interface Loopback0


R6:
interface FastEthernet0/0.26
 ip ospf network point-to-point
```

```
!
interface FastEthernet0/0.56
 ip ospf network point-to-point
!
interface FastEthernet0/0.619
 ip ospf network point-to-point
!
router ospf 1
 network 12.2.6.6 0.0.0.0 area 0
 network 12.5.6.6 0.0.0.0 area 0
 network 12.6.19.6 0.0.0.0 area 0
 network 6.6.6.6 0.0.0.0 area 0
 passive-interface Loopback0


XR1:
router ospf 1
 area 0
  network point-to-point
   interface Loopback0
    passive enable
  !
  interface GigabitEthernet0/1/0/1.619
  !
 !
!

XR2:
router ospf 1
 area 0
  network point-to-point
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/4/0/0.420
  !
 !
!
```

Task 2.1 Verification

```
R1#show ip ospf neighbor

Neighbor  ID     Pri   State          Dead Time     Address          Interface 3.3.3.3            0   FULL/
    -    00:00:37     12.1.3.3
```

```
FastEthernet0/0.13
R1#show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 1)
 Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#        Checksum Link count
1.1.1.1         1.1.1.1         112         0x80000002  0x006671 3
2.2.2.2         2.2.2.2         92          0x80000002  0x003482 3
3.3.3.3         3.3.3.3         96          0x80000003  0x0024E7 7
4.4.4.4         4.4.4.4         68          0x80000003  0x007C0E 7
5.5.5.5         5.5.5.5         90          0x80000002  0x005B75 7
6.6.6.6         6.6.6.6         78          0x80000002  0x0097D5 7
19.19.19.19     19.19.19.19     79          0x80000002  0x00F8BD 3
20.20.20.20     20.20.20.20     70          0x80000002  0x000EA5 3


R1#show ip route ospf
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
O     2.2.2.2 [110/5] via 12.1.3.3, 00:01:23, FastEthernet0/0.13
    3.0.0.0/32 is subnetted, 1 subnets
O     3.3.3.3 [110/2] via 12.1.3.3, 00:01:53, FastEthernet0/0.13
    4.0.0.0/32 is subnetted, 1 subnets
O     4.4.4.4 [110/3] via 12.1.3.3, 00:01:43, FastEthernet0/0.13
    5.0.0.0/32 is subnetted, 1 subnets
O     5.5.5.5 [110/3] via 12.1.3.3, 00:01:33, FastEthernet0/0.13
    6.0.0.0/32 is subnetted, 1 subnets
O     6.6.6.6 [110/4] via 12.1.3.3, 00:01:23, FastEthernet0/0.13
    12.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O     12.2.6.0/24 [110/4] via 12.1.3.3, 00:01:23, FastEthernet0/0.13
O     12.3.4.0/24 [110/2] via 12.1.3.3, 00:01:53, FastEthernet0/0.13
O     12.3.5.0/24 [110/2] via 12.1.3.3, 00:01:53, FastEthernet0/0.13
O     12.4.5.0/24 [110/3] via 12.1.3.3, 00:01:03, FastEthernet0/0.13
O     12.4.20.0/24 [110/3] via 12.1.3.3, 00:01:43, FastEthernet0/0.13
O     12.5.6.0/24 [110/3] via 12.1.3.3, 00:01:33, FastEthernet0/0.13
```

```
O     12.6.19.0/24 [110/4] via 12.1.3.3, 00:01:23, FastEthernet0/0.13
    19.0.0.0/32 is subnetted, 1 subnets
O     19.19.19.19 [110/5] via 12.1.3.3, 00:01:13, FastEthernet0/0.13
    20.0.0.0/32 is subnetted, 1 subnets
O     20.20.20.20 [110/4] via 12.1.3.3, 00:01:03, FastEthernet0/0.13
```

RP/0/0/CPU0:XR1#show ospf neighbor

```
Fri May 4 17:02:56.360 UTC

* Indicates MADJ interface

Neighbors for   OSPF 1

Neighbor ID       Pri   State          Dead Time    Address         Interface 6.6.6.6    1   FULL/    -
 00:00:38    12.6.19.6
GigabitEthernet0/1/0/1.619
Neighbor is up for 00:02:00

Total neighbor count: 1
```

RP/0/0/CPU0:XR1#show ospf database

```
Fri May 4 17:03:00.015 UTC



           OSPF Router with ID (19.19.19.19) (Process ID 1)
 Router Link States (Area 0)

Link ID        ADV Router      Age         Seq#       Checksum Link count
1.1.1.1        1.1.1.1         163         0x80000002 0x006671 3
2.2.2.2        2.2.2.2         137         0x80000002 0x003482 3
3.3.3.3        3.3.3.3         144         0x80000003 0x0024e7 7
4.4.4.4        4.4.4.4         117         0x80000003 0x007c0e 7
5.5.5.5        5.5.5.5         137         0x80000002 0x005b75 7
6.6.6.6        6.6.6.6         124         0x80000002 0x0097d5 7
19.19.19.19    19.19.19.19     123         0x80000002 0x00f8bd 3
20.20.20.20    20.20.20.20     118         0x80000002 0x000ea5 3
```

RP/0/0/CPU0:XR1#show route ospf

```
Fri May 4 17:03:02.661 UTC

O   1.1.1.1/32 [110/5] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   2.2.2.2/32 [110/3] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   3.3.3.3/32 [110/4] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   4.4.4.4/32 [110/4] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   5.5.5.5/32 [110/3] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
```

```
O   6.6.6.6/32 [110/2] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.1.3.0/24 [110/4] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.2.6.0/24 [110/2] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.3.4.0/24 [110/4] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.3.5.0/24 [110/3] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.4.5.0/24 [110/3] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.4.20.0/24 [110/4] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   12.5.6.0/24 [110/2] via 12.6.19.6, 00:02:05, GigabitEthernet0/1/0/1.619
O   20.20.20.20/32 [110/5] via 12.6.19.6, 00:01:52, GigabitEthernet0/1/0/1.619
```

Task 2.2 Solution

```
R1:
interface FastEthernet0/0.13
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
 area 0 authentication message-digest

R2:
interface FastEthernet0/0.26
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
 area 0 authentication message-digest

R3:
interface FastEthernet0/0.13
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.34
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.35
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
area 0 authentication message-digest

R4:
interface FastEthernet0/0.34
 ip ospf message-digest-key 1 md5 0 CCIE
!
```

```
interface FastEthernet0/0.45
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.420
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
 area 0 authentication message-digest

R5:
interface FastEthernet0/0.35
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.45
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.56
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
 area 0 authentication message-digest

R6:
interface FastEthernet0/0.26
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.56
 ip ospf message-digest-key 1 md5 0 CCIE
!
interface FastEthernet0/0.619
 ip ospf message-digest-key 1 md5 0 CCIE
!
router ospf 1
 area 0 authentication message-digest

XR1:
router ospf 1
 area 0
  authentication message-digest
   interface GigabitEthernet0/1/0/1.619
    message-digest-key 1 md5 CCIE

XR2:
router ospf 1
 area 0
  authentication message-digest interface GigabitEthernet0/4/0/0.420
```

```
    message-digest-key 1 md5 CCIE
```

Task 2.2 Verification

```
R1#show ip ospf interface
 Loopback0 is up, line protocol is up
   Internet Address 1.1.1.1/32, Area 0
   Process ID 1, Router ID 1.1.1.1, Network Type LOOPBACK, Cost: 1
   Topology-MTID Cost    Disabled    Shutdown    Topology Name
         0   1   no  no  Base
   Loopback interface is treated as a stub Host
 FastEthernet0/0.13 is up, line protocol is up
   Internet Address 12.1.3.1/24, Area 0
   Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
   Topology-MTID Cost    Disabled    Shutdown    Topology Name
         0   1   no  no  Base
   Transmit Delay is 1 sec, State POINT_TO_POINT
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     oob-resync timeout 40
     Hello due in 00:00:04
   Supports Link-local Signaling (LLS)
   Cisco NSF helper support enabled
   IETF NSF helper support enabled
   Index 1/1, flood queue length 0
   Next 0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 1
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 3.3.3.3
   Suppress hello for 0 neighbor(s)  Message digest authentication enabled
 Youngest key id is 1
 RP/0/0/CPU0:XR1#show ospf interface
 Fri May 4 17:05:16.204 UTC
 Interfaces for OSPF 1
 Loopback0 is up, line protocol is up
   Internet Address 19.19.19.19/32, Area 0
   Process ID 1, Router ID 19.19.19.19, Network Type LOOPBACK, Cost: 1
   Loopback interface is treated as a stub Host
 GigabitEthernet0/1/0/1.619 is up, line protocol is up
   Internet Address 12.6.19.19/24, Area 0
   Process ID 1, Router ID 19.19.19.19, Network Type POINT_TO_POINT, Cost: 1
   Transmit Delay is 1 sec, State POINT_TO_POINT, MTU 1500, MaxPktSz 1500
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:05
```

```
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 7
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 6.6.6.6
  Suppress hello for 0 neighbor(s)  Message digest authentication enabled
Youngest key id is 1

  Multi-area interface Count is 0
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solutions 3.1 - 3.3 (pending update)

Task 3.1
Task 3.2
Task 3.3

Task 3.1 Solution

```
R1:
router ospf 1
 mpls ldp autoconfig

R2:
router ospf 1
 mpls ldp autoconfig

R3:
router ospf 1
 mpls ldp autoconfig

R4:
router ospf 1
 mpls ldp autoconfig

R5:
router ospf 1
 mpls ldp autoconfig

R6:
router ospf 1
 mpls ldp autoconfig

XR1:
router ospf 1
 area 0
```

```
  mpls ldp auto-config
!
!
mpls ldp

XR2:
router ospf 1
 area 0
  mpls ldp auto-config
 !
!
mpls ldp
```

Task 3.1 Verification

```
R1#show mpls interfaces
Interface              IP              Tunnel    BGP  Static  Operational
FastEthernet0/0.13         Yes (ldp)
     No         No    No       Yes
RP/0/0/CPU0:XR1#show mpls interfaces
Fri May 4 17:07:43.890 UTC Interface LDP
      Tunnel   Enabled
-------------------------- -------- -------- --------GigabitEthernet0/1/0/1.619 Yes
      No        Yes
```

Task 3.2 Solution

```
R1:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 3.3.3.3 password CCIE

R2:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 6.6.6.6 password CCIE

R3:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 1.1.1.1 password CCIE
```

```
mpls ldp neighbor 4.4.4.4 password CCIE
mpls ldp neighbor 5.5.5.5 password CCIE

R4:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 3.3.3.3 password CCIE
mpls ldp neighbor 5.5.5.5 password CCIE
mpls ldp neighbor 20.20.20.20 password CCIE

R5:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 3.3.3.3 password CCIE
mpls ldp neighbor 4.4.4.4 password CCIE
mpls ldp neighbor 6.6.6.6 password CCIE

R6:
mpls ldp password required
mpls ldp password fallback DEFAULTMD5
mpls ldp neighbor 2.2.2.2 password CCIE
mpls ldp neighbor 5.5.5.5 password CCIE
mpls ldp neighbor 19.19.19.19 password CCIE

XR1:
mpls ldp
 neighbor password clear DEFAULTMD5
 neighbor 6.6.6.6 password clear CCIE

XR2:
mpls ldp
 neighbor password clear DEFAULTMD5
 neighbor 4.4.4.4 password clear CCIE
```

Task 3.2 Verification

```
R1#show mpls ldp neighbor detail
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 3.3.3.3.48274 - 1.1.1.1.646; MD5 on
 Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 20/20; Downstream; Last TIB rev sent 32
        Up time: 00:00:53; UID: 2; Peer Id 0;
        LDP discovery sources:
          FastEthernet0/0.13; Src IP addr: 12.1.3.3
```

```
          holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          12.1.3.3  12.3.4.3    12.3.5.3    3.3.3.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
        Capabilities Sent:
          [ICCP (type 0x0405) MajVer 1 MinVer 0]
          [Dynamic Announcement (0x0506)]
          [mLDP Point-to-Multipoint (0x0508)]
          [mLDP Multipoint-to-Multipoint (0x0509)]
        Capabilities Received:
          [ICCP (type 0x0405) MajVer 1 MinVer 0]
          [Dynamic Announcement (0x0506)]
          [mLDP Point-to-Multipoint (0x0508)]
          [mLDP Multipoint-to-Multipoint (0x0509)]
RP/0/0/CPU0:XR1#show mpls ldp neighbor detail
Fri May 4 17:10:17.259 UTC

Peer LDP Identifier: 6.6.6.6:0  TCP connection: 6.6.6.6:646 - 19.19.19.19:32413; MD5 on

  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 22/20
  Up time: 00:01:05
  LDP Discovery Sources:
    GigabitEthernet0/1/0/1.619
  Addresses bound to this peer:
    6.6.6.6 12.2.6.6    12.5.6.6    12.6.19.6
  Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
  NSR: Disabled
```

Task 3.3 Solution

```
R1:
router ospf 1
 mpls ldp sync

R2:
router ospf 1
 mpls ldp sync

R3:
router ospf 1
 mpls ldp sync
```

```
R4:
router ospf 1
 mpls ldp sync

R5:
router ospf 1
 mpls ldp sync

R6:
router ospf 1
 mpls ldp sync

XR1:
router ospf 1
 mpls ldp sync

XR2:
router ospf 1
 mpls ldp sync
```

Task 3.3 Verification

```
R1#show mpls ldp igp sync
    FastEthernet0/0.13: LDP configured; LDP-IGP Synchronization enabled.
 Sync status: sync achieved; peer reachable.

        Sync delay time: 0 seconds (0 seconds left)
        IGP holddown time: infinite.
        Peer LDP Ident: 3.3.3.3:0
        IGP enabled: OSPF 1
RP/0/0/CPU0:XR1#show mpls ldp igp sync
Fri May 4 17:11:55.030 UTC

GigabitEthernet0/1/0/1.619:  Sync status: Ready

  Peers:
    6.6.6.6:0
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solutions 4.1 - 4.5 (pending update)

Task 4.1 Solution

```
R2:
router bgp 1284
 no bgp default ipv4-unicast
 neighbor 5.5.5.5 remote-as 1284
 neighbor 5.5.5.5 update-source Loopback0
!
address-family vpnv4 unicast
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 route-reflector-client

R5:
router bgp 1284
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 1284
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 19.19.19.19 remote-as 1284
 neighbor 19.19.19.19 update-source Loopback0
 neighbor 20.20.20.20 remote-as 1284
 neighbor 20.20.20.20 update-source Loopback0
!
address-family vpnv4 unicast neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 route-reflector-client
 neighbor 19.19.19.19 activate
 neighbor 19.19.19.19 route-reflector-client
 neighbor 20.20.20.20 activate
```

```
 neighbor 20.20.20.20 route-reflector-client

XR1:
router bgp 1284
 address-family vpnv4 unicast
 !
neighbor 5.5.5.5
 remote-as 1284
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
!

XR2:
router bgp 1284
 address-family vpnv4 unicast
 !
 neighbor 5.5.5.5
  remote-as 1284
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
!
```

Task 4.1 Verification

```
R5#show bgp vpnv4 unicast all summary
BGP router identifier 5.5.5.5, local AS number 1284
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2.2.2.2         4         1284       2       2        1    0    0 00:00:33        0
19.19.19.19     4         1284       2       2        1    0    0 00:00:19        0
20.20.20.20     4         1284       2       2        1    0    0 00:00:05        0
RP/0/0/CPU0:XR1#sh bgp vpnv4 unicast summary

Fri May 4 17:13:58.913 UTC
BGP router identifier 19.19.19.19, local AS number 1284
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0
```

```
BGP main routing table version 1
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB    LabelVer    ImportVer    SendTblVer    StandbyVer
Speaker               1          1           1            1             1             1

Neighbor        Spk    AS MsgRcvd MsgSent    TblVer    InQ OutQ    Up/Down    St/PfxRcd
5.5.5.5           0  1284       4       3         1      0    0   00:01:05            0
```

Task 4.2 Solution

```
R2:
vrf definition Acme
 rd 2.2.2.2:10
 route-target export 2.2.2.2:10
 route-target import 19.19.19.19:10
 !
 address-family ipv4
 exit-address-family
!
interface FastEthernet1/0
 vrf forwarding Acme
 ip address 192.168.210.2 255.255.255.0
!
router ospf 10 vrf Acme
 redistribute bgp 1284 subnets
 network 192.168.210.2 0.0.0.0 area 0
!
router bgp 1284
 address-family ipv4 vrf Acme
  redistribute ospf 10 vrf Acme
 exit-address-family

XR1:
vrf Acme
 address-family ipv4 unicast
  import route-target
   2.2.2.2:10
  !
  export route-target
```

```
   19.19.19.19:10
  !
 !
!
interface GigabitEthernet0/1/0/0
 no ipv4 address
 vrf Acme
 ipv4 address 192.168.199.19 255.255.255.0
!
router ospf 10
 vrf Acme
  redistribute bgp 1284
  area 0
   interface GigabitEthernet0/1/0/0
!
router bgp 1284
 vrf Acme
  rd 19.19.19.19:10
  address-family ipv4 unicast
   redistribute ospf 10
```

Task 4.2 Verification

```
R2#show ip vrf detail
VRF Acme (VRF Id = 1); default RD 2.2.2.2:10
; default VPNID <not set>
  Interfaces:
    Fa1/0
VRF Table ID = 1 Export VPN route-target communities
RT:2.2.2.2:10
Import VPN route-target communities
RT:19.19.19.19:10
No import route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix
RP/0/0/CPU0:XR1#show vrf all detail
Fri May 4 17:16:38.416 UTC
VRF Acme; RD 19.19.19.19:10
; VPN ID not set
Description not set
Interfaces:
  GigabitEthernet0/1/0/0
Address family IPV4 Unicast
```

```
 Import VPN route-target communities:
  RT:2.2.2.2:10
 Export VPN route-target communities:
   RT:19.19.19.19:10
  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
```

R2#show ip ospf 10 neighbor

```
Neighbor ID     Pri   State           Dead Time    Address         Interface
192.168.0.10      1   FULL/DR         00:00:31     192.168.210.10   FastEthernet1/0
```

RP/0/0/CPU0:XR1#show ospf vrf Acme neighbor

```
Fri May 4 17:17:44.904 UTC

* Indicates MADJ interface

Neighbors for OSPF 10, VRF Acme

Neighbor ID     Pri   State            Dead Time    Address         Interface
192.168.0.9       1   FULL/DR          00:00:36     192.168.199.9
GigabitEthernet0/1/0/0
    Neighbor is up for 00:02:46

Total neighbor count: 1
```

R2#show bgp vpnv4 unicast vrf Acme

```
BGP table version is 16, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 2.2.2.2:10 (default for vrf Acme)
*>i7.7.7.7/32       19.19.19.19         3       100        0 ?
*> 8.8.8.8/32       192.168.210.10      3              32768 ?
*>i192.168.0.9/32   19.19.19.19         2       100        0 ?
*> 192.168.0.10/32  192.168.210.10      2              32768 ?
*>i192.168.7.0      19.19.19.19         3       100        0 ?
*> 192.168.78.0     192.168.210.10      3              32768 ?
*>i192.168.79.0     19.19.19.19         2       100        0 ?
*> 192.168.108.0    192.168.210.10      2              32768 ?
```

```
*>i192.168.199.0    19.19.19.19         0       100        0 ?
*> 192.168.210.0    0.0.0.0             0              32768 ?
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf Acme
Fri May 4 17:20:20.160 UTC
BGP router identifier 19.19.19.19, local AS number 1284
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0
BGP main routing table version 16
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 19.19.19.19:10 (default for vrf Acme)
*> 7.7.7.7/32         192.168.199.9            3         32768 ?
*>i8.8.8.8/32         2.2.2.2                  3    100      0 ?
*> 192.168.0.9/32     192.168.199.9            2         32768 ?
*>i192.168.0.10/32    2.2.2.2                  2    100      0 ?
*> 192.168.7.0/24     192.168.199.9            3         32768 ?
*>i192.168.78.0/24    2.2.2.2                  3    100      0 ?
*> 192.168.79.0/24    192.168.199.9            2         32768 ?
*>i192.168.108.0/24   2.2.2.2                  2    100      0 ?
*> 192.168.199.0/24   0.0.0.0                  0         32768 ?
*>i192.168.210.0/24   2.2.2.2                  0    100      0 ?

Processed 10 prefixes, 10 paths



#B#R2#show ip route vrf Acme#B#

Routing Table: Acme
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      7.0.0.0/32 is subnetted, 1 subnets
B        7.7.7.7 [200/3] via 19.19.19.19, 00:05:48
```

```
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/3] via 192.168.210.10, 00:06:04, FastEthernet1/0
      192.168.0.0/32 is subnetted, 2 subnets
B        192.168.0.9 [200/2] via 19.19.19.19, 00:05:48
O        192.168.0.10 [110/2] via 192.168.210.10, 00:06:04, FastEthernet1/0
B     192.168.7.0/24 [200/3] via 19.19.19.19, 00:05:48
O     192.168.78.0/24 [110/3] via 192.168.210.10, 00:06:04, FastEthernet1/0
B     192.168.79.0/24 [200/2] via 19.19.19.19, 00:05:48
O     192.168.108.0/24 [110/2] via 192.168.210.10, 00:06:04, FastEthernet1/0
B     192.168.199.0/24 [200/0] via 19.19.19.19, 00:05:56
      192.168.210.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.210.0/24 is directly connected, FastEthernet1/0
L        192.168.210.2/32 is directly connected, FastEthernet1/0

#B#RP/0/0/CPU0:XR1#show route vrf Acme#B#
Fri May 4 17:21:02.226 UTC

Codes: C - connected, S - static, R - RIP, 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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G - DAGR
       A - access/subscriber

Gateway of last resort is not set

O    7.7.7.7/32 [110/3] via 192.168.199.9, 00:06:02, GigabitEthernet0/1/0/0
B    8.8.8.8/32 [200/3] via 2.2.2.2 (nexthop in vrf default), 00:06:05
O    192.168.0.9/32 [110/2] via 192.168.199.9, 00:06:02, GigabitEthernet0/1/0/0
B    192.168.0.10/32 [200/2] via 2.2.2.2 (nexthop in vrf default), 00:06:05
O    192.168.7.0/24 [110/3] via 192.168.199.9, 00:06:02, GigabitEthernet0/1/0/0
B    192.168.78.0/24 [200/3] via 2.2.2.2 (nexthop in vrf default), 00:06:05
O    192.168.79.0/24 [110/2] via 192.168.199.9, 00:06:02, GigabitEthernet0/1/0/0
B    192.168.108.0/24 [200/2] via 2.2.2.2 (nexthop in vrf default), 00:06:05
C    192.168.199.0/24 is directly connected, 00:06:11, GigabitEthernet0/1/0/0
L    192.168.199.19/32 is directly connected, 00:06:11, GigabitEthernet0/1/0/0
B    192.168.210.0/24 [200/0] via 2.2.2.2 (nexthop in vrf default), 00:05:35
```

R7#show ip route ospf

```
O E2 192.168.210.0/24 [110/1] via 192.168.79.9, 00:00:01, FastEthernet0/0
O E2 192.168.78.0/24 [110/3] via 192.168.79.9, 00:00:24, FastEthernet0/0
O E2 192.168.108.0/24 [110/2] via 192.168.79.9, 00:00:24, FastEthernet0/0
O    192.168.199.0/24 [110/2] via 192.168.79.9, 00:00:24, FastEthernet0/0
     8.0.0.0/32 is subnetted, 1 subnets
```

```
O E2    8.8.8.8 [110/3] via 192.168.79.9, 00:00:24, FastEthernet0/0
     192.168.0.0/32 is subnetted, 2 subnets
O       192.168.0.9 [110/2] via 192.168.79.9, 00:00:24, FastEthernet0/0
O E2    192.168.0.10 [110/2] via 192.168.79.9, 00:00:24, FastEthernet0/0
R7#traceroute 8.8.8.8


Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 192.168.79.9 0 msec 0 msec 0 msec
  2 192.168.199.19 4 msec 4 msec 4 msec
  3 12.6.19.6 0 msec 4 msec 4 msec
  4 192.168.210.2 0 msec 4 msec 0 msec
  5 192.168.210.10 4 msec 4 msec 0 msec
  6 192.168.108.8 4 msec *  0 msec
```

Task 4.3 Solution

```
R1:
frame-relay switching
!
pseudowire-class R7_R8_L2VPN
 encapsulation mpls
 interworking ip
!
interface Serial2/0
 encapsulation frame-relay
 clock rate 64000
 frame-relay intf-type dce
 no shutdown
!
connect FR Serial2/0 100 l2transport
 xconnect 20.20.20.20 1 pw-class R7_R8_L2VPN

R8:
interface FastEthernet0/0
 ip ospf network point-to-point

XR2:
interface GigabitEthernet0/4/0/1
 no cdp
 l2transport
```

```
 !
!
l2vpn
 pw-class R7_R8_L2VPN
 encapsulation mpls
  !
 !
xconnect group R7_TO_R8_L2VPN_GROUP
 p2p AC_TO_R8
  interworking ipv4
  interface GigabitEthernet0/4/0/1
  neighbor 1.1.1.1
   pw-id 1 pw-class R7_R8_L2VPN
```

Task 4.3 Verification

```
R1#show mpls ldp neighbor 20.20.20.20
    Peer LDP Ident: 20.20.20.20:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 20.20.20.20.40601 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 22/23; Downstream
        Up time: 00:02:13
        LDP discovery sources: Targeted Hello 1.1.1.1 -> 20.20.20.20
, active, passive
        Addresses bound to peer LDP Ident:
          20.20.20.20     12.4.20.20      10.0.0.20
RP/0/3/CPU0:XR2#show mpls ldp neighbor 1.1.1.1
Fri May 4 17:24:51.571 UTC

Peer LDP Identifier: 1.1.1.1:0  TCP connection: 1.1.1.1:646 - 20.20.20.20:40601; MD5 on
  Graceful Restart: No Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 23/22
  Up time: 00:02:27
  LDP Discovery Sources: Targeted Hello (20.20.20.20 -> 1.1.1.1, active)

  Addresses bound to this peer:
    1.1.1.1          12.1.3.1
R1#show mpls l2transport vc detail
Local interface: Se2/0 up, line protocol up, FR DLCI 100 up
  Interworking type is IP
 Destination address: 20.20.20.20
, VC ID: 1, VC status: up     Output interface: Fa0/0.13, imposed label stack {27 16014}

    Preferred path: not configured
    Default path: active
```

```
    Next hop: 12.1.3.3
  Create time: 00:03:36, last status change time: 00:03:23
  Signaling protocol: LDP, peer 20.20.20.20:0 up
Targeted Hello: 1.1.1.1(LDP Id) -> 20.20.20.20, LDP is UP
    Status TLV support (local/remote)   : enabled/not supported
      LDP route watch   : enabled
      Label/status state machine    : established, LruRru
      Last local dataplane  status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local LDP TLV status sent: No fault
      Last remote LDP TLV status rcvd: Not sent
      Last remote LDP ADJ   status rcvd: No fault
    MPLS VC labels: local 30, remote 16014
    Group ID: local 0, remote 83887104
    MTU: local 1500, remote 1500
    Remote interface description: GigabitEthernet0_4_0_1
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VC statistics:
    transit packet totals: receive 49, send 46
    transit byte totals:   receive 4448, send 5828
    transit packet drops:  receive 0, seq error 0, send 0


RP/0/3/CPU0:XR2#show l2vpn xconnect detail
Fri May 4 17:26:49.356 UTC
Group R7_TO_R8_L2VPN_GROUP, XC AC_TO_R8, state is up; Interworking IPv4
 AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking IPv4
    Statistics:
      packets: received 59, sent 54
      bytes: received 6018, sent 5036 PW: neighbor 1.1.1.1, PW ID 1, state is up ( established )
    PW class R7_R8_L2VPN, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type IP, control word enabled, interworking IPv4
    PW backup disable delay 0 sec
    Sequencing not set

    MPLS         Local                          Remote
    ------------ ------------------------------ -----------------------------
    Label        16014                          30
    Group ID     0x5000400                      0x0
    Interface    GigabitEthernet0/4/0/1         unknown
    MTU          1500                           1500
```

```
    Control word enabled                       enabled
    PW type      IP                            IP
    VCCV CV type 0x2                           0x2
                 (LSP ping verification)       (LSP ping verification)
    VCCV CC type 0x7                           0x7
                 (control word)                (control word)
                 (router alert label)          (router alert label)
                 (TTL expiry)                  (TTL expiry)
    ------------ ------------------------------ -----------------------------
  MIB cpwVcIndex: 1
  Create time: 04/05/2012 17:22:24 (00:04:25 ago)
  Last time status changed: 04/05/2012 17:22:25 (00:04:23 ago)
  Statistics:
    packets: received 54, sent 59
    bytes: received 5036, sent 6018
R7#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address         Interface
192.168.0.9      1   FULL/DR         00:00:33    192.168.79.9    FastEthernet0/0
8.8.8.8          0   FULL/  -        00:00:39    192.168.78.8  Serial0/0.100
R7#show ip route ospf
O      192.168.210.0/24 [110/66] via 192.168.78.8, 00:00:47, Serial0/0.100
O      192.168.108.0/24 [110/65] via 192.168.78.8, 00:00:47, Serial0/0.100
O      192.168.199.0/24 [110/2] via 192.168.79.9, 00:00:47, FastEthernet0/0
       8.0.0.0/32 is subnetted, 1 subnets
O       8.8.8.8 [110/65] via 192.168.78.8, 00:00:47, Serial0/0.100

       192.168.0.0/32 is subnetted, 2 subnets
O         192.168.0.9 [110/2] via 192.168.79.9, 00:00:47, FastEthernet0/0
O         192.168.0.10 [110/66] via 192.168.78.8, 00:00:47, Serial0/0.100
```

Task 4.4 Solution

```
R2:
interface Loopback192
 vrf forwarding Acme
 ip address 192.168.2.2 255.255.255.255
!
router ospf 10 vrf Acme
 area 0 sham-link 192.168.2.2 192.168.19.19
!
router bgp 1284
 address-family ipv4 vrf Acme
```

```
  network 192.168.2.2 mask 255.255.255.255

R7:
interface Serial0/0.100 point-to-point
 ip ospf cost 100

R8:
interface FastEthernet0/0
 ip ospf cost 100

XR1:
interface Loopback192
 vrf Acme
 ipv4 address 192.168.19.19 255.255.255.255
!
router ospf 10
 vrf Acme
  area 0
   sham-link 192.168.19.19 192.168.2.2
   !
  !
 !
!
router bgp 1284
 vrf Acme
  address-family ipv4 unicast
   network 192.168.19.19/32
   !
  !
!
```

Task 4.4 Verification

```
R2#show ip ospf sham-links
 Sham Link OSPF_SL0 to address 192.168.19.19 is up

Area 0 source address 192.168.2.2
   Run as demand circuit
  DoNotAge LSA allowed. Cost of using 1 State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Hello due in 00:00:03
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
```

```
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
RP/0/0/CPU0:XR1#show ospf vrf Acme sham-links
Fri May 4 17:29:24.545 UTC

Sham Links for OSPF 10, VRF Acme
Sham Link OSPF_SL0 to address 192.168.2.2 is up
Area 0, source address 192.168.19.19
IfIndex = 2
  Run as demand circuit
  DoNotAge LSA allowed., Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency State FULL (Hello suppressed)
    Number of DBD retrans during last exchange 0
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0(0)/0(0) Next 0(0)/0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
R7#show ip route ospf
O     192.168.210.0/24 [110/4] via 192.168.79.9, 00:01:22, FastEthernet0/0
O     192.168.108.0/24 [110/5] via 192.168.79.9, 00:01:22, FastEthernet0/0
O     192.168.199.0/24 [110/2] via 192.168.79.9, 00:01:22, FastEthernet0/0
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/6] via 192.168.79.9, 00:01:22, FastEthernet0/0
      192.168.0.0/32 is subnetted, 2 subnets
O        192.168.0.9 [110/2] via 192.168.79.9, 00:01:22, FastEthernet0/0
O        192.168.0.10 [110/5] via 192.168.79.9, 00:01:22, FastEthernet0/0
      192.168.2.0/32 is subnetted, 1 subnets
O E2     192.168.2.2 [110/1] via 192.168.79.9, 00:01:22, FastEthernet0/0
      192.168.19.0/32 is subnetted, 1 subnets
O E2     192.168.19.19 [110/1] via 192.168.79.9, 00:01:22, FastEthernet0/0

R7#traceroute 8.8.8.8



Type escape sequence to abort.
Tracing the route to 8.8.8.8

1 192.168.79.9 0 msec 0 msec 0 msec
2 192.168.199.19 4 msec 0 msec 4 msec
3 12.6.19.6 4 msec 0 msec 0 msec 4 msec
4 192.168.210.2 0 msec 0 msec 0 msec
5 192.168.210.10 0 msec 4 msec 4 msec
```

```
6 192.168.108.8 4 msec *    0 msec
```

Task 4.5 Solution

```
XR1:
vrf ENT
 address-family ipv4 unicast
  import route-target
   20.20.20.20:20
  !
  export route-target
   19.19.19.19:20
  !
 !
!
interface GigabitEthernet0/1/0/1.1019
 no ipv4 address
 vrf ENT
 ipv4 address 10.1.0.19 255.255.255.0
!
router bgp 1284
 vrf ENT
  rd 19.19.19.19:20
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
router eigrp 65535
 vrf ENT
  address-family ipv4
   autonomous-system 1
   redistribute bgp 1284
   interface GigabitEthernet0/1/0/1.1019
   !
  !
 !
!

XR2:
vrf ENT
 address-family ipv4 unicast
  import route-target
```

```
  19.19.19.19:20
  !
 export route-target
  20.20.20.20:20
  !
 !
!
interface GigabitEthernet0/4/0/0.920
 no ipv4 address
 vrf ENT
 ipv4 address 10.0.0.20 255.255.255.0
!
router bgp 1284
 vrf ENT
  rd 20.20.20.20:20
  address-family ipv4 unicast
   redistribute eigrp 1
  !
 !
!
router eigrp 65535
 vrf ENT
  address-family ipv4
   autonomous-system 1
   redistribute bgp 1284
   interface GigabitEthernet0/4/0/0.920
   !
  !
 !
!
```

Task 4.5 Verification

```
RP/0/0/CPU0:XR1#show vrf ENT detail
Fri May 4 17:34:44.924 UTC
VRF ENT; RD 19.19.19.19:20
; VPN ID not set
Description not set
Interfaces:
  GigabitEthernet0/1/0/1.1019
Address family IPV4 Unicast Import VPN route-target communities:
RT:20.20.20.20:20
Export VPN route-target communities:
```

```
RT:19.19.19.19:20

  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
```

RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf ENT

```
Fri May 4 17:35:56.177 UTC
BGP router identifier 19.19.19.19, local AS number 1284
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0
BGP main routing table version 70
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 19.19.19.19:20 (default for vrf ENT)
*>i10.0.0.0/24        20.20.20.20              0    100      0 ?
*> 10.1.0.0/24        0.0.0.0                  0         32768 ?
*>i10.9.9.9/32        20.20.20.20         130816    100      0 ?
*> 10.10.10.10/32     10.1.0.10           130816         32768 ?

Processed 4 prefixes, 4 paths



RP/0/0/CPU0:XR1#show route vrf ENT
Fri May 4 17:36:11.756 UTC

Codes: C - connected, S - static, R - RIP, 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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G - DAGR
        A - access/subscriber

Gateway of last resort is not set

B    10.0.0.0/24 [200/0] via 20.20.20.20 (nexthop in vrf default), 00:01:45
```

```
C    10.1.0.0/24 is directly connected, 00:01:52, GigabitEthernet0/1/0/1.1019
L    10.1.0.19/32 is directly connected, 00:01:52, GigabitEthernet0/1/0/1.1019
B  10.9.9.9/32 [200/130816] via 20.20.20.20 (nexthop in vrf default), 00:01:36
D    10.10.10.10/32 [90/130816] via 10.1.0.10, 00:01:32,
GigabitEthernet0/1/0/1.1019
SW2#show ip route vrf ENT

Routing Table: ENT
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

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.10.10/32 is directly connected, Loopback10
D      10.9.9.9/32 [90/131072] via 10.1.0.19, 00:03:05, Vlan1019
D       10.0.0.0/24 [90/3072] via 10.1.0.19, 00:03:15, Vlan1019
C       10.1.0.0/24 is directly connected, Vlan1019
SW2#ping vrf ENT 10.9.9.9


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
SW2#
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solutions 5.1 - 5.3 (pending update)

Task 5.1 Solution

```
R1:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.13
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R2:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.26
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.13
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.35
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.420
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.35
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.45
 mpls traffic-eng tunnels
```

```
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R6:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.26
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
interface FastEthernet0/0.619
 mpls traffic-eng tunnels
 ip rsvp bandwidth percent 90
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

XR1:
router ospf 1
 area 0
  mpls traffic-eng
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/1.619
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/1.619
 !
!

XR2:
router ospf 1
 area 0
  mpls traffic-eng
 !
 mpls traffic-eng router-id Loopback0
```

```
!
rsvp
 interface GigabitEthernet0/4/0/0.420
  bandwidth 900000
 !
mpls traffic-eng
 interface GigabitEthernet0/4/0/0.420
 !
!
```

Task 5.1 Verification

```
R1#show ip rsvp interface
interface    rsvp       allocated   i/f max    flow max sub max
Fa0/0        ena        0           0          0        0
Fa0/0.13     ena        0           90M        90M      0

RP/0/3/CPU0:XR2#show rsvp interface
Fri May 4 17:53:59.494 UTC

*: RDM: Default I/F B/W %: 75% [default] (max resv/bc0), 0% [default] (bc1)

Interface   MaxBW (bps)  MaxFlow (bps) Allocated (bps)      MaxSub (bps)
----------- ------------ ------------- -------------------- -------------
Gi0/4/0/0.420       900M          900M              0 ( 0%)            0*
R1#show mpls traffic-eng topology brief
My_System_id: 1.1.1.1 (ospf 1  area 0)

Signalling error holddown: 10 sec Global Link Generation 17

IGP Id: 1.1.1.1, MPLS TE Id:1.1.1.1 Router Node (ospf 1 area 0)
      link[0]: Point-to-Point, Nbr IGP Id: 3.3.3.3, nbr_node_id:3, gen:3
          frag_id 10, Intf Address:12.1.3.1, Nbr Intf Address:12.1.3.3
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None

IGP Id: 2.2.2.2, MPLS TE Id:2.2.2.2 Router Node (ospf 1 area 0)
      link[0]: Point-to-Point, Nbr IGP Id: 6.6.6.6, nbr_node_id:6, gen:4
          frag_id 10, Intf Address:12.2.6.2, Nbr Intf Address:12.2.6.6
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None

IGP Id: 3.3.3.3, MPLS TE Id:3.3.3.3 Router Node (ospf 1 area 0)
      link[0]: Point-to-Point, Nbr IGP Id: 1.1.1.1, nbr_node_id:1, gen:7
```

```
        frag_id 5, Intf Address:12.1.3.3, Nbr Intf Address:12.1.3.1
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

    link[1]: Point-to-Point, Nbr IGP Id: 5.5.5.5, nbr_node_id:5, gen:7
        frag_id 7, Intf Address:12.3.5.3, Nbr Intf Address:12.3.5.5
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

    link[2]: Point-to-Point, Nbr IGP Id: 4.4.4.4, nbr_node_id:4, gen:7
        frag_id 6, Intf Address:12.3.4.3, Nbr Intf Address:12.3.4.4
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

IGP Id: 4.4.4.4, MPLS TE Id:4.4.4.4 Router Node (ospf 1 area 0)
    link[0]: Point-to-Point, Nbr IGP Id: 20.20.20.20, nbr_node_id:8, gen:10
        frag_id 7, Intf Address:12.4.20.4, Nbr Intf Address:12.4.20.20
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

    link[1]: Point-to-Point, Nbr IGP Id: 5.5.5.5, nbr_node_id:5, gen:10
        frag_id 6, Intf Address:12.4.5.4, Nbr Intf Address:12.4.5.5
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

    link[2]: Point-to-Point, Nbr IGP Id: 3.3.3.3, nbr_node_id:3, gen:10
        frag_id 5, Intf Address:12.3.4.4, Nbr Intf Address:12.3.4.3
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

IGP Id: 5.5.5.5, MPLS TE Id:5.5.5.5 Router Node (ospf 1 area 0)
    link[0]: Point-to-Point, Nbr IGP Id: 4.4.4.4, nbr_node_id:4, gen:12
        frag_id 6, Intf Address:12.4.5.5, Nbr Intf Address:12.4.5.4
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

    link[1]: Point-to-Point, Nbr IGP Id: 3.3.3.3, nbr_node_id:3, gen:12
        frag_id 5, Intf Address:12.3.5.5, Nbr Intf Address:12.3.5.3
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None

IGP Id: 6.6.6.6, MPLS TE Id:6.6.6.6 Router Node (ospf 1 area 0)
    link[0]: Point-to-Point, Nbr IGP Id: 2.2.2.2, nbr_node_id:2, gen:15
        frag_id 5, Intf Address:12.2.6.6, Nbr Intf Address:12.2.6.2
        TE metric:1, IGP metric:1, attribute flags:0x0
        SRLGs: None
```

```
      link[1]: Point-to-Point, Nbr IGP Id: 19.19.19.19, nbr_node_id:7, gen:15
          frag_id 7, Intf Address:12.6.19.6, Nbr Intf Address:12.6.19.19
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None

      link[2]: Point-to-Point, Nbr IGP Id: 5.5.5.5, nbr_node_id:5, gen:15
          frag_id 6, Intf Address:12.5.6.6, Nbr Intf Address:12.5.6.5
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None

IGP Id: 19.19.19.19, MPLS TE Id:19.19.19.19 Router Node (ospf 1 area 0)
      link[0]: Point-to-Point, Nbr IGP Id: 6.6.6.6, nbr_node_id:6, gen:16
          frag_id 22, Intf Address:12.6.19.19, Nbr Intf Address:12.6.19.6
          TE metric:1, IGP metric:1, attribute flags:0x0
          SRLGs: None

IGP Id: 20.20.20.20, MPLS TE Id:20.20.20.20 Router Node (ospf 1 area 0)
      link[0]: Point-to-Point, Nbr IGP Id: 4.4.4.4, nbr_node_id:4, gen:17
      frag_id 19, Intf Address:12.4.20.20, Nbr Intf Address:12.4.20.4
      TE metric:1, IGP metric:1, attribute flags:0x0
      SRLGs: None
```

RP/0/3/CPU0:XR2#show mpls traffic-eng topology summary

```
Fri May 4 17:54:35.577 UTC
My_System_id: 20.20.20.20 (OSPF 1 area 0)
My_BC_Model_Type: RDM

Signalling error holddown: 10 sec Global Link Generation 120

OSPF 1  area 0
  Local System Id:           20.20.20.20
  TE router ID configured:   20.20.20.20
             in use:         20.20.20.20

  IGP Id: 1.1.1.1, MPLS TE Id: 1.1.1.1 Router Node
      1 links

  IGP Id: 2.2.2.2, MPLS TE Id: 2.2.2.2 Router Node
      1 links

  IGP Id: 3.3.3.3, MPLS TE Id: 3.3.3.3 Router Node
      3 links

  IGP Id: 4.4.4.4, MPLS TE Id: 4.4.4.4 Router Node
      3 links
```

```
  IGP Id: 5.5.5.5, MPLS TE Id: 5.5.5.5 Router Node
      2 links

  IGP Id: 6.6.6.6, MPLS TE Id: 6.6.6.6 Router Node
      3 links

  IGP Id: 19.19.19.19, MPLS TE Id: 19.19.19.19 Router Node
      1 links

  IGP Id: 20.20.20.20, MPLS TE Id: 20.20.20.20 Router Node
      1 links

  Total: 8 nodes (8 router, 0 network), 15 links

Grand Total: 8 nodes (8 router, 0 network)  15 links
```

Task 5.2 Solution

```
R1:
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 20.20.20.20
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng bandwidth 45000
 tunnel mpls traffic-eng path-option 1 dynamic

XR2:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 signalled-bandwidth 45000
 destination 1.1.1.1
 path-option 1 dynamic
```

Task 5.2 Verification

```
R1#show mpls traffic-eng tunnels
```

```
P2P TUNNELS/LSPs:

Name: R1_t0                                   (Tunnel0)  Destination: 20.20.20.20
  Status:
    Admin: up              Oper: up         Path: valid     Signalling: connected
    path option 1, type dynamic (Basis for Setup, path weight 3)

  Config Parameters: Bandwidth: 45000
    kbps (Global)   Priority: 7 7    Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: enabled LockDown: disabled Loadshare: 45000 bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled LockDown: disabled  Verbatim: disabled



  InLabel   :   -
  OutLabel : FastEthernet0/0.13, 28
  Next Hop : 12.1.3.3
  RSVP Signalling Info:
       Src 1.1.1.1, Dst 20.20.20.20, Tun_Id 0, Tun_Instance 1
    RSVP Path Info:
      My Address: 12.1.3.1 Explicit Route: 12.1.3.3 12.3.4.4 12.4.20.20 20.20.20.20
      Record    Route:  NONE
      Tspec: ave rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits
    RSVP Resv Info:
      Record    Route:  NONE
      Fspec: ave rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits
  History:
    Tunnel:
      Time since created: 19 seconds
      Time since path change: 19 seconds
      Number of LSP IDs (Tun_Instances) used: 1
    Current LSP: [ID: 1]
      Uptime: 19 seconds

LSP Tunnel XR2_t0 is signalled, connection is up
  InLabel   : FastEthernet0/0.13, implicit-null
  Prev Hop : 12.1.3.3
  OutLabel :    -
  RSVP Signalling Info:
       Src 20.20.20.20, Dst 1.1.1.1, Tun_Id 0, Tun_Instance 2
  RSVP Path Info:
    My Address: 1.1.1.1
    Explicit Route: NONE
```

```
    Record  Route:  NONE
    Tspec: ave rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits
  RSVP Resv Info:
    Record  Route:  NONE
    Fspec: ave rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits



P2MP TUNNELS:


P2MP SUB-LSPS:
```

RP/0/3/CPU0:XR2#show mpls traffic-eng tunnels

```
Fri May 4 17:57:22.445 UTC
Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 3004 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 19 seconds
          Auto-bw enabled tunnels:  0 (disabled)

Name: tunnel-te0   Destination: 1.1.1.1
  Status:
    Admin:    up Oper:    up   Path:  valid   Signalling:  connected

    path option 1,  type dynamic  (Basis for Setup, path weight 3)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 45000 kbps CT0

  Config Parameters: Bandwidth:    45000 kbps
 (CT0) Priority:  7  7  Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute:  enabled LockDown: disabled  Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  History:
    Tunnel has been up for: 00:01:05 (since Fri May 04 17:56:17 UTC 2012)
    Current LSP:
      Uptime: 00:01:05 (since Fri May 04 17:56:17 UTC 2012)

Path info (OSPF 1 area 0): Hop0: 12.4.20.4
Hop1: 12.3.4.3
Hop2: 12.1.3.1
  Hop3: 1.1.1.
```

```
LSP Tunnel 1.1.1.1 0 [1] is signalled, connection is up
  Tunnel Name: R1_t0 Tunnel Role: Tail
  InLabel: GigabitEthernet0/4/0/0.420, implicit-null
  Signalling Info:
    Src 1.1.1.1 Dst 20.20.20.20, Tun ID 0, Tun Inst 1, Ext ID 1.1.1.1
    Router-IDs: upstream   4.4.4.4
                local      20.20.20.20
    Bandwidth: 45000 kbps (CT0) Priority:  7  7 DSTE-class: 0
    Path Info:
      Incoming:
      Explicit Route:
        Strict, 12.4.20.20
        Strict, 20.20.20.20
      Record Route: Disabled
      Tspec: avg rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
    Resv Info: None
      Record Route: Disabled
      Fspec: avg rate=45000 kbits, burst=1000 bytes, peak rate=45000 kbits
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 1 (of 1) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
R1#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing  Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         17         2.2.2.2/32       0             Fa0/0.13  12.1.3.3
17         Pop Label  3.3.3.3/32       0             Fa0/0.13  12.1.3.3
18         18         4.4.4.4/32       0             Fa0/0.13  12.1.3.3
19         19         5.5.5.5/32       0             Fa0/0.13  12.1.3.3
20         20         6.6.6.6/32       0             Fa0/0.13  12.1.3.3
21         21         12.2.6.0/24      0             Fa0/0.13  12.1.3.3
22         Pop Label  12.3.4.0/24      0             Fa0/0.13  12.1.3.3
23         Pop Label  12.3.5.0/24      0             Fa0/0.13  12.1.3.3
24         22         12.4.5.0/24      0             Fa0/0.13  12.1.3.3
25         23         12.4.20.0/24     0             Fa0/0.13  12.1.3.3
26         24         12.5.6.0/24      0             Fa0/0.13  12.1.3.3
27         25         12.6.19.0/24     0             Fa0/0.13  12.1.3.3
28         26         19.19.19.19/32   0             Fa0/0.13  12.1.3.3
29     [T] Pop Label  20.20.20.20/32   0             Tu0       point2point
30         No Label   l2ckt(1)       27464           Se2/0     point2point

[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option


RP/0/3/CPU0:XR2#show mpls forwarding
```

```
Fri May 4 17:58:47.460 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  Pop         1.1.1.1/32       tt0          1.1.1.1         3416

16001  17          2.2.2.2/32         Gi0/4/0/0.420 12.4.20.4       0
16002  18          3.3.3.3/32         Gi0/4/0/0.420 12.4.20.4       0
16003  Pop         4.4.4.4/32         Gi0/4/0/0.420 12.4.20.4       8369
16004  19          5.5.5.5/32         Gi0/4/0/0.420 12.4.20.4       6417
16005  20          6.6.6.6/32         Gi0/4/0/0.420 12.4.20.4       0
16006  26          19.19.19.19/32     Gi0/4/0/0.420 12.4.20.4       1000
16007  21          12.1.3.0/24        Gi0/4/0/0.420 12.4.20.4       0
16008  22          12.2.6.0/24        Gi0/4/0/0.420 12.4.20.4       0
16009  Pop         12.3.4.0/24        Gi0/4/0/0.420 12.4.20.4       0
16010  23          12.3.5.0/24        Gi0/4/0/0.420 12.4.20.4       0
16011  Pop         12.4.5.0/24        Gi0/4/0/0.420 12.4.20.4       0
16012  24          12.5.6.0/24        Gi0/4/0/0.420 12.4.20.4       0
16013  25          12.6.19.0/24       Gi0/4/0/0.420 12.4.20.4       0
16014  Pop         PW(1.1.1.1:1)      Gi0/4/0/1    point2point     27402
16015  Aggregate   ENT: Per-VRF Aggr[V]   \
                                      ENT                           0
16016  Unlabelled  10.9.9.9/32[V]     Gi0/4/0/0.920 10.0.0.9         520
RP/0/3/CPU0:XR2#
```

Task 5.3 Solution

```
R1:
interface Tunnel0
 tunnel mpls traffic-eng fast-reroute

R3:
ip rsvp signalling hello bfd
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 4.4.4.4
 tunnel mpls traffic-eng path-option 1 explicit name PROTECTION
!
interface FastEthernet0/0.34
 mpls traffic-eng backup-path Tunnel1
 ip rsvp signalling hello bfd
```

```
 bfd interval 50 min_rx 50 multiplier 3
!
ip explicit-path name PROTECTION enable
 exclude-address 12.3.4.3
 exclude-address 12.3.4.4

R4:
ip rsvp signalling hello bfd
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 3.3.3.3
 tunnel mpls traffic-eng path-option 1 explicit name PROTECTION
!
interface FastEthernet0/0.34
 mpls traffic-eng backup-path Tunnel1
 ip rsvp signalling hello bfd
 bfd interval 50 min_rx 50 multiplier 3
!
ip explicit-path name PROTECTION enable
 exclude-address 12.3.4.3
 exclude-address 12.3.4.4

XR1:
interface tunnel-te0
 fast-reroute
```

Task 5.3 Verification

```
R1#show mpls traffic-eng tunnels protection

P2P TUNNELS:
R1_t0
  LSP Head, Tunnel0, Admin: up, Oper: up
  Src 1.1.1.1, Dest 20.20.20.20, Instance 2  Fast Reroute Protection: Requested
    Outbound: Unprotected: no backup tunnel assigned
    LSP signalling info:
      Original: out i/f: Fa0/0.13, label: 30, nhop: 12.1.3.3
                nnhop: 4.4.4.4; nnhop rtr id: 4.4.4.4
  Path Protection: None

P2MP TUNNELS:
RP/0/3/CPU0:XR2#show mpls traffic-eng tunnels protection
```

```
Fri May 4 18:04:14.259 UTC
R1_t0 Tunnel Id: 0
  LSP Tail, signaled, connection up
  Src: 1.1.1.1, Dest: 20.20.20.20, Instance: 2
  Fast Reroute Protection: Requested
    Inbound: FRR Inactive
     LSP signalling info:
      Original: in i/f: GigabitEthernet0/4/0/0.420, label:  3, phop: 12.4.20.4

XR2_t0 Tunnel Id: 0
  LSP Head, Admin: up, Oper: up
  Src: 20.20.20.20, Dest: 1.1.1.1, Instance: 2 Fast Reroute Protection: Requested
    Outbound: FRR Inactive
     LSP signalling info:
      Original: out i/f: GigabitEthernet0/4/0/0.420, label: 29, nhop: 12.4.20.4
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

1 12.1.3.3 [MPLS: Label 30 Exp 0] 4 msec 0 msec 4 msec
2 12.3.4.4 [MPLS: Label 30 Exp 0] 0 msec 0 msec 4 msec
3 12.4.20.20 4 msec *  4 msec

R4#config t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#int f0/0.34
R4(config-subif)#shut
R1#traceroute 20.20.20.20

Type escape sequence to abort.
Tracing the route to 20.20.20.20

1 12.1.3.3 [MPLS: Label 30 Exp 0] 4 msec 0 msec 4 msec
2 12.3.5.5 [MPLS: Labels 28/30 Exp 0] 0 msec 4 msec 0 msec
3 12.4.5.4 [MPLS: Label 30 Exp 0] 0 msec 0 msec 0 msec
4 12.4.20.20 4 msec *  0 msec
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
Fri May 4 18:05:58.501 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

1 12.4.20.4 [MPLS: Label 33 Exp 0]  5 msec  4 msec  2 msec
2 12.3.4.3 [MPLS: Label 32 Exp 0]  4 msec  3 msec  2 msec
2 12.1.3.1 2 msec *  2 msec
```

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0.34
R3(config-subif)#shut
RP/0/3/CPU0:XR2#traceroute 1.1.1.1
Fri May 4 18:06:33.976 UTC

Type escape sequence to abort.
Tracing the route to 1.1.1.1

1 12.4.20.4 [MPLS: Label 33 Exp 0] 6 msec  3 msec  2 msec
2 12.4.5.5 [MPLS: Labels 29/32 Exp 0] 3 msec 3 msec  2 msec

3 12.3.5.3 [MPLS: Label 32 Exp 0] 3 msec  20 msec  8 msec
4 12.1.3.1 2 msec  *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 1 v4

Full-Scale Lab 1 Solutions 6.1 - 6.3 (pending update)

Task 6.1
Task 6.2
Task 6.3

Task 6.1 Solution

```
R2:
ip multicast-routing
ip multicast-routing vrf Acme
ip pim ssm default
!
vrf definition Acme address-
 family ipv4
 mdt default 232.100.100.100
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet0/0.26
 ip pim sparse-mode
!
interface FastEthernet1/0
 ip pim sparse-mode
!
router bgp 1284
 address-family ipv4 mdt
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
 exit-address-family

R5:
router bgp 1284
 address-family ipv4 mdt
```

```
  neighbor 19.19.19.19 activate
  neighbor 19.19.19.19 send-community extended
  neighbor 19.19.19.19 route-reflector-client
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
 exit-address-family

R6:
ip multicast-routing
 ip pim ssm default
!
interface FastEthernet0/0.26
 ip pim sparse-mode
!
interface FastEthernet0/0.619
 ip pim sparse-mode

XR1:
router bgp 1284
 address-family ipv4 mdt
 !
 neighbor 5.5.5.5
  address-family ipv4 mdt
!
multicast-routing
 address-family ipv4
  mdt source Loopback0
  interface all enable
!
vrf Acme
 address-family ipv4
  mdt default ipv4 232.100.100.100
  interface all enable
```

Task 6.1 Verification

```
R2#show ip pim vrf Acme neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
19.19.19.19       Tunnel0                  00:00:10/00:01:40 v2    1 / DR G
```

```
192.168.210.10    FastEthernet1/0          00:00:42/00:01:31 v2    1 / DR S P G
RP/0/0/CPU0:XR1#show pim vrf Acme neighbor
Fri May 4 18:11:20.087 UTC

PIM neighbors in VRF Acme

Neighbor Address             Interface              Uptime    Expires   DR pri
Flags

192.168.19.19*               Loopback192            00:03:19  00:01:36  1  (DR) B P
2.2.2.2                      mdtAcme                00:01:18  00:01:24  1        P
19.19.19.19*                 mdtAcme                00:03:19  00:01:32  1  (DR) B
192.168.199.9                GigabitEthernet0/1/0/0 00:02:46  00:01:27  1        P
192.168.199.19*              GigabitEthernet0/1/0/0 00:03:19  00:01:35  1  (DR) B P
SW2#ping vrf MULTICAST 224.1.2.3

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.1.2.3, timeout is 2 seconds:
.

RP/0/0/CPU0:XR1#show pim vrf Acme topology
Fri May 4 18:12:29.240 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.40) DM Up: 00:04:28 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
  GigabitEthernet0/1/0/0      00:04:28  off LI II LH
(192.168.7.100,224.1.2.3)SPT SM Up: 00:00:27
JP: Join(00:00:22) RPF: GigabitEthernet0/1/0/0,192.168.199.9 Flags:
  mdtAcme                     00:00:27  fwd Join(00:03:02)
R2#show ip mroute vrf Acme
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
```

```
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.2.3), 00:00:42/stopped, RP 192.168.0.10, flags: SP
  Incoming interface: FastEthernet1/0, RPF nbr 192.168.210.10
  Outgoing interface list: Null
(192.168.7.100, 224.1.2.3), 00:00:42/00:02:47, flags: T

  Incoming interface: Tunnel0, RPF nbr 19.19.19.19
  Outgoing interface list:
    FastEthernet1/0, Forward/Sparse, 00:00:42/00:02:47

(*, 224.0.1.40), 00:05:36/00:02:26, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:05:34/00:00:08
```

Task 6.2 Solution

```
R7:
router bgp 65000
 no bgp default ipv4-unicast
 neighbor 192.168.78.8 remote-as 65000
!
address-family ipv4 multicast
 neighbor 192.168.78.8 activate
 network 192.168.7.0
exit-address-family

R8:
router bgp 65000
 no bgp default ipv4-unicast
 neighbor 192.168.78.7 remote-as 65000
 !
 address-family ipv4 multicast
  neighbor 192.168.78.7 activate
```

```
 distance bgp 20 109 200 exit-address-
family
```

Task 6.2 Verification

```
R7#show ip bgp ipv4 multicast summary
BGP router identifier 7.7.7.7, local AS number 65000
BGP table version is 2, main routing table version 2
1 network entries using 101 bytes of memory
1 path entries using 44 bytes of memory
1 BGP path attribute entries using 60 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 205 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.78.8    4 65000       4       5        2    0    0 00:00:34        0
R8#show ip bgp ipv4 multicast summary
BGP router identifier 8.8.8.8, local AS number 65000
BGP table version is 2, main routing table version 2
1 network entries using 101 bytes of memory
1 path entries using 44 bytes of memory
1 BGP path attribute entries using 60 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 205 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.78.7    4 65000       6       5        2    0    0 00:01:03        1
R8#show ip bgp ipv4 multicast
BGP table version is 2, local router ID is 8.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.7.0      192.168.78.7             0    100      0 i
R8#show ip rpf 192.168.7.0
RPF information for ? (192.168.7.0)
  RPF interface: FastEthernet0/0
  RPF neighbor: ? (192.168.78.7)
  RPF route/mask: 192.168.7.0/24
```

```
RPF type: mbgp

  RPF recursion count: 0
  Doing distance-preferred lookups across tables
SW2#ping vrf MULTICAST 224.4.5.6

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.4.5.6, timeout is 2 seconds:
.
R8#show ip mroute 224.4.5.6
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T    - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U    - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.4.5.6), 01:25:18/00:02:44, RP 192.168.0.10, flags: SJCL
  Incoming interface: FastEthernet0/1, RPF nbr 192.168.108.10
  Outgoing interface list:
    Loopback0, Forward/Sparse, 01:25:18/00:02:09
(192.168.7.100, 224.4.5.6), 00:00:15/00:02:44, flags: LJ
  Incoming interface: FastEthernet0/0, RPF nbr 192.168.78.7, Mbgp

  Outgoing interface list:
    Loopback0, Forward/Sparse, 00:00:16/00:02:43
```

Task 6.3 Solution

```
R1:
policy-map IN_FROM_CE
  class class-default
    police cir 45000000
     conform-action set-mpls-exp-imposition-transmit 3
     exceed-action drop
!
class-map match-all MPLS_EXP_3
 match mpls experimental topmost 3
```

```
!
policy-map OUT_TO_P
  class MPLS_EXP_3
    bandwidth 45000
!
interface Serial2/0
 service-policy input IN_FROM_CE
!
interface FastEthernet0/0
 service-policy output OUT_TO_P

R3:
class-map match-all MPLS_EXP_3
  match mpls experimental topmost 3
!
policy-map OUT_TO_P
  class MPLS_EXP_3
    bandwidth 45000
!
interface FastEthernet0/0
 service-policy output OUT_TO_P

R4:
class-map match-all MPLS_EXP_3
  match mpls experimental topmost 3
!
policy-map OUT_TO_P
  class MPLS_EXP_3
    bandwidth 45000
!
interface FastEthernet0/0
 service-policy output OUT_TO_P

R5:
class-map match-all MPLS_EXP_3
 match mpls experimental topmost 3
!
policy-map OUT_TO_P
  class MPLS_EXP_3
    bandwidth 45000
!
interface FastEthernet0/0 service-
 policy output OUT_TO_P

XR2:
policy-map IN_FROM_CE
```

```
 class class-default
  police rate 45 mbps
   conform-action set mpls experimental imposition 3
   exceed-action drop
  !
 !
 end-policy-map
!
class-map match-any MPLS_EXP_3
 match mpls experimental topmost 3
 end-class-map
!
policy-map OUT_TO_P
 class MPLS_EXP_3
  bandwidth 45 mbps
 !
 class class-default
 !
 end-policy-map
!
interface GigabitEthernet0/4/0/1
 l2transport
  service-policy input IN_FROM_CE
!
interface GigabitEthernet0/4/0/0.420
 service-policy output OUT_TO_P
```

Task 6.3 Verification

```
R3#debug mpls packet
Packet debugging is on
R7#ping 192.168.78.8 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.78.8, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 32/32/32 ms

R3# MPLS turbo: Fa0/0.13: rx: Len 110 Stack {31 3 255} {16014 3 255}
 CW {0 0 0} MPLS turbo: Fa0/0.35: tx: Len 110 Stack {31 3 254} {16014 3 255}
 CW {0 0 0} MPLS turbo: Fa0/0.35: rx: Len 86 Stack {33 3 253} {30 3 254}
 CW {0 60 0} MPLS turbo: Fa0/0.13: tx: Len 82 Stack {30 3 252}
 CW {0 60 0}
R1#show policy-map interface
```

```
 FastEthernet0/0

  Service-policy output: OUT_TO_P Class-

    map: MPLS_EXP_3 (match-all)
      33 packets, 3243 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 3 Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 33/3243
      bandwidth 45000 kbps

    Class-map: class-default (match-any)
      116 packets, 12649 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 118/12895
Serial2/0

 Service-policy input: IN_FROM_CE

   Class-map: class-default (match-any)
     35 packets, 3093 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      police:
        cir 45000000 bps, bc 1406250 bytes
      conformed 35 packets, 3093 bytes; actions:
        set-mpls-exp-imposition-transmit 3
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps
RP/0/3/CPU0:XR2#show policy-map interface gig0/4/0/1
Fri May 4 18:19:55.497 UTC

GigabitEthernet0/4/0/1 input: IN_FROM_CE

Class class-default
  Classification statistics          (packets/bytes)        (rate - kbps)
    Matched             :                  36/3011                    0
    Transmitted         :                  36/3011                    0
    Total Dropped       :                   0/0                       0
```

```
  Policing statistics                (packets/bytes)       (rate - kbps)
    Policed(conform)     :                 36/3011                   0
    Policed(exceed)      :                  0/0                      0
    Policed(violate)     :                  0/0                      0
    Policed and dropped  :                  0/0
```

RP/0/3/CPU0:XR2#show policy-map interface gig0/4/0/0.420

```
Fri May 4 18:23:00.314 UTC
GigabitEthernet0/4/0/0.420 direction input: Service Policy not installed

GigabitEthernet0/4/0/0.420 output: OUT_TO_P

Class MPLS_EXP_3
  Classification statistics           (packets/bytes)     (rate - kbps)
    Matched             :                   70/5678                0
    Transmitted         :                   70/5678                0
    Total Dropped       :                    0/0                   0
  Queueing statistics
    Queue ID                              : 8
    High watermark  (Unknown)             : 0
    Inst-queue-len  (packets)             : 0
    Avg-queue-len   (packets)             : 0
    Taildropped(packets/bytes)            : 0/0
Class class-default
  Classification statistics           (packets/bytes)     (rate - kbps)
    Matched             :                    0/0                   0
    Transmitted         :                    0/0                   0
    Total Dropped       :                    0/0                   0
  Queueing statistics
    Queue ID                              : 9
    High watermark  (Unknown)             : 0
    Inst-queue-len  (packets)             : 0
    Avg-queue-len   (packets)             : 0
    Taildropped(packets/bytes)            : 0/0
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Tasks (pending update)

Difficulty Rating (10 highest): 7

Lab Overview

The following scenario is a practice lab exam designed to test your skills at configuring Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco's CCIE Service Provider Version 3.0 Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab to complete all the configuration steps, take the time to research each networking technology and gain a deeper understanding of the principles behind its operation.

Lab Instructions

Before starting, ensure that the initial configuration scripts for this lab have been applied. If you have any questions related to the scenario solutions, visit our Online Community.

Refer to the attached diagrams for interface and protocol assignments. Upon completion, all devices in the Service Provider core should have full IP reachability to all networks in the core, and all customer devices should have full IP reachability to other sites belonging to the same customer, unless otherwise explicitly specified.

Lab Do's and Don'ts

- Do not change or add any IP addresses from the initial configuration unless otherwise specified or required for troubleshooting.
- If additional IP addresses are needed but not specifically permitted by the task, use IP unnumbered.
- Do not change any interface encapsulations unless otherwise specified.
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified.
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified.
- Save your configurations often.

Grading

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to pass the exam. A section must work 100% with the requirements given to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Point Values

This lab is broken into 6 main technology sections, with point values for each section distributed as follows:

Section	Point Value
Bridging & Switching	16
IGP	12
MPLS	18

Section	Point Value
VPN	33
MPLS TE	14
Services	7

GOOD LUCK!

---

1. Bridging & Switching

1.1 Trunking

- Configure trunking on SW2 to the routers in the core of the SP network per the diagram.
- Configure trunking between SW1 and SW2 on their interconnected ports.
- Limit all trunk links to only forward traffic for VLANs that are required per the diagram; additionally allow VLANs 9 and 10 to be trunked between SW1 and SW2.

Score: 5 Points

1.2 VLANs

- Create and assign only the necessary VLANs per the diagram on SW1 and SW2.
- Hardcode all links to the routers as full duplex.
- Do not use the `port-type` command on SW1 on any links connected to the routers.

Score: 6 Points

1.3 STP

- Configure SW1 and SW2 to run the Rapid-PVST algorithm on the trunk links connecting them.
- SW1 should be the root bridge for VLANs that span between the two switches.

- Use the higher numbered trunk port between the switches as the primary link for traffic forwarding; the lowered numbered trunk port should only be used for forwarding if the higher numbered trunk link is down.
- All STP enabled links connecting to the routers should be edge ports.

Score: 5 Points

---

2. IGP

2.1 IS-IS

- Configure IS-IS Level 2 on all links in the Service Provider core.
- Use NET addresses in the format 49.0001.0000.0000.00YY.00, where YY is the IPv4 host address assigned to the router's connected links.
- Advertise the Loopbacks of these routers into IS-IS, but do not send hello packets out these interfaces.
- Do not generate a Pseudonode LSP for any transit links in the SP core.
- Use the minimum number of commands necessary to accomplish this task.

Score: 6 Points

2.2 IS-IS Security

- Authenticate all Level 2 adjacencies with an MD5 hash of the password CCIE.

Score: 6 Points

---

3. MPLS

3.1 LDP

- Configure LDP on all interfaces in the Service Provider core.
- Use the minimum number of commands to accomplish this.

Score: 6 Points

3.2 Label Allocation

- Configure the network so that labels are only allocated for the Loopback interfaces of R1, R2, R5, and XR1.

Score: 6 Points

3.3 LDP Session Protection

- Configure R3, R4, R5, and R6 so that if a connected link in the core goes down the labels allocated by that connected neighbor are maintained in the LIB for five minutes.
- If the link is not restored within five minutes these stale labels should be flushed from the LIB.

Score: 6 Points

---

4. VPN

4.1 VPNv4 BGP

- Configure a full mesh of VPNv4 iBGP peerings between the PE routers in AS 26.
- Do not activate any other AFI/SAFIs.
- Use the minimum number of `remote-as` statements necessary to accomplish this task.

Score: 6 Points

4.2 MPLS L3VPN

- VRF “ABC” will be used to provide a full mesh of connectivity between the ABC sites 1, 2, and 3 per the diagram.
- Configure this VRF using the RD and RT 26:65001 on the PE routers, and use IPv4 addressing per the diagram with host addresses equal to their IPv4 host addresses on their other links.

- Use IPv4 Unicast BGP as the PE to CE routing protocol with the Autonomous System information provided in the diagram.
- Advertise the LAN interfaces of the CE routers and the PE to CE links into IPv4 Unicast BGP on the CE routers.
- Once complete R7, R8, and XR2 should have a full mesh of IPv4 connectivity to each other.

Score: 7 Points

4.3 6PE

- VRF “ABC” will also be used for IPv6 transport over the provider’s IPv4 only core using the same RD and RT policy.
- Configure IPv6 addressing on the PE to CE links of R1, R2, and XR1 per the diagram, with host addresses equal to their IPv4 host addresses on their other links.
- Use BGP to advertise the IPv6 Unicast NLRI between the PE and CE routers, but do not initiate an additional TCP control plane session between XR1 and XR2 to accomplish this.
- Advertise the LAN interfaces of the CE routers and the PE to CE links into IPv6 Unicast BGP on the CE routers.
- Once complete, R7, R8, and XR2 should have a full mesh of IPv6 connectivity to each other.

Score: 7 Points

4.4 L3VPN

- Configure VRF “XYZ” on XR1 for the connection to AS 10 per the diagram.
- Use the RD and RT 26:10 on the XR1, and use IPv4 addressing per the diagram.
- Using the BGP AS information in the diagram, use BGP as the PE to CE routing protocol between these ASes.
- Advertise the LAN interface and PE to CE link into BGP on SW2.
- Once complete XR1 should have IPv4 reachability to the LAN interface of SW2 inside this VRF.

Score: 6 Points

4.5 IPv4 Internet Access

- The MPLS L3VPN service provider connects to the Internet via its upstream peer AS 2000. Configure R5 in such a way that all MPLS L3VPN customer sites are able to reach SW1 in AS 2000.
- Any RFC 1918 address space used by the ABC L3VPN customers should be translated to the public address block 26.255.1.0/24 as their traffic routes out to the Internet.
- Any RFC 1918 address space used by the XYZ L3VPN customers should be translated to the public address block 26.255.2.0/24 as their traffic routes out to the Internet.
- Once complete, R5 and the ABC & XYZ sites should have reachability to the VLAN 9 link in AS 2000, but ABC and XYZ sites should not have reachability to each other; do not apply any data plane filters to accomplish this.
- Ensure to account for any arbitrary IPv4 prefixes on the Internet that the L3VPN customers are trying to reach.
- R5's link to SW1 should remain in the global routing table.
- Do not make changes on any device besides R5 to accomplish this.
- Static routing is allowed to accomplish this task.

Score: 7 Points

---

5. MPLS TE

5.1 MPLS TE

- Configure an MPLS TE tunnel from XR1 to R2 that is used to route traffic from ABC Site 1 to ABC Site 3.
- Traffic sent over the tunnel should be routed from XR1 to R3 to R6 to R5 to R4 and then to R2.
- Do not use an explicit path to accomplish this.
- Do not modify the IGP metrics of any links in the core to accomplish this.

Score: 7 Points

6. Services

6.1 Multicast L3VPN

- Configure the Service Provider core to support multicast forwarding between the ABC L3VPN sites.
- R1, R2, and XR1 should use the group address 232.1.2.19 to tunnel multicast traffic over the SP core.
- Additional data MDTs should be created on R1, R2, and XR1 using the addresses 232.1.255.0/24, 232.2.255.0/24, and 232.19.255.0/24 respectively.

Score: 7 Points

6.2 Anycast RP

- Configure multicast routing on all of the interfaces of the CE routers in the ABC sites.
- Create and advertise a new Loopback address 10.0.0.1/32 into BGP on R8 and XR2 for use as the Anycast RP address.
- Configure static RP assignments and MSDP as necessary to accommodate the Anycast RP in the ABC sites.
- Once complete you should be able to perform the following verification and receive the highlighted output below:

```
SW1#ping vrf VLAN20 224.20.20.20 repeat 10



Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 224.20.20.20, timeout is 2 seconds:
..........
SW2#ping vrf VLAN7 224.7.7.7 repeat 10



Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 224.7.7.7, timeout is 2 seconds:
..........
R8#show ip msdp sa-cache

MSDP Source-Active Cache - 2 entries (10.7.7.100, 224.7.7.7), RP 10.0.0.1
, BGP/AS 65001, 00:00:15/00:05:44, Peer
10.20.20.20 (10.20.20.100, 224.20.20.20), RP 10.0.0.1
, BGP/AS 65001, 00:06:10/00:03:41, Peer 10.20.20.20
```

Score: 7 Points

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solutions 1.1 - 1.3 (pending update)

Task 1.1 Solution

```
SW1:
interface FastEthernet0/20
 switchport mode trunk
 switchport trunk allowed vlan 9,59,1910
 no shutdown
!
interface FastEthernet0/21
 switchport mode trunk
 switchport trunk allowed vlan 9,59,1910
 no shutdown

SW2:
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 16
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 24
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 34,35,36,319
!
```

```
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 24,34,45
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 35,45,56,59
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 16,36,56
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,59,1910
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,59,1910
```

Task 1.1 Verification

```
SW1#show interface trunk



Port        Mode            Encapsulation  Status        Native vlan Fa0/20        on
              802.1q         trunking      1  Fa0/21        on
              802.1q         trunking      1

Port        Vlans allowed on trunk          Fa0/20        9,59,1910
Fa0/21        9,59,1910
SW2#show interface trunk

Port        Mode            Encapsulation  Status        Native vlan  Fa0/1          on
              802.1q         trunking      1 Fa0/2           on
              802.1q         trunking      1 Fa0/3           on
              802.1q         trunking      1 Fa0/4           on
              802.1q         trunking      1 Fa0/5           on
              802.1q         trunking      1 Fa0/6           on
              802.1q         trunking      1 Fa0/20          on
              802.1q         trunking      1 Fa0/21          on
```

```
Port        Vlans allowed on trunk Fa0/1
       16 Fa0/2
       24 Fa0/3        34-36,319
Fa0/4       24,34,45
Fa0/5       35,45,56,59
Fa0/6       16,36,56
Fa0/20      10,59,1910
Fa0/21      10,59,1910
```

Task 1.2 Solution

```
SW1:
vlan 9,17,20,28,59,1910
!
vlan 17
 uni-vlan community
!
vlan 28
 uni-vlan community
!
interface FastEthernet0/1
 switchport access vlan 17
 duplex full
 no shutdown
!
interface FastEthernet0/2
 switchport access vlan 28
 duplex full
 no shutdown
!
interface FastEthernet0/7
 switchport access vlan 17
 duplex full
 no shutdown
!
interface FastEthernet0/8
 switchport access vlan 28
 duplex full
 no shutdown
!
interface GigabitEthernet0/1
```

```
 speed nonegotiate switchport
 access vlan 1910
 no shutdown
!
interface GigabitEthernet0/2
 speed nonegotiate switchport
 access vlan 20
 no shutdown



SW2:
vtp mode transparent
!
vlan 8,7,10,16,24,34,35,36,45,56,59,319,1910
!
interface range fastEthernet 0/1 - 6
 duplex full
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 7
 duplex full
!
interface FastEthernet0/8
 switchport mode access
 switchport access vlan 8
 duplex full
!
interface GigabitEthernet0/1
 speed nonegotiate
 switchport mode access
 switchport access vlan 319
```

Task 1.2 Verification

```
SW1#show vlan uni-vlan

VLAN Type              Ports
---- ----------------- -------------------------------------------------------17   UNI community
     Fa0/1, Fa0/728   UNI community
     Fa0/2, Fa0/8
SW1#show interface status | include connected
Fa0/1                            connected 17
       full  a-100 10/100BaseTX
```

```
Fa0/2                       connected 28
       full  a-100 10/100BaseTX Fa0/7                       connected 17
       full  a-100 10/100BaseTX Fa0/8                       connected 28
       full  a-100 10/100BaseTX
Fa0/20                      connected    trunk   a-full  a-100 10/100BaseTX
Fa0/21                      connected    trunk   a-full  a-100 10/100BaseTX
Gi0/1                       connected 1910
     full   1000 1000BaseSX SFP Gi0/2                       connected 20
      full   1000 1000BaseSX SFP
```

Task 1.3 Solution

```
SW1:
spanning-tree vlan 59,1910 priority 4096
!
interface FastEthernet0/20
 port-type nni
!
interface FastEthernet0/21
 port-type nni
!
interface GigabitEthernet0/1
 spanning-tree portfast
!
interface GigabitEthernet0/2
 spanning-tree portfast



SW2:
spanning-tree mode rapid-pvst
!
interface FastEthernet0/1
 spanning-tree portfast trunk
!
interface FastEthernet0/2
 spanning-tree portfast trunk
!
interface FastEthernet0/3
 spanning-tree portfast trunk
!
interface FastEthernet0/4
 spanning-tree portfast trunk
!
```

```
interface FastEthernet0/5
 spanning-tree portfast trunk
!
interface FastEthernet0/6
 spanning-tree portfast trunk
!
interface FastEthernet0/7
 spanning-tree portfast
!
interface FastEthernet0/8
 spanning-tree portfast
!
interface FastEthernet0/20
 spanning-tree cost 100
```

Task 1.3 Verification

```
SW1#show spanning-tree root
  Root
  Hello Max Fwd Vlan                    Root ID   Cost
  Time  Age Dly   Root Port
---------------- -------------------- --------- ----- --- ---   ------------
VLAN0009         32777 0023.ac2a.3c80          0
   2   20   15 VLAN0020          32788 0023.ac2a.3c80          0
   2   20   15 VLAN0059           4155 0023.ac2a.3c80          0
   2   20   15 VLAN1910           6006 0023.ac2a.3c80          0
   2   20   15

SW1#show spanning-tree | include VLAN|Gi0/[1-2]
VLAN0009
VLAN0020 Gi0/2              Desg FWD 4         128.2 P2p Edge

VLAN0059
VLAN1910 Gi0/1              Desg FWD 4         128.1 P2p Edge

SW2#show spanning-tree | include VLAN|Fa0/[1-6]_
VLAN0007
VLAN0008
VLAN0010
VLAN0016 Fa0/1              Desg FWD 19        128.1 P2p Edge
Fa0/6              Desg FWD 19        128.6 P2p Edge
VLAN0024                    Fa0/2              Desg FWD 19        128.2 P2p Edge
Fa0/4              Desg FWD 19        128.4 P2p Edge
```

```
VLAN0034                         Fa0/3              Desg FWD 19         128.3 P2p Edge
Fa0/4               Desg FWD 19         128.4 P2p Edge
VLAN0035                         Fa0/3              Desg FWD 19         128.3 P2p Edge
Fa0/5               Desg FWD 19         128.5 P2p Edge
VLAN0036                         Fa0/3              Desg FWD 19         128.3 P2p Edge
Fa0/6               Desg FWD 19         128.6 P2p Edge
VLAN0045                         Fa0/4              Desg FWD 19         128.4 P2P Edge
Fa0/5               Desg FWD 19         128.5 P2p Edge
VLAN0056                         Fa0/5              Desg FWD 19         128.5 P2p Edge
Fa0/6               Desg FWD 19         128.6 P2p Edge
VLAN0059                         Fa0/5              Desg FWD 19         128.5 P2p Edge
VLAN0319      Fa0/3              Desg FWD 19         128.3 P2p Edge

VLAN1910
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solutions 2.1 - 2.2 (pending update)

Task 2.1 Solution

```
R1:
router isis 1
 net 49.0001.0000.0000.0001.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.16
 ip router isis 1
 isis network point-to-point

R2:
router isis 1
 net 49.0001.0000.0000.0002.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.24
 ip router isis 1
 isis network point-to-point

R3:
router isis 1
 net 49.0001.0000.0000.0003.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.34
 ip router isis 1
```

```
isis network point-to-point
 !
interface FastEthernet1/0.35
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.36
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.319
 ip router isis 1
 isis network point-to-point

R4:
router isis 1
 net 49.0001.0000.0000.0004.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.24
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.34
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.45
 ip router isis 1
 isis network point-to-point

R5:
router isis 1
 net 49.0001.0000.0000.0005.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.35
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.45
 ip router isis 1
 isis network point-to-point
!
```

```
interface FastEthernet1/0.56
 ip router isis 1
 isis network point-to-point

R6:
router isis 1
 net 49.0001.0000.0000.0006.00
 is-type level-2
 passive-interface Loopback0
!
interface FastEthernet1/0.16
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.36
 ip router isis 1
 isis network point-to-point
!
interface FastEthernet1/0.56
 ip router isis 1
 isis network point-to-point

XR1:
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0019.00
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/1/0/1
  point-to-point
  address-family ipv4 unicast
  !
 !
!
```

Task 2.1 Verification

```
R3#show isis neighbors

System Id           Type Interface     IP Address       State Holdtime Circuit Id
R4                  L2   Fa1/0.34      26.3.4.4         UP    27       02
```

```
R5                  L2    Fa1/0.35      26.3.5.5         UP     21        01
R6                  L2    Fa1/0.36      26.3.6.6         UP     29        02
XR1                 L2    Fa1/0.319     26.3.19.19       UP     21        00
RP/0/0/CPU0:XR1#show route ipv4 isis
Wed Jun 27 15:02:00.780 UTC
i L2 1.1.1.1/32
 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1 i L2 2.2.2.2/32
 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1 i L2 3.3.3.3/32
 [115/10] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1 i L2 4.4.4.4/32
 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1 i L2 5.5.5.5/32
 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1 i L2 6.6.6.6/32
 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.1.6.0/24 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.2.4.0/24 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.3.4.0/24 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.3.5.0/24 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.3.6.0/24 [115/20] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.4.5.0/24 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1
i L2 26.5.6.0/24 [115/30] via 26.3.19.3, 00:01:07, GigabitEthernet0/1/0/1

RP/0/0/CPU0:XR1#show isis database
Wed Jun 27 15:02:24.244 UTC

IS-IS 1  (Level-2) Link State Database
LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
R1.00-00               0x00000003   0xd57b        1083            0/0/0
R2.00-00               0x00000003   0x56f3        1060            0/0/0
R3.00-00               0x00000006   0xee29        1108            0/0/0
R4.00-00               0x00000004   0x8806        1071            0/0/0
R5.00-00               0x00000004   0x7506        1084            0/0/0
R6.00-00               0x00000004   0xd89d        1083            0/0/0
XR1.00-00            * 0x00000003   0xc47e        1110            0/0/0
 Total Level-2 LSP count: 7
   Local Level-2 LSP count: 1
```

Task 2.2 Solution

```
R1:
key chain ISIS
 key 1
  key-string CCIE
!
interface FastEthernet1/0.16
 isis authentication mode md5 level-2
```

```
 isis authentication key-chain ISIS

R2:
key chain ISIS
 key 1
 key-string CCIE
!
interface FastEthernet1/0.24
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

R3:
key chain ISIS
 key 1
  key-string CCIE
!
interface FastEthernet1/0.34
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.35
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.36
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.319
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

R4:
key chain ISIS
 key 1
  key-string CCIE
!
interface FastEthernet1/0.24
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.34
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.45
```

```
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

R5:
key chain ISIS
 key 1
  key-string CCIE
!
interface FastEthernet1/0.35
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.45
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.56
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

R6:
key chain ISIS
 key 1
  key-string CCIE
!
interface FastEthernet1/0.16
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.36
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS
!
interface FastEthernet1/0.56
 isis authentication mode md5 level-2
 isis authentication key-chain ISIS

XR1:
router isis 1
 interface GigabitEthernet0/1/0/1
  hello-password hmac-md5 CCIE
  !
 !
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solutions 3.1 - 3.3 (pending update)

Task 3.1 Solution

```
R1:
router isis 1
 mpls ldp autoconfig

R2:
router isis 1
 mpls ldp autoconfig

R3:
router isis 1
 mpls ldp autoconfig

R4:
router isis 1
 mpls ldp autoconfig

R5:
router isis 1
 mpls ldp autoconfig

R6:
router isis 1
 mpls ldp autoconfig

XR1:
router isis 1
 address-family ipv4 unicast
```

```
  mpls ldp auto-config
 !
!
mpls ldp
```

Task 3.1 Verification

```
R3#show mpls ldp neighbor | include Peer|State
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 3.3.3.3:0  State: Oper
; Msgs sent/rcvd: 19/19; Downstream
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 3.3.3.3:0  State: Oper
; Msgs sent/rcvd: 19/20; Downstream
    Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 3.3.3.3:0  State: Oper
; Msgs sent/rcvd: 19/19; Downstream
    Peer LDP Ident: 19.19.19.19:0; Local LDP Ident 3.3.3.3:0  State: Oper
; Msgs sent/rcvd: 18/18; Downstream
RP/0/0/CPU0:XR1#show mpls forwarding

Wed Jun 27 15:11:23.835 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  Pop         3.3.3.3/32         Gi0/1/0/1    26.3.19.3       106
16001  18          4.4.4.4/32         Gi0/1/0/1    26.3.19.3       0
16002  19          5.5.5.5/32         Gi0/1/0/1    26.3.19.3       0
16003  17          2.2.2.2/32         Gi0/1/0/1    26.3.19.3       0
16004  Pop         26.3.4.0/24        Gi0/1/0/1    26.3.19.3       0
16005  24          26.4.5.0/24        Gi0/1/0/1    26.3.19.3       0
16006  Pop         26.3.5.0/24        Gi0/1/0/1    26.3.19.3       0
16007  23          26.2.4.0/24        Gi0/1/0/1    26.3.19.3       0
16008  Pop         26.3.6.0/24        Gi0/1/0/1    26.3.19.3       0
16009  20          6.6.6.6/32         Gi0/1/0/1    26.3.19.3       0
16010  25          26.5.6.0/24        Gi0/1/0/1    26.3.19.3       0
16011  22          26.1.6.0/24        Gi0/1/0/1    26.3.19.3       0
16012  16          1.1.1.1/32         Gi0/1/0/1    26.3.19.3       0
```

Task 3.2

```
R1 - R6:
ip prefix-list PE_ROUTERS seq 5 permit 1.1.1.1/32
ip prefix-list PE_ROUTERS seq 10 permit 2.2.2.2/32
```

```
ip prefix-list PE_ROUTERS seq 15 permit 5.5.5.5/32
ip prefix-list PE_ROUTERS seq 20 permit 19.19.19.19/32
!
mpls ldp label
 allocate global prefix-list PE_ROUTERS

XR1:
ipv4 access-list PE_ROUTERS
 10 permit ipv4 host 1.1.1.1 any
 20 permit ipv4 host 2.2.2.2 any
 30 permit ipv4 host 5.5.5.5 any
 40 permit ipv4 host 19.19.19.19 any
!
mpls ldp
 label
  allocate for PE_ROUTERS
```

Task 3.2 Verification

```
R3#show mpls forwarding-table
Local      Outgoing    Prefix           Bytes Label    Outgoing    Next Hop
Label      Label       or Tunnel Id     Switched       interface   16          161.1.1.1/32
    0              Fa1/0.36    26.3.6.617          172.2.2.2/32
    0              Fa1/0.34    26.3.4.419          Pop Label5.5.5.5/32
    0              Fa1/0.35    26.3.5.521          Pop Label19.19.19.19/32
 0              Fa1/0.319   26.3.19.19
RP/0/0/CPU0:XR1#show mpls forwarding
Wed Jun 27 15:13:19.874 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------ 16002   195.5.5.5/32
        Gi0/1/0/1    26.3.19.3       016003   172.2.2.2/32
        Gi0/1/0/1    26.3.19.3       016012   161.1.1.1/32
        Gi0/1/0/1    26.3.19.3       0
```

Task 3.3

```
R3 - R6:
mpls ldp session protection for P_ROUTERS duration 300
!
ip access-list standard P_ROUTERS
```

```
 permit 3.3.3.3
 permit 4.4.4.4
 permit 5.5.5.5
 permit 6.6.6.6
```

Task 3.3 Verification

```
R3#show mpls ldp neighbor 6.6.6.6 detail | s Protection
        LDP Session Protection enabled, state: Ready

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.R3(config)#int fa1/0.36
R3(config-subif)#shut
R3(config-subif)#
%LDP-5-SP: 6.6.6.6:0: session hold up initiated R3(config-subif)#
do show mpls ldp neighbor 6.6.6.6 detail | s Protection
        LDP Session Protection enabled, state: Protecting
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solutions 4.1 - 4.5 (pending update)

Task 4.1 Solution

```
R1:
router bgp 26
 no bgp default ipv4-unicast
 neighbor PE_ROUTERS peer-group
 neighbor PE_ROUTERS remote-as 26
 neighbor PE_ROUTERS update-source Loopback0
 neighbor 2.2.2.2 peer-group PE_ROUTERS
 neighbor 5.5.5.5 peer-group PE_ROUTERS
 neighbor 19.19.19.19 peer-group PE_ROUTERS
 !
 address-family vpnv4
  neighbor PE_ROUTERS send-community extended
  neighbor 2.2.2.2 activate
  neighbor 5.5.5.5 activate
  neighbor 19.19.19.19 activate

R2:
router bgp 26
 no bgp default ipv4-unicast
 neighbor PE_ROUTERS peer-group
 neighbor PE_ROUTERS remote-as 26
 neighbor PE_ROUTERS update-source Loopback0
 neighbor 1.1.1.1 peer-group PE_ROUTERS
 neighbor 5.5.5.5 peer-group PE_ROUTERS
 neighbor 19.19.19.19 peer-group PE_ROUTERS
```

```
 !
 address-family vpnv4
  neighbor PE_ROUTERS send-community extended
  neighbor 1.1.1.1 activate
  neighbor 5.5.5.5 activate
  neighbor 19.19.19.19 activate

R5:
router bgp 26
 no bgp default ipv4-unicast
 neighbor PE_ROUTERS peer-group
 neighbor PE_ROUTERS remote-as 26
 neighbor PE_ROUTERS update-source Loopback0
 neighbor 2.2.2.2 peer-group PE_ROUTERS
 neighbor 1.1.1.1 peer-group PE_ROUTERS
 neighbor 19.19.19.19 peer-group PE_ROUTERS
 !
 address-family vpnv4
  neighbor PE_ROUTERS send-community extended
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 19.19.19.19 activate

XR1:
router bgp 26
 address-family vpnv4 unicast
 !
 neighbor-group PE_ROUTERS
  remote-as 26
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 neighbor 1.1.1.1
  use neighbor-group PE_ROUTERS
 !
 neighbor 2.2.2.2
  use neighbor-group PE_ROUTERS
 !
 neighbor 5.5.5.5
  use neighbor-group PE_ROUTERS
 !
!
```

```
end
```

Task 4.1 Verification

```
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast summary
Wed Jun 27 15:21:58.352 UTC
BGP router identifier 19.19.19.19, local AS number 26
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0
BGP main routing table version 1
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.



Process       RcvTblVer   bRIB/RIB   LabelVer   ImportVer   SendTblVer   StandbyVer
Speaker               1          0          0           0            0            0

Neighbor        Spk    AS MsgRcvd MsgSent    TblVer   InQ OutQ   Up/Down   St/PfxRcd1.1.1.1
         0     26       4       2        0      0     0  00:00:19           02.2.2.2
         0     26       4       2        0      0     0  00:00:19           05.5.5.5
         0     26       2       2        0      0     0  00:00:21           0
```

Task 4.2 Solution

```
R1:
vrf definition ABC
 rd 26:65001
 route-target export 26:65001
 route-target import 26:65001
 !
 address-family ipv4 exit-
 address-family
!
interface FastEthernet0/0
 vrf forwarding ABC
 ip address 10.1.7.1 255.255.255.0
 no shutdown
!
router bgp 26
```

```
 address-family ipv4 vrf ABC
  neighbor 10.1.7.7 remote-as 65001
  neighbor 10.1.7.7 activate
  neighbor 10.1.7.7 as-override
 exit-address-family

R2:
vrf definition ABC
 rd 26:65001
 route-target export 26:65001
 route-target import 26:65001
 !
 address-family ipv4
 exit-address-family
!
interface FastEthernet0/0
 vrf forwarding ABC
 ip address 10.2.8.2 255.255.255.0
 no shutdown
!
router bgp 26
 address-family ipv4 vrf ABC
  neighbor 10.2.8.8 remote-as 65001
  neighbor 10.2.8.8 activate
  neighbor 10.2.8.8 as-override
 exit-address-family

R7:
router bgp 65001
 network 10.1.7.0 mask 255.255.255.0
 network 10.7.7.0 mask 255.255.255.0
 neighbor 10.1.7.1 remote-as 26

R8:
router bgp 65001
 network 10.2.8.0 mask 255.255.255.0
 network 10.8.8.0 mask 255.255.255.0
 neighbor 10.2.8.2 remote-as 26

XR1:
vrf ABC
 address-family ipv4 unicast
  import route-target
   26:65001
  !
  export route-target
```

```
   26:65001
  !
 !
!
interface POS0/6/0/0
 vrf ABC
 no ipv4 address
 ipv4 address 10.19.20.19 255.255.255.0
!
route-policy PASS
  pass
end-policy
!
router bgp 26
 vrf ABC
  rd 26:65001
  address-family ipv4 unicast
  !
  neighbor 10.19.20.20
   remote-as 65001
    address-family ipv4 unicast
    as-override
    route-policy PASS in
    route-policy PASS out
   !
  !
 !
!
end

XR2:
route-policy PASS
  pass
end-policy
!
router bgp 65001
 bgp router-id 10.19.20.20
 address-family ipv4 unicast
  network 10.19.20.0/24
  network 10.20.20.0/24
 !
 neighbor 10.19.20.19
  remote-as 26
  address-family ipv4 unicast
   route-policy PASS in
   route-policy PASS out
```

```
  !
 !
!
```

Task 4.2 Verification

```
RP/0/3/CPU0:XR2#show bgp ipv4 unicast
Wed Jun 27 15:49:27.951 UTC
BGP router identifier 10.19.20.20, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 7
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
*> 10.1.7.0/24        10.19.20.19                            0 26 26 i
*> 10.2.8.0/24        10.19.20.19                            0 26 26 i
*> 10.7.7.0/24        10.19.20.19                            0 26 26 i
*> 10.8.8.0/24        10.19.20.19                            0 26 26 i
*> 10.19.20.0/24      0.0.0.0                  0         32768 i
*> 10.20.20.0/24      0.0.0.0                  0         32768 i

Processed 6 prefixes, 6 paths
RP/0/3/CPU0:XR2#traceroute 10.7.7.7
Wed Jun 27 15:49:36.524 UTC

Type escape sequence to abort.
Tracing the route to 10.7.7.7

1  10.19.20.19 129 msec 5 msec  3 msec 2  26.3.19.3 [MPLS: Labels 16/18 Exp 5]
 4 msec  4 msec  3 msec 3  26.3.6.6 [MPLS: Labels 16/18 Exp 5]
 2 msec   3 msec  2 msec 4  10.1.7.1 [MPLS: Label 18 Exp 5]
 3 msec   2 msec  2 msec
5  10.1.7.7 4 msec  *  3 msec
RP/0/3/CPU0:XR2#traceroute 10.8.8.8
Wed Jun 27 15:49:48.651 UTC

Type escape sequence to abort.
Tracing the route to 10.8.8.8
```

```
1  10.19.20.19 6 msec  3 msec   1 msec 2  26.3.19.3 [MPLS: Labels 17/18 Exp 5]
 3 msec  4 msec  3 msec 3  26.3.4.4 [MPLS: Labels 17/18 Exp 5]
 3 msec   4 msec  2 msec 4  10.2.8.2 [MPLS: Label 18 Exp 5]
 2 msec   4 msec  2 msec
5  10.2.8.8 3 msec  *  3 msec
R7#show ip route bgp
      10.0.0.0/24 is subnetted, 6 subnets B 10.2.8.0
 [20/0] via 10.1.7.1, 00:02:24 B 10.20.20.0
 [20/0] via 10.1.7.1, 00:02:50 B 10.8.8.0
 [20/0] via 10.1.7.1, 00:02:24 B 10.19.20.0
 [20/0] via 10.1.7.1, 00:02:50
R7#ping 10.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Task 4.3 Solution

```
R1:
vrf definition ABC
 address-family ipv6
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 ipv6 address 2001:10:1:7::1/64
!
router bgp 26
 address-family vpnv6
  neighbor 2.2.2.2 activate
  neighbor 19.19.19.19 activate
 exit-address-family
 !
 address-family ipv6 vrf ABC
  neighbor 2001:10:1:7::7 remote-as 65001
  neighbor 2001:10:1:7::7 activate
  neighbor 2001:10:1:7::7 as-override
 exit-address-family

R2:
```

```
vrf definition ABC address-
 family ipv6
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 ipv6 address 2001:10:2:8::2/64
!
router bgp 26
 address-family vpnv6
  neighbor 1.1.1.1 activate
  neighbor 19.19.19.19 activate
 exit-address-family
 !
 address-family ipv6 vrf ABC
  neighbor 2001:10:2:8::8 remote-as 65001
  neighbor 2001:10:2:8::8 activate
  neighbor 2001:10:2:8::8 as-override
 exit-address-family

R7:
ipv6 unicast-routing
!
router bgp 65001
 neighbor 2001:10:1:7::1 remote-as 26
 !
 address-family ipv6
 neighbor 2001:10:1:7::1 activate
 network 2001:10:1:7::/64
 network 2001:10:7:7::/64
 exit-address-family

R8:
ipv6 unicast-routing
!
router bgp 65001
 neighbor 2001:10:2:8::2 remote-as 26
 !
 address-family ipv6
 neighbor 2001:10:2:8::2 activate
 network 2001:10:2:8::/64
 network 2001:10:8:8::/64
 exit-address-family

XR1:
```

```
vrf ABC
 address-family ipv6 unicast
  import route-target
   26:65001
  !
  export route-target
   26:65001
  !
 !
!
interface POS0/6/0/0
 ipv6 address 2001:10:19:20::19/64
!
router bgp 26
 address-family vpnv6 unicast
!
neighbor 1.1.1.1
 address-family vpnv6 unicast
!
neighbor 2.2.2.2
 address-family vpnv6 unicast
!
vrf ABC
 address-family ipv6 unicast
 !
 neighbor 10.19.20.20
  address-family ipv6 unicast
   route-policy PASS in
   route-policy PASS out as-override
  !
 !

XR2:
router bgp 65001
 address-family ipv6 unicast
  network 2001:10:19:20::/64
  network 2001:10:20:20::/64
 !
 neighbor 10.19.20.19
  address-family ipv6 unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
```

```
!
```

Task 4.3 Verification

```
RP/0/3/CPU0:XR2#show bgp ipv6 unicast
Wed Jun 27 15:57:59.955 UTC
BGP router identifier 10.19.20.20, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0800000
BGP main routing table version 7
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path*> 2001:10:1:7::/64
 2001:10:19:20::19
                        0 26 26 i   *> 2001:10:2:8::/64
 2001:10:19:20::19
                        0 26 26 i   *> 2001:10:7:7::/64
 2001:10:19:20::19
                        0 26 26 i   *> 2001:10:8:8::/64
 2001:10:19:20::19
                                              0 26 26 i
*> 2001:10:19:20::/64 ::                        0         32768 i
*> 2001:10:20:20::/64 ::                        0         32768 i

Processed 6 prefixes, 6 paths
RP/0/3/CPU0:XR2#traceroute 2001:10:7:7::7
Wed Jun 27 15:59:38.069 UTC

Type escape sequence to abort.
Tracing the route to 2001:10:7:7::7

1  2001:10:19:20::19 6 msec 5 msec 5 msec 2  ::ffff:26.3.19.3 [MPLS: Labels 16/22 Exp 0]
 4 msec 4 msec 5 msec 3  ::ffff:26.3.6.6 [MPLS: Labels 16/22 Exp 0]
 4 msec 4 msec 3 msec
4  2001:10:1:7::1 [MPLS: Label 22 Exp 0] 3 msec 4 msec 3 msec
5  2001:10:1:7::7 3 msec 3 msec 3 msec

RP/0/3/CPU0:XR2#traceroute 2001:10:8:8::8
Wed Jun 27 15:59:40.578 UTC
```

```
Type escape sequence to abort.
Tracing the route to 2001:10:8:8::8

1  2001:10:19:20::19 5 msec 5 msec 3 msec 2  ::ffff:26.3.19.3 [MPLS: Labels 17/22 Exp 0]
 3 msec 4 msec 4 msec 3  ::ffff:26.3.4.4 [MPLS: Labels 17/22 Exp 0]
 5 msec 4 msec 3 msec
4  2001:10:2:8::2 [MPLS: Label 22 Exp 0] 2 msec 4 msec 3 msec
5  2001:10:2:8::8 21 msec 4 msec 4 msec
R7#show ipv6 route bgp
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 B   2001:10:2:8::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0 B   2001:10:8:8::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0B   2001:10:19:20::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0B   2001:10:20:20::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0
R7#ping 2001:10:8:8::8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10:8:8::8, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 4.4 Solution

```
SW2:
ip routing
!
router bgp 10
 network 172.16.10.0 mask 255.255.255.0
 network 172.19.10.0 mask 255.255.255.0
 neighbor 172.19.10.19 remote-as 26

XR1:
vrf XYZ
 address-family ipv4 unicast
  import route-target
   26:10
  !
  export route-target
```

```
   26:10
  !
 !
!
interface GigabitEthernet0/1/0/0
 no ipv4 address
 vrf XYZ
 ipv4 address 172.19.10.19 255.255.255.0
!
router bgp 26
 vrf XYZ
  rd 26:10
  address-family ipv4 unicast
  !
  neighbor 172.19.10.10
   remote-as 10
   address-family ipv4 unicast
    route-policy PASS in
    route-policy PASS out
   !
  !
 !
!
end
```

Task 4.4 Verification

```
RP/0/0/CPU0:XR1#show ipv4 vrf all interface brief
Wed Jun 27 16:19:31.388 UTC

Interface                      IP-Address      Status          Protocol Vrf-Name
Loopback0                      19.19.19.19     Up              Up       default
MgmtEth0/0/CPU0/0              unassigned      Up              Up       default
MgmtEth0/0/CPU0/1              unassigned      Up              Up       default
MgmtEth0/0/CPU0/2              unassigned      Down            Down     default
GigabitEthernet0/1/0/0         172.19.10.19    Up              Up
      XYZ
GigabitEthernet0/1/0/1         26.3.19.19      Up              Up       default
GigabitEthernet0/1/0/2         unassigned      Up              Up       default
GigabitEthernet0/1/0/3         unassigned      Up              Up       default
POS0/6/0/0                     10.19.20.19     Up              Up       ABC

RP/0/0/CPU0:XR1#show bgp vrf XYZ ipv4 unicast summary
```

```
Wed Jun 27 16:18:47.704 UTC
BGP VRF XYZ, state: Active
BGP Route Distinguisher: 26:10
VRF ID: 0x60000003
BGP router identifier 19.19.19.19, local AS number 26
BGP table state: Active
Table ID: 0xe0000003
BGP main routing table version 41

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer   ImportVer   SendTblVer   StandbyVer
Speaker              41         41         41          41           41           41

Neighbor        Spk    AS MsgRcvd MsgSent    TblVer   InQ OutQ  Up/Down   St/PfxRcd
172.19.10.10      0    10       5       4        41     0    0 00:01:29           2

RP/0/0/CPU0:XR1#show bgp vrf XYZ ipv4 unicast
Wed Jun 27 16:18:50.569 UTC
BGP VRF XYZ, state: Active
BGP Route Distinguisher: 26:10
VRF ID: 0x60000003
BGP router identifier 19.19.19.19, local AS number 26
BGP table state: Active
Table ID: 0xe0000003
BGP main routing table version 41

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 26:10 (default for vrf XYZ)
*> 172.16.10.0/24    172.19.10.10             0             0 10 i
*> 172.19.10.0/24    172.19.10.10             0             0 10 i

Processed 2 prefixes, 2 paths
RP/0/0/CPU0:XR1#ping vrf XYZ 172.16.10.10
Wed Jun 27 16:19:14.481 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.10, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Task 4.5 Solution

```
R5:
vrf definition ABC
 rd 26:65001
 address-family ipv4
 route-target export 26:65001
 route-target import 26:65001
!
vrf definition XYZ
 rd 26:10
 address-family ipv4
 route-target export 26:10
 route-target import 26:10
!
interface FastEthernet1/0.35
 ip nat inside
!
interface FastEthernet1/0.45
 ip nat inside
!
interface FastEthernet1/0.56
 ip nat inside
!
interface FastEthernet1/0.59
 ip nat outside
!
router bgp 26
 neighbor 169.254.0.9 remote-as 2000
 !
 address-family ipv4
  network 26.255.1.0 mask 255.255.255.0
  network 26.255.2.0 mask 255.255.255.0
  neighbor 169.254.0.9 activate
 exit-address-family
 !
address-family ipv4 vrf ABC
  network 0.0.0.0 exit-
 address-family
!
address-family ipv4 vrf XYZ
  network 0.0.0.0
 exit-address-family
```

```
!
ip nat pool ABC_INTERNET 26.255.1.0 26.255.1.255 prefix-length 24
ip nat pool XYZ_INTERNET 26.255.2.0 26.255.2.255 prefix-length 24
ip nat inside source list RFC1918 pool ABC_INTERNET vrf ABC
ip nat inside source list RFC1918 pool XYZ_INTERNET vrf XYZ

!
ip route 26.255.1.0 255.255.255.0 Null0
ip route 26.255.2.0 255.255.255.0 Null0
ip route vrf ABC 0.0.0.0 0.0.0.0 169.254.0.9 global
ip route vrf XYZ 0.0.0.0 0.0.0.0 169.254.0.9 global
!

ip access-list standard RFC1918
 permit 10.0.0.0 0.255.255.255
 permit 172.16.0.0 0.15.255.255
 permit 192.168.0.0 0.0.255.255
```

Task 4.5 Verification

```
SW1#show ip bgp
BGP table version is 8, local router ID is 169.254.9.9
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path*> 26.255.1.0/24
    169.254.0.5              0             0 26 i*> 26.255.2.0/24
    169.254.0.5              0             0 26 i
*> 169.254.9.0/24   0.0.0.0                  0         32768 i
RP/0/3/CPU0:XR2#show route 169.254.9.9
Wed Jun 27 17:46:16.764 UTC
Routing entry for 0.0.0.0/0
  Known via "bgp 65001", distance 20, metric 0, candidate default path
  Tag 26, type external
  Installed Jun 27 17:00:01.348 for 00:46:15
  Routing Descriptor Blocks
    10.19.20.19, from 10.19.20.19
      Route metric is 0
  No advertising protos.
RP/0/3/CPU0:XR2#ping 169.254.9.9
Wed Jun 27 17:46:25.782 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 169.254.9.9, timeout is 2 seconds:!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms
RP/0/3/CPU0:XR2#ping 172.16.10.10
Wed Jun 27 17:46:47.028 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.10, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
R7#show ip route 169.254.9.9
% Network not in table
R7#show ip route 172.16.10.10
% Network not in table
R7#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "bgp 65001", distance 20, metric 0, candidate default path
  Tag 26, type external
  Last update from 10.1.7.1 00:49:19 ago
  Routing Descriptor Blocks:
  * 10.1.7.1, from 10.1.7.1, 00:49:19 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
R7#ping 169.254.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 169.254.9.9, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R7#ping 172.16.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.10, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
R8#show ip route 169.254.9.9
% Network not in table
R8#show ip route 172.16.10.10
% Network not in table
R8#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet Known via "bgp 65001",
 distance 20, metric 0, candidate default path
  Tag 26, type external
  Last update from 10.2.8.2 00:50:00 ago
  Routing Descriptor Blocks:
  * 10.2.8.2, from 10.2.8.2, 00:50:00 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
R8#ping 169.254.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 169.254.9.9, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/16 ms
R8#ping 172.16.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SW2#show ip route 169.254.9.9
% Network not in table
SW2#show ip route 10.20.20.20
% Subnet not in table
SW2#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet Known via "bgp 10",
 distance 20, metric 0, candidate default path
  Tag 26, type external
  Last update from 172.19.10.19 00:51:46 ago
  Routing Descriptor Blocks:
  * 172.19.10.19, from 172.19.10.19, 00:51:46 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 26
SW2#ping 169.254.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 169.254.9.9, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
SW2#ping 10.20.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.20, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R5#show ip route 169.254.9.9
Routing entry for 169.254.9.0/24
 Known via "bgp 26",
 distance 20, metric 0
  Tag 2000, type external
  Last update from 169.254.0.9 01:27:38 ago
  Routing Descriptor Blocks:
  * 169.254.0.9, from 169.254.0.9, 01:27:38 ago
    Route metric is 0, traffic share count is 1
   AS Hops 1
    Route tag 2000
    MPLS label: none
R5#ping 169.254.9.9
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 169.254.9.9, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R5#show ip nat translations vrf ABC
Pro Inside global      Inside local       Outside local      Outside global
icmp 26.255.1.2:8      10.1.7.7:8         169.254.9.9:8      169.254.9.9:8
--- 26.255.1.2         10.1.7.7           ---                ---
icmp 26.255.1.3:5      10.2.8.8:5         169.254.9.9:5      169.254.9.9:5
--- 26.255.1.3         10.2.8.8           ---                ---
icmp 26.255.1.1:20677  10.19.20.20:20677  169.254.9.9:20677  169.254.9.9:20677
--- 26.255.1.1         10.19.20.20        ---                ---
--- 26.255.1.4         10.20.20.20        ---                ---
R5#show ip nat translations vrf XYZ
Pro Inside global      Inside local       Outside local      Outside global
icmp 26.255.2.1:7      172.19.10.10:7     169.254.9.9:7      169.254.9.9:7

--- 26.255.2.1         172.19.10.10       ---                ---
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solution 5.1 (pending update)

Task 5.1 Solution

```
R1:
router isis 1
 address-family ipv4 unicast
  metric-style wide

R2:
mpls traffic-eng tunnels
!
interface FastEthernet1/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R3:
mpls traffic-eng tunnels
!
interface FastEthernet1/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng administrative-weight 1000
!
interface FastEthernet1/0.35
 mpls traffic-eng tunnels
 ip rsvp bandwidth
 mpls traffic-eng administrative-weight 1000
!
interface FastEthernet1/0.36
```

```
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.319
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R4:
mpls traffic-eng tunnels
!
interface FastEthernet1/0.24
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.34
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R5:
mpls traffic-eng tunnels
!
interface FastEthernet1/0.35
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.45
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
```

```
!
router isis 1
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

R6:
mpls traffic-eng tunnels
!
interface FastEthernet1/0.36
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet1/0.56
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2

XR1:
interface tunnel-te0
 ipv4 unnumbered Loopback0
 autoroute announce
 destination 2.2.2.2
 path-option 1 dynamic
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/1
 !
mpls traffic-eng
 interface GigabitEthernet0/1/0/1
```

Task 5.1 Verification

```
RP/0/0/CPU0:XR1#show mpls traffic-eng tunnels

Wed Jun 27 17:58:05.315 UTC
Signalling Summary:
              LSP Tunnels Process:   running
                     RSVP Process:   running
                       Forwarding:   enabled
          Periodic reoptimization:   every 3600 seconds, next in 2802 seconds
           Periodic FRR Promotion:   every 300 seconds, next in 274 seconds
          Auto-bw enabled tunnels:   0 (disabled)

Name: tunnel-te0  Destination: 2.2.2.2
  Status:
    Admin:    up Oper:   up   Path:  valid    Signalling: connected

    path option 1,  type dynamic  (Basis for Setup, path weight 50)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0

  Config Parameters:
    Bandwidth:         0 kbps (CT0) Priority: 7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute:  enabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  History:
    Tunnel has been up for: 00:00:35 (since Wed Jun 27 17:57:30 UTC 2012)
    Current LSP:
      Uptime: 00:00:35 (since Wed Jun 27 17:57:30 UTC 2012)

  Path info (IS-IS 1 level-2): Hop0: 26.3.19.3
Hop1: 26.3.6.6
Hop2: 26.5.6.5
Hop3: 26.4.5.4
Hop4: 26.2.4.2
    Hop5: 2.2.2.2

Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
RP/0/0/CPU0:XR1#show route 2.2.2.2
Wed Jun 27 17:58:10.735 UTC

Routing entry for 2.2.2.2/32
```

```
  Known via "isis 1", distance 115, metric 30, type level-2
  Installed Jun 27 17:57:30.507 for 00:00:40
  Routing Descriptor Blocks    2.2.2.2, from 2.2.2.2, via tunnel-te0
      Route metric is 30
  No advertising protos.
RP/0/0/CPU0:XR1#traceroute 2.2.2.2
Wed Jun 27 17:58:13.669 UTC

Type escape sequence to abort.
Tracing the route to 2.2.2.2
 1 26.3.19.3 [MPLS: Label 18 Exp 0]
 5 msec 3 msec  4 msec 2 26.3.6.6 [MPLS: Label 18 Exp 0]
 4 msec  3 msec  2 msec 3 26.5.6.5 [MPLS: Label 22 Exp 0]
 2 msec  3 msec  2 msec 4 26.4.5.4 [MPLS: Label 18 Exp 0]
 4 msec  3 msec  3 msec
 5  26.2.4.2 4 msec *  3 msec
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 2 v4

Full-Scale Lab 2 Solutions 6.1 - 6.2 (pending update)

Task 6.1 Solution

```
R1:
ip multicast-routing
ip pim ssm default
!
ip multicast-routing vrf ABC
!
vrf definition ABC
 address-family ipv4
 mdt default 232.1.2.19
 mdt data 232.1.255.0 0.0.0.255
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet0/0
 ip pim sparse-mode
!
interface FastEthernet1/0.16
 ip pim sparse-mode
!
router bgp 26
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 19.19.19.19 activate
 exit-address-family

R2:
ip multicast-routing
```

```
ip pim ssm default
!
ip multicast-routing vrf ABC
!
vrf definition ABC
 address-family ipv4
 mdt default 232.1.2.19
 mdt data 232.2.255.0 0.0.0.255
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet0/0
 ip pim sparse-mode
!
interface FastEthernet1/0.24
 ip pim sparse-mode
!
router bgp 26
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 19.19.19.19 activate
 exit-address-family

R3:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet1/0.34
 ip pim sparse-mode
!
interface FastEthernet1/0.35
 ip pim sparse-mode
!
interface FastEthernet1/0.36
 ip pim sparse-mode
!
interface FastEthernet1/0.319
 ip pim sparse-mode

R4:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet1/0.24
 ip pim sparse-mode
```

```
!
interface FastEthernet1/0.34
 ip pim sparse-mode
!
interface FastEthernet1/0.45
 ip pim sparse-mode

R5:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet1/0.35
 ip pim sparse-mode
!
interface FastEthernet1/0.45
 ip pim sparse-mode
!
interface FastEthernet1/0.56
 ip pim sparse-mode

R6:
ip multicast-routing
ip pim ssm default
!
interface FastEthernet1/0.16
 ip pim sparse-mode
!
interface FastEthernet1/0.36
 ip pim sparse-mode
!
interface FastEthernet1/0.56
 ip pim sparse-mode

XR1:
router bgp 26
 address-family ipv4 mdt
 !
 neighbor 1.1.1.1
  address-family ipv4 mdt
 !
 neighbor 2.2.2.2
  address-family ipv4 mdt
!
multicast-routing
 address-family ipv4
  mdt source Loopback0
```

```
  interface all enable
!
vrf ABC
 address-family ipv4
  mdt data 232.19.255.0/24
  mdt default ipv4 232.1.2.19
  interface all enable
!
router isis 1
 address-family ipv4 unicast
  mpls traffic-eng multicast-intact
!
end
```

Task 6.1 Verification

```
R1#sh bgp ipv4 mdt all summary
BGP router identifier 1.1.1.1, local AS number 26
BGP table version is 4, main routing table version 4
3 network entries using 444 bytes of memory
3 path entries using 168 bytes of memory
3/3 BGP path/bestpath attribute entries using 372 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1032 total bytes of memory
BGP activity 28/12 prefixes, 34/18 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd 2.2.2.2          4            26        6        6         4    0     0 00:02:28         1
19.19.19.19      4            26        7        10        4    0     0 00:01:22         1
R1#sh bgp ipv4 mdt all

BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 26:65001 (default for vrf ABC) *> 1.1.1.1/32
       0.0.0.0                                  0 ? *>i2.2.2.2/32
       2.2.2.2                  0    100        0 ? *>i19.19.19.19/32
   19.19.19.19                   100      0 i
```

```
R1#show ip pim vrf ABC neighbor

PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode 19.19.19.19         Tunnel0
                  00:00:30/00:01:21 v2    1 / DR G 2.2.2.2           Tunnel0
                  00:02:34/00:01:44 v2    1 / S P G
RP/0/0/CPU0:XR1#show pim rpf 2.2.2.2
Wed Jun 27 18:06:02.674 UTC

Table: IPv4-Multicast-default * 2.2.2.2/32 [115/30]
 via GigabitEthernet0/1/0/1 with rpf neighbor 26.3.19.3
```

RPF lookup fails without multicast intact for IS-IS for MPLS TE.

```
RP/0/0/CPU0:XR1#config t
Wed Jun 27 18:06:58.527 UTC
RP/0/0/CPU0:XR1(config)#router isis 1 RP/0/0/CPU0:XR1(config-
isis)# address-family ipv4 unicastRP/0/0/CPU0:XR1(config-isis-af)#no  mpls traffic-eng multicast-intact
RP/0/0/CPU0:XR1(config-isis-af)#commit
RP/0/0/CPU0:Jun 27 18:07:16.138 : config[65748]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xr1'. Use 'show configuration commit changes
1000000332' to view the changes.
RP/0/0/CPU0:XR1(config-isis-af)#end
RP/0/0/CPU0:Jun 27 18:07:16.177 : config[65748]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xr1RP/0/0/CPU0:XR1#show pim rpf 2.2.2.2
Wed Jun 27 18:07:18.252 UTC

Table: IPv4-Unicast-default
* 2.2.2.2/32 [115/30] via Null with rpf neighbor 0.0.0.0
```

Task 6.2 Solution

```
R1:
ip pim vrf ABC rp-address 10.0.0.1

R2:
ip pim vrf ABC rp-address 10.0.0.1
```

```
R7:
ip multicast-routing
ip pim rp-address 10.0.0.1
!
interface FastEthernet0/0
 ip pim sparse-mode
!
interface FastEthernet0/1
 ip pim sparse-mode

R8:
ip multicast-routing
ip pim rp-address 10.0.0.1
!
interface Loopback10
 ip address 10.0.0.1 255.255.255.255
 ip pim sparse-mode
!
interface FastEthernet0/0
 ip pim sparse-mode
!
interface FastEthernet0/1
 ip pim sparse-mode
!
router bgp 65001
 network 10.0.0.1 mask 255.255.255.255
!
ip msdp peer 10.20.20.20 connect-source FastEthernet0/1

XR1:
router pim
 vrf ABC
  address-family ipv4
   rp-address 10.0.0.1

XR2:
interface Loopback10
 ipv4 address 10.0.0.1 255.255.255.255
!
router bgp 65001
 address-family ipv4 unicast
  network 10.0.0.1/32
!
multicast-routing address-
 family ipv4
```

```
  interface all enable
 !
!
router pim
  address-family ipv4
   rp-address 10.0.0.1
!
router msdp
 peer 10.8.8.8
  connect-source GigabitEthernet0/4/0/0
 !
!
```

Task 6.2 Verification

```
RP/0/3/CPU0:XR2#show msdp peer
Wed Jun 27 18:12:07.870 UTC MSDP Peer 10.8.8.8 (?), AS 26
Description:
  Connection status: State: Up, Resets: 0, Connection Source: 10.20.20.20

    Uptime(Downtime): 00:01:08, SA messages received: 0
    TLV messages sent/received: 3/3
  Output messages discarded: 0
    Connection and counters cleared 00:01:08 ago
  SA Filtering:
    Input (S,G) filter: none
    Input RP filter: none
    Output (S,G) filter: none
    Output RP filter: none
  SA-Requests:
    Input filter: none
    Sending SA-Requests to peer: disabled
  Password: None
  Peer ttl threshold: 0
  Input queue size: 0, Output queue size: 0
  KeepAlive timer period: 30
  Peer Timeout timer period: 75
R7#traceroute 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.1.7.1 4 msec 0 msec 4 msec
  2 26.1.6.6 [AS 26] 0 msec 0 msec 4 msec
```

```
  3 26.3.6.3 [AS 26] 0 msec 0 msec 4 msec
  4 26.3.19.19 [AS 26] 4 msec 4 msec 4 msec 5 10.19.20.20 [AS 26] 56 msec * 4 msec

R7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#int f0/0R7(config-if)#ip igmp join 224.1.1.1
RP/0/3/CPU0:XR2#show pim topology 224.1.1.1
Wed Jun 27 18:13:56.476 UTC

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
    RA - Really Alive, IA - Inherit Alive, LH - Last Hop
    DSS - Don't Signal Sources, RR - Register Received
    SR - Sending Registers, E - MSDP External, EX - Extranet
    DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
    MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
    II - Internal Interest, ID - Internal Dissinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
 (*,224.1.1.1) SM Up: 00:00:15 RP: 10.0.0.1*
JP: Join(never) RPF: Decapstunnel0,10.0.0.1 Flags:
  POS0/7/0/0                  00:00:15  fwd Join(00:03:14)
R8#show ip mroute 224.1.1.1
Group 224.1.1.1 not found

RP/0/0/CPU0:XR1#conf t
Wed Jun 27 18:14:35.863 UTC
RP/0/0/CPU0:XR1(config)#int pos0/6/0/0RP/0/0/CPU0:XR1(config-if)#shut
RP/0/0/CPU0:XR1(config-if)#commit
R7#traceroute 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.1.7.1 4 msec 0 msec 0 msec
  2 26.1.6.6 [AS 26] 0 msec 0 msec 4 msec
  3 26.5.6.5 [AS 26] 4 msec 4 msec 4 msec
  4 26.4.5.4 [AS 26] 0 msec 0 msec 0 msec
  5 10.2.8.2 [AS 26] 4 msec 4 msec 0 msec  6 10.2.8.8 [AS 26] 0 msec * 4 msec

R7#config t
Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#int f0/0
R7(config-if)#ip igmp join 224.2.2.2
R8#show ip mroute 224.2.2.2
```

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 224.2.2.2), 00:00:04/00:03:25, RP 10.0.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:00:04/00:03:25
RP/0/0/CPU0:XR1#rollback config last 1
Wed Jun 27 18:15:42.439 UTC
Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.LC/0/6/CPU0:Jun 27 18:15:43.695 : ifmgr[173]: %PKT_INFRA-LINK-3-UPDOWN :
Interface POS0/6/0/0, changed state to Down
LC/0/6/CPU0:Jun 27 18:15:43.695 : ifmgr[173]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line
protocol on Interface POS0/6/0/0, changed state to Down
LC/0/6/CPU0:Jun 27 18:15:43.699 : ifmgr[173]: %PKT_INFRA-LINK-3-UPDOWN : Interface
POS0/6/0/0, changed state to Up

1 items committed in 1 sec (0)items/sec
Updating..RP/0/0/CPU0:Jun 27 18:15:46.016 : config_rollback[65748]: %MGBL-CONFIG-6-
DB_COMMIT : Configuration committed by user 'xr1'. Use 'show configuration commit
changes 1000000336' to view the changes.
R8#debug ip msdp routes
MSDP Routes debugging is on
SW1#ping vrf VLAN20 224.20.20.20 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 224.20.20.20, timeout is 2 seconds:
..........
R8#
MSDP(0): (10.20.20.100/32, 224.20.20.20), accepted
R8#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.20.20.100, 224.20.20.20), RP 10.0.0.1, BGP/AS 65001, 00:00:10/00:05:49, Peer 10.20.20.20
RP/0/3/CPU0:XR2#show msdp sa-cache 224.7.7.7
Wed Jun 27 18:19:01.190 UTC No SA entries found
SW2#ping vrf VLAN7 224.7.7.7 repeat 10
```

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 224.7.7.7, timeout is 2 seconds:
..........
RP/0/3/CPU0:XR2#show msdp sa-cache 224.7.7.7
Wed Jun 27 18:20:21.144 UTC

MSDP Flags:
E - set MRIB E flag , L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.  Timers age/expiration,
Cache Entry: (10.7.7.100, 224.7.7.7), RP 10.0.0.1, MBGP/AS 0, 00:00:05/local

  Learned from peer local, RPF peer local
  SAs recvd 0, Encapsulated data received: 0
    grp flags: none,  src flags: L
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Tasks (pending update)

Difficulty Rating (10 highest): 8

Lab Overview

The following scenario is a practice lab exam designed to test your skills at configuring Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco's CCIE Service Provider Version 3.0 Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab to complete all the configuration steps, take the time to research each networking technology and gain a deeper understanding of the principles behind its operation.

Lab Instructions

Before starting, ensure that the initial configuration scripts for this lab have been applied. If you have any questions related to the scenario solutions, visit our Online Community.

Refer to the attached diagrams for interface and protocol assignments. Upon completion, all devices in the Service Provider core should have full IP reachability to all networks in the core, and all customer devices should have full IP reachability to other sites belonging to the same customer, unless otherwise explicitly specified.

Lab Do’s and Don’ts

- Do not change or add any IP addresses from the initial configuration unless otherwise specified or required for troubleshooting.
- If additional IP addresses are needed but not specifically permitted by the task, use IP unnumbered.
- Do not change any interface encapsulations unless otherwise specified.
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified.
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified.
- Save your configurations often.

Grading

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to pass the exam. A section must work 100% with the requirements given to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Point Values

This lab is broken into 6 main technology sections, with point values for each section distributed as follows:

Section	Point Value
Bridging & Switching	5
IGP	11
MPLS	12

Section	Point Value
VPN	48
MPLS TE	12
Services	12

GOOD LUCK!

---

1. Bridging & Switching

1.1 Layer 2 Troubleshooting

- XR1 is unable to reach R2 or R7. Resolve this problem, but do not make any changes to SW1 to accomplish this.

Score: 5 Points

---

2. IGP

2.1 IS-IS Troubleshooting

- IS-IS Level 1 is preconfigured in AS 248, but the routers in this AS do not have full IGP connectivity to each other.
- Resolve any IS-IS-related issues so that R2, R4, and R8 have full connectivity to their Loopback0 interfaces and the core-facing links.

Score: 6 Points

2.2 OSPF Troubleshooting

- OSPF Area 0 is preconfigured in AS 3719, but the routers in this AS do not have full

IGP connectivity to each other.
- Resolve any OSPF-related issues so that R3, R7, and XR1 have full connectivity to their Loopback0 interfaces and the core-facing links.
- Do not make any changes to R7 to accomplish this.

Score: 5 Points

---

3. MPLS

3.1 MPLS Troubleshooting

- MPLS forwarding is preconfigured in AS 248, but end-to-end LSPs have not been established.
- Resolve any MPLS-related issues so that R2, R4, and R8 can build LSPs to each other's Loopback0 interfaces.

Score: 6 Points

3.2 MPLS Troubleshooting

- MPLS forwarding is preconfigured in AS 3719, but end-to-end LSPs have not been established.
- Resolve any MPLS-related issues so that R3, R7, and XR1 can build LSPs to each other's Loopback0 interfaces.
- Do not make any changes to R7 to accomplish this.

Score: 6 Points

---

4. VPN

4.1 IPv4 Unicast BGP Troubleshooting

- IPv4 Unicast BGP peerings are preconfigured within and between AS 248 and AS 3719.
- Resolve any BGP-related issues so that devices in AS 248 and AS 3719 have full IP

reachability to all of their Loopback0 networks, even if one of the Inter-AS links is down.

- Do not add any additional BGP peerings to accomplish this.
- Do not advertise the transit links between the ASes into IGP or BGP.

Score: 6 Points

4.2 IPv4 Unicast BGP Traffic Engineering

- Modify the BGP configuration of XR1 to reflect the following outputs:

```
R2#traceroute 34.0.0.19 source lo0

Type escape sequence to abort.
Tracing the route to 34.0.0.19

  1 46.2.8.8 [MPLS: Label 16 Exp 0] 0 msec 4 msec 0 msec
  2 46.4.8.4 4 msec 0 msec 4 msec
  3 169.254.34.3 0 msec 4 msec 0 msec
  4 34.3.7.7 [MPLS: Label 17 Exp 0] 0 msec 4 msec 0 msec
  5 34.7.19.19 20 msec *  4 msec
R3#traceroute 46.0.0.4 source lo0


Type escape sequence to abort.
Tracing the route to 46.0.0.4

  1 34.3.7.7 [MPLS: Label 17 Exp 0] 4 msec 0 msec 4 msec
  2 34.7.19.19 4 msec 0 msec 4 msec
  3 169.254.219.2 0 msec 4 msec 0 msec
  4 46.2.8.8 [MPLS: Label 16 Exp 0] 4 msec 0 msec 4 msec
  5 46.4.8.4 0 msec *  0 msec
```

- Note that the label numbers are arbitrary.
- This configuration should not affect forwarding to the other Loopback0 networks in AS 248 or 3719.

Score: 6 Points

4.3 Inter-AS MPLS L3VPN

- R3, R4, R7, and R8 are preconfigured with Loopbacks in VRF *ONE*.
- Modify the existing configuration in AS 248 and AS 3719 to allow for full Intra-AS and Inter-AS connectivity between Loopback addresses.
- Do not add any additional BGP peerings to accomplish this.
- Ensure that connectivity remains even if the Inter-AS link between R3 and R4 goes down.
- One static route is allowed to accomplish this task.

Score: 6 Points

4.4 Inter-AS MPLS L3VPN Traffic Engineering

- Configure R4 in such a way that all L3VPN traffic for VRF *ONE* prefers to use the link between XR1 and R2 for Inter-AS transit.
- If the link between XR1 and R2 is down, traffic should reroute via the R3/R4 link.
- Ensure that both XR1 and R2 can detect a loss of connectivity on their Inter-AS link in less than one second.

Score: 6 Points

4.5 Inter-AS MPLS L3VPN

- R7 and R8 use VRF *ONE* to connect to the AS 65001 customer sites.
- Modify the existing configuration so that R1, R5, R6, and XR2 have full connectivity to each other's Loopback0 networks and the transit links within AS 65001.
- Do not add any additional BGP peerings to accomplish this task.
- Do not redistribute between IGP and BGP on XR2 for this or any other task.

Score: 6 Points

4.6 Inter-AS MPLS L3VPN

- R5 and R6 are preconfigured with VRF *TWO* to connect to the SW1 and SW2 customer sites respectively. Additionally R1, R5, R6, and XR2 have Loopback1 interfaces which are part of VRF *TWO*.
- Modify the existing configuration so that there is a full mesh of connectivity for all links that are part of VRF *TWO*.
- Do not add any additional BGP peerings to accomplish this task.

- One static route is allowed to accomplish this task.
- Note that on SW1 and SW2 their links are preconfigured in the VRF *RIP* table.

Score: 6 Points

4.7 MPLS L2VPN

- Configure MPLS Layer 2 VPN so that the following verification can be performed:

```
SW1#show spanning-tree vlan 101
VLAN0101
  Spanning tree enabled protocol rstp
  Root ID    Priority    101
             Address     000c.8563.6f00
             Cost        19
             Port        3 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32869 (priority 32768 sys-id-ext 101)
             Address     0023.ac2a.3c80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------Fa0/1               Root FWD
 19        128.3    P2p Peer(STP)
SW1#show spanning-tree vlan 102
VLAN0102
  Spanning tree enabled protocol rstp
  Root ID    Priority    102
             Address     000c.8563.6f00
             Cost        19
             Port        3 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32870  (priority 32768 sys-id-ext 102)
             Address     0023.ac2a.3c80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------Fa0/1               Root FWD
 19        128.3    P2p Peer(STP)
SW1#traceroute 172.16.101.10
```

```
Type escape sequence to abort.
Tracing the route to 172.16.101.10
 1 172.16.101.10
 9 msec *  0 msec
SW1#traceroute 172.16.102.10

Type escape sequence to abort.
Tracing the route to 172.16.102.10
 1 172.16.102.10
 9 msec *  0 msec
```

Score: 6 Points

4.8 6VPE

- R1, R5, R6, and XR2's Loopback1 interfaces in VRF *TWO* are preconfigured with IPv6 addresses.
- Modify the existing configuration to allow for a full mesh of connectivity between these interfaces.
- Do not add additional BGP peerings to accomplish this.

Score: 6 Points

---

5. MPLS TE

5.1 Inter-AS MPLS TE

- R7 is preconfigured with a Loopback with the IP address 7.7.7.7/32.
- Configure an MPLS TE tunnel from R2 to R7 in such a way that the following verification can be performed:

```
R2#traceroute 7.7.7.7 source lo0



Type escape sequence to abort.
Tracing the route to 7.7.7.7

  1 46.2.8.8 [MPLS: Label 31 Exp 0] 4 msec 4 msec 0 msec
  2 46.4.8.4 [MPLS: Label 33 Exp 0] 4 msec 4 msec 4 msec
```

```
  3 169.254.34.3 [MPLS: Label 30 Exp 0] 0 msec 4 msec 4 msec
  4 34.3.7.7 0 msec * 0 msec
```

- One static route is allowed to accomplish this task.

Score: 6 Points

5.2 Inter-AS MPLS TE

- R8 is preconfigured with a Loopback with the IP address 8.8.8.8/32.
- Configure an MPLS TE tunnel from XR1 to R8 in such a way that the following verification can be performed:

```
RP/0/0/CPU0:XR1#traceroute 8.8.8.8 source 34.0.0.19

Thu Jun 21 17:59:38.796 UTC

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 34.7.19.7 [MPLS: Label 26 Exp 0] 6 msec 4 msec  4 msec
  2 34.3.7.3 [MPLS: Label 31 Exp 0] 4 msec  4 msec  3 msec
  3 169.254.34.4 [MPLS: Label 32 Exp 0] 4 msec  6 msec  3 msec
  4 46.4.8.8 5 msec *  4 msec
```

- One static route is allowed to accomplish this task.

Score: 6 Points

---

6. Services

6.1 Intra-AS Multicast Routing

- Configure Multicast Routing for AS 65001 on R1, R4, R6, R7, R8, and XR2.
- Enable PIM Sparse Mode on all the transit links within this AS.
- R1's Loopback0 should be the BSR and RP Candidate address.
- Do not enable multicast routing in the core of AS 248 or 3719.
- You are allowed to add an additional interface and IPv4 addressing on R7 and R8 to

accomplish this.

Score: 6 Points

6.2 Multicast L3VPN

- Using PIM Dense Mode, establish Multicast connectivity between the VRF TWO sites that connect R5 and R6 to SW1 and SW2, respectively.
- Use the MDT address 239.255.255.1.
- Do not add any additional BGP peerings to accomplish this.
- Configure R5’s link to SW1 to join the multicast group 224.9.9.9.
- Configure R6’s link to SW2 to join the multicast group 224.10.10.10.
- When complete, you should be able to perform the following verifications:

```
SW1#ping vrf RIP 224.10.10.10 repeat 5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 224.10.10.10, timeout is 2 seconds:

Reply to request 0 from 192.168.106.6, 25 ms
Reply to request 1 from 192.168.106.6, 1 ms
Reply to request 2 from 192.168.106.6, 1 ms
Reply to request 3 from 192.168.106.6, 1 ms
Reply to request 4 from 192.168.106.6, 1 ms
SW2#ping vrf RIP 224.9.9.9 repeat 5


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 224.9.9.9, timeout is 2 seconds:

Reply to request 0 from 192.168.59.5, 28 ms
Reply to request 1 from 192.168.59.5, 4 ms
Reply to request 2 from 192.168.59.5, 4 ms
Reply to request 3 from 192.168.59.5, 4 ms
Reply to request 4 from 192.168.59.5, 4 ms
```

Score: 6 Points

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solution 1.1 (pending update)

Task 1.1 Solution

```
XR1:
interface GigabitEthernet0/1/0/0
  auto
```

Task 1.1 Verification

```
SW1#show int gig0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type Gi0/1 notconnect
  trunk        full   1000 1000BaseSX SFP
SW1#

RP/0/0/CPU0:XR1#config t
Thu Jun 21 21:09:04.352 UTCRP/0/0/CPU0:XR1(config)#interface GigabitEthernet0/1/0/0
 RP/0/0/CPU0:XR1(config-if)# negotiation auto

RP/0/0/CPU0:XR1(config-if)#commit

SW1#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to upSW1#show int gig0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type Gi0/1 connected
    trunk        full   1000 1000BaseSX SFP
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solutions 2.1 - 2.2 (pending update)

Task 2.1 Solution

```
R2:
interface FastEthernet0/0.28
 no ip router isis
 ip router isis 1
!
no router isis
!
router isis 1
 no net 49.0001.0018.18ce.eb00.00
 !
 ! Any arbitrary unique NET address
 !
 net 49.0001.0018.18ce.eb01.00

R8:
router isis 1
 metric-style wide
```

Task 2.1 Verification

```
R2#show ip route isis
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      46.0.0.0/8 is variably subnetted, 6 subnets, 2 masksi L146.0.0.4/32
 [115/20] via 46.2.8.8, 00:00:22, FastEthernet0/0.28  i L146.0.0.8/32
 [115/10] via 46.2.8.8, 00:01:34, FastEthernet0/0.28
i L1     46.4.8.0/24 [115/20] via 46.2.8.8, 00:01:34, FastEthernet0/0.28
R2#ping 46.0.0.4 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 46.0.0.4, timeout is 2 seconds:
Packet sent with a source address of 46.0.0.2!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 2.2

```
XR1:
router ospf 1
 area 0
  interface GigabitEthernet0/1/0/0.719
   network broadcast

R3:
router ospf 1
 no network 43.0.0.3 0.0.0.0 area 0
 network 34.0.0.3 0.0.0.0 area 0
```

Task 2.2 Verification

```
RP/0/0/CPU0:XR1#show route ospf
Thu Jun 21 21:13:14.480 UTC
 O34.0.0.3/32
 [110/3] via 34.7.19.7, 00:00:16, GigabitEthernet0/1/0/0.719  O34.0.0.7/32
 [110/2] via 34.7.19.7, 00:00:16, GigabitEthernet0/1/0/0.719  O34.3.7.0/24
 [110/2] via 34.7.19.7, 00:00:16, GigabitEthernet0/1/0/0.719
RP/0/0/CPU0:XR1#ping 34.0.0.3 source lo0
Thu Jun 21 21:13:16.159 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 34.0.0.3, timeout is 2 seconds:!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solutions 3.1 - 3.2 (pending update)

Task 3.1 Solution

```
R2:
mpls ldp router-id Loopback0 force
```

Task 3.1 Verification

```
R2#show mpls ldp discovery
 Local LDP Identifier:
  169.254.219.2:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/0.28 (ldp): xmit/recv
            LDP Id: 46.0.0.8:0
R8#show ip route 169.254.219.2
% Network not in table

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#mpls ldp router-id Loopback0 force
R2(config)#end
R2#
%TDP-5-INFO: default: TDP ID removed
%SYS-5-CONFIG_I: Configured from console by console%LDP-5-NBRCHG: LDP Neighbor 46.0.0.8:0 (1) is UP
R2#show mpls ldp discovery
 Local LDP Identifier:
  46.0.0.2:0
    Discovery Sources:
    Interfaces:
```

```
        FastEthernet0/0.28 (ldp): xmit/recv
            LDP Id: 46.0.0.8:0
R2#show mpls ldp neighbor
    Peer LDP Ident: 46.0.0.8:0; Local LDP Ident 46.0.0.2:0
TCP connection: 46.0.0.8.42003 - 46.0.0.2.646

        State: Oper; Msgs sent/rcvd: 9/9; Downstream
        Up time: 00:00:14
        LDP discovery sources:
          FastEthernet0/0.28, Src IP addr: 46.2.8.8
        Addresses bound to peer LDP Ident:
          46.2.8.8        46.4.8.8        46.0.0.8        8.8.8.8
R2#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  46.0.0.8/32       0            Fa0/0.28   46.2.8.8
17         19         46.0.0.4/32       0            Fa0/0.28   46.2.8.8

18         Pop Label  46.4.8.0/24       0            Fa0/0.28   46.2.8.8
```

Task 3.2 Solution

```
R3:
mpls ldp neighbor 34.0.0.7 password 7 013025557E28573C021C
mpls label protocol ldp

XR1:
mpls ldp
 neighbor 34.0.0.7 password encrypted 06255E126F1E2A3A5432
```

Task 3.2 Verification

```
R7#debug mpls ldp transport events
LDP transport events debugging is on
<snip> %TCP-6-BADAUTH: Invalid MD5 digest from 34.0.0.19(16669) to 34.0.0.7(646)
<snip> ldp: Ignore Hello from 34.3.7.3, FastEthernet0/0.37; protocol mismatch
<snip>

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#mpls ldp neighbor 34.0.0.7 password 7 013025557E28573C021C
 R3(config)#mpls label protocol ldp
```

```
R3(config)#end
R3#%LDP-5-NBRCHG: LDP Neighbor 34.0.0.7:0 (1) is UP
%SYS-5-CONFIG_I: Configured from console by console

RP/0/0/CPU0:XR1#config t
Thu Jun 21 21:26:12.733 UTCRP/0/0/CPU0:XR1(config)#mpls ldp
RP/0/0/CPU0:XR1(config-ldp)# neighbor 34.0.0.7 password encrypted 06255E126F1E$
RP/0/0/CPU0:XR1(config-ldp)#commit

R7#%LDP-5-NBRCHG: LDP Neighbor 34.0.0.19:0 is UP
RP/0/0/CPU0:XR1#show mpls forwarding
Thu Jun 21 21:27:09.606 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  Pop         34.0.0.7/32        Gi0/1/0/0.719 34.7.19.7      190
16001  Pop         34.3.7.0/24        Gi0/1/0/0.719 34.7.19.7      0
16002  17          34.0.0.3/32        Gi0/1/0/0.719 34.7.19.7      0
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solutions 4.1 - 4.8 (pending update)

Task 4.1 Solution

```
R2:
router bgp 248
 no neighbor 169.254.129.19 remote-as 3719
 neighbor 169.254.219.19 remote-as 3719
 neighbor 169.254.219.19 password 7 112A3036343D282F2D0F
 !
 address-family ipv4
  neighbor 46.0.0.8 next-hop-self
  neighbor 169.254.219.19 activate
 exit-address-family

R3:
router bgp 3719
 address-family ipv4
  neighbor 34.0.0.7 next-hop-self

R4:
router bgp 248
 no neighbor 169.254.34.3 ebgp-multihop
 neighbor 169.254.34.3 ttl-security hops 1
 !
 address-family ipv4
```

```
  neighbor 46.0.0.8 next-hop-self
 exit-address-family

R7:
router bgp 3719
 address-family ipv4
  neighbor 34.0.0.3 route-reflector-client
  neighbor 34.0.0.19 route-reflector-client

R8:
router bgp 248
 address-family ipv4
  neighbor 46.0.0.2 route-reflector-client
  neighbor 46.0.0.4 route-reflector-client

XR1:
route-policy PASS
  pass
end-policy
!
router bgp 3719
 neighbor 34.0.0.7
  address-family ipv4 unicast
   next-hop-self
  !
 !
 neighbor 169.254.219.2
  address-family ipv4 unicast
   route-policy PASS in
   route-policy PASS out
```

Task 4.1 Verification

```
R7#show ip bgp
BGP table version is 19, local router ID is 34.0.0.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r>i34.0.0.3/32      34.0.0.3                 0    100      0 i
*> 34.0.0.7/32      0.0.0.0                  0         32768 i
r>i34.0.0.19/32     34.0.0.19                0    100      0 i* i46.0.0.2/32
      34.0.0.19              0    100      0 248 i*>i
        34.0.0.3               0    100      0 248 i* i46.0.0.4/32
      34.0.0.19                   100      0 248 i*>i
```

```
R8#show ip bgp

BGP table version is 21, local router ID is 46.0.0.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path   *>i34.0.0.3/32
     46.0.0.2                 0    100      0 3719 i* i
     46.0.0.4                 0    100      0 3719 i*>i34.0.0.7/32
     46.0.0.2                 0    100      0 3719 i* i
     46.0.0.4                 0    100      0 3719 i*>i34.0.0.19/32
     46.0.0.2                 0    100      0 3719 i* i
     46.0.0.4                 0    100      0 3719 i
r>i46.0.0.2/32       46.0.0.2                 0    100      0 i
r>i46.0.0.4/32       46.0.0.4                 0    100      0 i
*> 46.0.0.8/32       0.0.0.0                  0         32768 i
```

Task 4.2 Solution

```
XR1:
route-policy OUT_TO_R2
  if destination in (34.0.0.19/32) then
    prepend as-path 3719 2
  else
    pass
  endif
end-policy
!
route-policy IN_FROM_R2
  if destination in (46.0.0.4/32) then
    set local-preference 200
  else
    pass
  endif
end-policy
!
router bgp 3719
 neighbor 169.254.219.2
  address-family ipv4 unicast
   route-policy IN_FROM_R2 in
   route-policy OUT_TO_R2 out
```

Task 4.2 Verification

```
R2#traceroute 34.0.0.19 source lo0

Type escape sequence to abort.
Tracing the route to 34.0.0.19
 1 169.254.219.19 4 msec * 4 msec
R3#traceroute 46.0.0.4 source lo0

Type escape sequence to abort.
Tracing the route to 46.0.0.4
 1 169.254.34.4 0 msec * 0 msec

RP/0/0/CPU0:XR1#config t
Thu Jun 21 21:33:09.348 UTC
RP/0/0/CPU0:XR1(config)#router bgp 3719
RP/0/0/CPU0:XR1(config-bgp)# neighbor 169.254.219.2
RP/0/0/CPU0:XR1(config-bgp-nbr)#  address-family ipv4 unicast
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#  route-policy IN_FROM_R2 in
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#  route-policy OUT_TO_R2 out
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#commit
```

```
RP/0/0/CPU0:Jun 21 21:33:14.081 : config[65735]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xr1'. Use 'show configuration commit changes
1000000205' to view the changes.
RP/0/0/CPU0:XR1(config-bgp-nbr-af)#end
RP/0/0/CPU0:Jun 21 21:33:16.205 : config[65735]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xr1RP/0/0/CPU0:XR1#clear bgp ipv4 unicast * soft out

Thu Jun 21 21:33:34.393 UTCRP/0/0/CPU0:XR1#clear bgp ipv4 unicast * soft in
Thu Jun 21 21:33:36.321 UTC RP/0/0/CPU0:XR1#
R2#traceroute 34.0.0.19 source lo0

Type escape sequence to abort.
Tracing the route to 34.0.0.19

1 46.2.8.8 [MPLS: Label 19 Exp 0] 0 msec 0 msec 0 msec
  2 46.4.8.4 0 msec 4 msec 0 msec
  3 169.254.34.3 4 msec 0 msec 0 msec
  4 34.3.7.7 [MPLS: Label 18 Exp 0] 4 msec 0 msec 4 msec   5 34.7.19.19 4 msec *  4 msec

R3#traceroute 46.0.0.4 source lo0

Type escape sequence to abort.
Tracing the route to 46.0.0.4

1 34.3.7.7 [MPLS: Label 18 Exp 0] 4 msec 0 msec 4 msec
  2 34.7.19.19 4 msec 0 msec 4 msec
  3 169.254.219.2 4 msec 0 msec 0 msec
  4 46.2.8.8 [MPLS: Label 19 Exp 0] 0 msec 4 msec 0 msec   5 46.4.8.4 4 msec *  0 msec
R2#show ip bgp 34.0.0.19
BGP routing table entry for 34.0.0.19/32, version 14
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     4 3719
46.0.0.4 (metric 20) from 46.0.0.8 (46.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 46.0.0.4, Cluster list: 46.0.0.8 3719 3719 3719
    169.254.219.19 from 169.254.219.19 (34.0.0.19)
      Origin IGP, metric 0, localpref 100, valid, external
R3#show ip bgp 46.0.0.04
BGP routing table entry for 46.0.0.4/32, version 10
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     3
  248 34.0.0.19 (metric 3) from 34.0.0.7 (34.0.0.7)
      Origin IGP, localpref 200, valid, internal, best
```

```
      Originator: 34.0.0.19, Cluster list: 34.0.0.7
  248
    169.254.34.4 from 169.254.34.4 (46.0.0.4)      Origin IGP, metric 0, localpref 100
, valid, external
```

Task 4.3 Solution

```
R2:
router bgp 248
 no bgp default route-target filter
 address-family vpnv4
  neighbor 46.0.0.8 activate
  neighbor 46.0.0.8 next-hop-self
  neighbor 169.254.219.19 activate
 exit-address-family

R3:
ip vrf ONE
 route-target import 1:1
 route-target export 1:1
!
router bgp 3719
 address-family vpnv4 neighbor 34.0.0.7 activate
  neighbor 34.0.0.7 next-hop-self
  neighbor 169.254.34.4 activate
 exit-address-family

R4:
ip vrf ONE
 route-target import 1:1
 route-target export 1:1
!
router bgp 248
 address-family vpnv4
  neighbor 46.0.0.8 activate
  neighbor 46.0.0.8 next-hop-self
  neighbor 169.254.34.3 activate
 exit-address-family

R7:
ip vrf ONE
 route-target import 1:1
 route-target export 1:1
```

```
!
router bgp 3719
 address-family vpnv4
 neighbor 34.0.0.3 activate
 neighbor 34.0.0.3 route-reflector-client
 neighbor 34.0.0.19 activate
 neighbor 34.0.0.19 route-reflector-client

R8:
ip vrf ONE
 route-target import 1:1
 route-target export 1:1
!
router bgp 248
 address-family vpnv4
 neighbor 46.0.0.2 activate
 neighbor 46.0.0.2 route-reflector-client
 neighbor 46.0.0.4 activate
 neighbor 46.0.0.4 route-reflector-client

XR1:
router bgp 3719
 address-family vpnv4 unicast
  retain route-target all
 neighbor 34.0.0.7
  address-family vpnv4 unicast
   next-hop-self
  !
 !
 neighbor 169.254.219.2
  address-family vpnv4 unicast
   route-policy PASS in
   route-policy PASS out
!
router static
 address-family ipv4 unicast
  169.254.219.2/32 GigabitEthernet0/1/0/0.219
```

Task 4.3 Verification

```
R7#show ip bgp vpnv4 all
BGP table version is 10, local router ID is 34.0.0.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 34.0.0.3:1
*>i10.0.0.3/32      34.0.0.3                 0    100      0 i
Route Distinguisher: 34.0.0.7:1 (default for vrf ONE)*> i10.0.0.3/32
      34.0.0.3                 0    100      0 i*> i10.0.0.4/32
      34.0.0.3                 0    100      0 248 i*>  10.0.0.7/32
      0.0.0.0                  0         32768 i*> i10.0.0.8/32
      34.0.0.3                 0    100      0 248 i
Route Distinguisher: 46.0.0.4:1* i10.0.0.4/32       34.0.0.19
                    100      0 248 i*>i                   34.0.0.3
               0    100      0 248 i
Route Distinguisher: 46.0.0.8:1* i10.0.0.8/32       34.0.0.19
                    100      0 248 i*>i                   34.0.0.3
               0    100      0 248 i
R8#show ip bgp vpnv4 all
BGP table version is 14, local router ID is 46.0.0.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 34.0.0.3:1*>i10.0.0.3/32       46.0.0.2
               0    100      0 3719 i* i                   46.0.0.4
               0    100      0 3719 i
Route Distinguisher: 34.0.0.7:1*>i10.0.0.7/32       46.0.0.2
               0    100      0 3719 i* i                   46.0.0.4
               0    100      0 3719 i
Route Distinguisher: 46.0.0.4:1
*>i10.0.0.4/32      46.0.0.4                 0    100      0 i
Route Distinguisher: 46.0.0.8:1 (default for vrf ONE)*>i10.0.0.3/32       46.0.0.2
               0    100      0 3719 i*>i10.0.0.4/32       46.0.0.4
               0    100      0 i   *>i10.0.0.7/32       46.0.0.2
               0    100      0 3719 i*> 10.0.0.8/32       0.0.0.0
               0         32768 i
```

Task 4.4 Solution

```
R2:
interface FastEthernet0/0.219
 bfd interval 100 min_rx 100 multiplier 3
!
```

```
router bgp 248
 neighbor 169.254.219.19 fall-over bfd

R4:
router bgp 248
 address-family vpnv4
  neighbor 169.254.34.3 route-map VPNV4_IN in
  neighbor 169.254.34.3 route-map VPNV4_OUT out
!
route-map VPNV4_OUT permit 10
 set as-path prepend 248 248 248
!
route-map VPNV4_IN permit 10
 set local-preference 50

XR1:
router bgp 3719
 bfd minimum-interval 100
 bfd multiplier 3
 !
 neighbor 169.254.219.2
  bfd fast-detect
```

Task 4.4 Verification

```
R4#show bgp vpnv4 unicast rd 34.0.0.7:1 10.0.0.7/32
BGP routing table entry for 34.0.0.7:1:10.0.0.7/32, version 10
Paths: (2 available, best #1, no table)
  Advertised to update-groups:
     3
  3719 46.0.0.2 (metric 20) from 46.0.0.8 (46.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1 OSPF DOMAIN ID:0x0005:0x000000640200
        OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.0.0.7:0
      Originator: 46.0.0.2, Cluster list: 46.0.0.8
      mpls labels in/out 22/23
  3719 169.254.34.3 from 169.254.34.3 (34.0.0.3)
      Origin IGP, localpref 50
, valid, external
      Extended Community: RT:1:1 OSPF DOMAIN ID:0x0005:0x000000640200
        OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.0.0.7:0
      mpls labels in/out 22/22
R3#show bgp vpnv4 unicast rd 46.0.0.8:1 10.0.0.8/32
```

```
BGP routing table entry for 46.0.0.8:1:10.0.0.8/32, version 15
Paths: (2 available, best #1, no table)
  Advertised to update-groups:
     1 248
34.0.0.19 (metric 3) from 34.0.0.7 (34.0.0.7
)      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Originator: 34.0.0.19, Cluster list: 34.0.0.7
      mpls labels in/out 23/16007 248 248 248 248
169.254.34.4 from 169.254.34.4 (46.0.0.4)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:1
      mpls labels in/out 23/23
R7#traceroute vrf ONE 10.0.0.8

Type escape sequence to abort.
Tracing the route to 10.0.0.8

  1 34.7.19.19 [MPLS: Label 16007 Exp 0] 4 msec 4 msec 4 msec
2 169.254.219.2 [MPLS: Label 21 Exp 0] 0 msec 0 msec 4 msec

  3 10.0.0.8 4 msec *  0 msec
R8#traceroute vrf ONE 10.0.0.7

Type escape sequence to abort.
Tracing the route to 10.0.0.7

  1 46.2.8.2 [MPLS: Label 23 Exp 0] 0 msec 4 msec 0 msec
2 169.254.219.19 [MPLS: Label 16006 Exp 0] 4 msec 4 msec 4 msec
  3 10.0.0.7 4 msec *  0 msec

SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.SW1(config)#no vlan 219

RP/0/0/CPU0:XR1#
LC/0/1/CPU0:Jun 21 21:47:02.395 : bfd_agent[121]:
%L2-BFD-6-SESSION_STATE_DOWN :
BFD session to neighbor 169.254.219.2 on interface GigabitEthernet0/1/0/0.219 has
gone down. Reason: Echo function failed
RP/0/0/CPU0:Jun 21 21:47:02.401 : bgp[137]:
%ROUTING-BGP-5-ADJCHANGE : neighbor
169.254.219.2 Down - BFD (Bidirectional forwarding detection) session down
 (VRF:
default)
R7#traceroute vrf ONE 10.0.0.8
```

```
Type escape sequence to abort.
Tracing the route to 10.0.0.8

  1 34.3.7.3 [MPLS: Label 23 Exp 0] 0 msec 0 msec 4 msec
 2 169.254.34.4 [MPLS: Label 23 Exp 0] 5 msec 4 msec 0 msec
  3 10.0.0.8 0 msec *  0 msec
R8#traceroute vrf ONE 10.0.0.7

Type escape sequence to abort.
Tracing the route to 10.0.0.7

  1 46.4.8.4 [MPLS: Label 22 Exp 0] 4 msec 4 msec 4 msec
 2 169.254.34.3 [MPLS: Label 22 Exp 0] 0 msec 0 msec 4 msec

  3 10.0.0.7 4 msec *  0 msec
```

Task 4.5 Solution

```
R6:
router bgp 65001
 address-family ipv4
  network 10.0.0.6 mask 255.255.255.255
  neighbor 10.0.0.20 activate

R7:
router ospf 100 vrf ONE
redistribute bgp 3719 subnets
 !
router bgp 3719
 address-family ipv4 vrf ONE
  redistribute ospf 100
  exit-address-family

XR2:
route-policy PASS
  pass
end-policy
!
router bgp 65001
 neighbor 10.8.20.8
  address-family ipv4 unicast
   route-policy PASS in
```

```
   route-policy PASS out
   router bgp 65001
  !
 neighbor 10.0.0.6
  address-family ipv4 unicast
```

Task 4.5 Verification

```
R5#show ip route ospf
<snip>

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
O        10.0.0.1/32 [110/2] via 10.1.5.1, 00:45:14, FastEthernet0/0.15
O E2     10.0.0.3/32 [110/1] via 10.5.7.7, 00:01:00, FastEthernet0/0.57
O E2     10.0.0.4/32 [110/1] via 10.5.7.7, 00:01:00, FastEthernet0/0.57
O E2     10.0.0.6/32 [110/1] via 10.5.7.7, 00:00:00, FastEthernet0/0.57
O        10.0.0.7/32 [110/2] via 10.5.7.7, 00:45:14, FastEthernet0/0.57
O E2     10.0.0.8/32 [110/1] via 10.5.7.7, 00:01:00, FastEthernet0/0.57
O E2     10.0.0.20/32 [110/1] via 10.5.7.7, 00:00:30, FastEthernet0/0.57
O        10.1.7.0/24 [110/2] via 10.5.7.7, 00:45:14, FastEthernet0/0.57
                     [110/2] via 10.1.5.1, 00:45:14, FastEthernet0/0.15
O E2     10.6.20.0/24 [110/1] via 10.5.7.7, 00:00:30, FastEthernet0/0.57
O E2     10.8.20.0/24 [110/1] via 10.5.7.7, 00:00:30, FastEthernet0/0.57
R6#show ip route bgp
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
B        10.0.0.1/32 [200/0] via 10.8.20.8, 00:00:13
B        10.0.0.3/32 [200/0] via 10.8.20.8, 00:00:32
B        10.0.0.4/32 [200/0] via 10.8.20.8, 00:00:32
B        10.0.0.5/32 [200/0] via 10.8.20.8, 00:00:13
B        10.0.0.7/32 [200/0] via 10.8.20.8, 00:00:32
B        10.0.0.8/32 [200/0] via 10.8.20.8, 00:00:32
```

```
B        10.1.5.0/24 [200/0] via 10.8.20.8, 00:00:13
B        10.1.7.0/24 [200/0] via 10.8.20.8, 00:00:13
B        10.5.7.0/24 [200/0] via 10.8.20.8, 00:00:13
B        10.8.20.0/24 [200/0] via 10.0.0.20, 00:00:37
R5#traceroute 10.0.0.6 source lo0


Type escape sequence to abort.
Tracing the route to 10.0.0.6

  1 10.5.7.7 4 msec 0 msec 0 msec
  2 34.7.19.19 [MPLS: Label 16016 Exp 0] 8 msec 4 msec 0 msec
  3 169.254.219.2 [MPLS: Label 32 Exp 0] 4 msec 0 msec 4 msec
  4 10.8.20.8 [MPLS: Label 22 Exp 0] 4 msec 0 msec 4 msec
  5 10.8.20.20 32 msec 4 msec 4 msec
  6 10.6.20.6 0 msec *  0 msec
```

Task 4.6 Solution

```
R1:
vrf definition TWO
 rd 65001:1
 !
 address-family ipv4
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
 !
router bgp 65001
 !
 ! Cluster ID must be unique between R1 and XR2
 ! since they are both route reflectors in the same AS
 !
 no bgp cluster-id 65001
 neighbor 10.0.0.5 update-source Loopback0
 neighbor 10.0.0.20 update-source Loopback0
 !
 address-family vpnv4
  neighbor 10.0.0.5 route-reflector-client
 exit-address-family
 !
 address-family ipv4 vrf TWO
  no synchronization
```

```
  network 192.168.0.1 mask 255.255.255.255
 exit-address-family
!
router ospf 100
 mpls ldp autoconfig

R5:
vrf definition TWO
 rd 65001:1
 !
 address-family ipv4
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
 !
router bgp 65001
 neighbor 10.0.0.1 update-source Loopback0
!
router rip
 !
 address-family ipv4 vrf TWO
  redistribute bgp 65001 metric 1
 exit-address-family
!
router ospf 100
 mpls ldp autoconfig

R6:
vrf definition TWO
 rd 65001:1
 !
 address-family ipv4
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
!
router bgp 65001
 address-family ipv4
  neighbor 10.0.0.20 send-label
!
router rip
 !
 address-family ipv4 vrf TWO
  redistribute bgp 65001 metric 1
 exit-address-family
!
```

```
router ospf 1
 mpls ldp autoconfig

R7:
interface FastEthernet0/0.17
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/0.57
 mpls label protocol ldp
 mpls ip

R8:
router bgp 248
 address-family ipv4 vrf ONE
  neighbor 10.8.20.20 send-label
 exit-address-family

XR2:
vrf TWO
 address-family ipv4 unicast
  import route-target
   65001:1
  !
  export route-target
   65001:1
  !
 !
!
router static
 address-family ipv4 unicast
  10.8.20.8/32 GigabitEthernet0/4/0/0.820
 !
!
router bgp 65001
 address-family ipv4 unicast
  allocate-label all
 !
 neighbor 10.0.0.6
  no address-family ipv4 unicast
  address-family ipv4 labeled-unicast
  !
  address-family vpnv4 unicast
   route-reflector-client
 !
 neighbor 10.8.20.8
```

```
  no address-family ipv4 unicast address-
  family ipv4 labeled-unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
 vrf TWO
  rd 65001:1
  address-family ipv4 unicast
   network 192.168.0.20/32
!
router ospf 1
 mpls ldp auto-config
!
mpls ldp
!
end
```

Task 4.6 Verification

```
SW1#show ip route vrf RIP

Routing Table: RIP
<snip>

Gateway of last resort is not set

R    192.168.106.0/24 [120/1] via 192.168.59.5, 00:00:02, Vlan59
C    192.168.59.0/24 is directly connected, Vlan59
C    192.168.9.0/24 is directly connected, Vlan9
R    192.168.10.0/24 [120/1] via 192.168.59.5, 00:00:02, Vlan59
     192.168.0.0/32 is subnetted, 6 subnets
C       192.168.0.9 is directly connected, Loopback0
R       192.168.0.10 [120/1] via 192.168.59.5, 00:00:02, Vlan59
R       192.168.0.1 [120/1] via 192.168.59.5, 00:00:02, Vlan59
R       192.168.0.5 [120/1] via 192.168.59.5, 00:00:02, Vlan59
R       192.168.0.6 [120/1] via 192.168.59.5, 00:00:03, Vlan59
R       192.168.0.20 [120/1] via 192.168.59.5, 00:00:03, Vlan59
SW1#ping vrf RIP 192.168.0.10 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.9!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
R5#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  192.168.0.5/32[V]   \
                                       3196          aggregate/TWO
17         No Label   192.168.0.9/32[V]   \
                                       3578          Fa0/0.59   192.168.59.9
18         No Label   192.168.9.0/24[V]   \
                                       0             Fa0/0.59   192.168.59.9
19         No Label   192.168.59.0/24[V]  \
                                       0             aggregate/TWO
20         Pop Label  10.0.0.1/32      0             Fa0/0.15   10.1.5.1
21         25         10.0.0.3/32      0             Fa0/0.57   10.5.7.7
22         26         10.0.0.4/32      0             Fa0/0.57   10.5.7.7
23         30         10.0.0.6/32      0             Fa0/0.57   10.5.7.7
24         16         10.0.0.7/32      0             Fa0/0.57   10.5.7.7
25         24         10.0.0.8/32      0             Fa0/0.57   10.5.7.7
26         31         10.0.0.20/32     0             Fa0/0.57   10.5.7.7
27         Pop Label  10.1.7.0/24      0             Fa0/0.15   10.1.5.1
           21         10.1.7.0/24      0             Fa0/0.57   10.5.7.7
28         32         10.6.20.0/24     0             Fa0/0.57   10.5.7.7
29         33         10.8.20.0/24     0             Fa0/0.57   10.5.7.7

R5#show ip cef vrf TWO 192.168.0.10/32 detail
192.168.1.10    /32, epoch 0, flags rib defined all labels   recursive via 10.0.0.6 label 17
    nexthop 10.5.7.7 FastEthernet0/0.57 label 30
R5#traceroute vrf TWO 192.168.0.10 source 192.168.0.5

Type escape sequence to abort.
Tracing the route to 192.168.0.10
  1 34.7.19.7 [MPLS: Labels 30/17
 Exp 0] 4 msec 4 msec 4 msec  2 34.7.19.19 [MPLS: Labels 16016/17
 Exp 0] 4 msec 4 msec 4 msec  3 169.254.219.2 [MPLS: Labels 33/17
 Exp 0] 4 msec 4 msec 4 msec  4 10.8.20.8 [MPLS: Labels 31/17
 Exp 0] 4 msec 4 msec 4 msec  5 10.8.20.20 [MPLS: Labels 16000/17
 Exp 0] 24 msec 8 msec 4 msec  6 192.168.106.6 [MPLS: Label 17
 Exp 0] 0 msec 4 msec 4 msec  7 192.168.106.10
 0 msec * 0 msec
R6#show ip bgp labels
Network              Next Hop      In label/Out label
10.0.0.1/32          10.0.0.20      nolabel/16003
10.0.0.3/32          10.0.0.20      nolabel/16004
10.0.0.4/32          10.0.0.20      nolabel/16005 10.0.0.5/32          10.0.0.20      nolabel/16006
10.0.0.6/32          0.0.0.0       imp-null/nolabel
10.0.0.7/32          10.0.0.20      nolabel/16007
```

```
10.0.0.8/32          10.0.0.20     nolabel/16008
10.0.0.20/32         10.0.0.20     nolabel/imp-null
10.1.5.0/24          10.0.0.20     nolabel/16009
10.1.7.0/24          10.0.0.20     nolabel/16010
10.5.7.0/24          10.0.0.20     nolabel/16011
10.6.20.0/24         10.0.0.20     nolabel/imp-null
10.8.20.0/24         10.0.0.20     nolabel/imp-null
R6#show ip cef vrf TWO 192.168.0.9/32 detail
192.168.1.9 /32, epoch 0, flags rib defined all labels  recursive via 10.0.0.5 label 17
 recursive via 10.0.0.20 label 16006
      nexthop 10.6.20.20 FastEthernet0/0.620
R6#traceroute vrf TWO 192.168.0.9 source 192.168.0.6

Type escape sequence to abort.
Tracing the route to 192.168.0.9
  1 10.6.20.20 [MPLS: Labels 16006/17
 Exp 0] 4 msec 4 msec 4 msec  2 46.2.8.8 [MPLS: Labels 26/17
 Exp 0] 4 msec 0 msec 4 msec  3 46.2.8.2 [MPLS: Labels 28/17
 Exp 0] 4 msec 4 msec 0 msec  4 169.254.219.19 [MPLS: Labels 16012/17
 Exp 0] 8 msec 4 msec 4 msec  5 10.5.7.7 [AS 3719] [MPLS: Labels 23/17
 Exp 0] 0 msec 0 msec 4 msec  6 192.168.59.5 [MPLS: Label 17
 Exp 0] 4 msec 0 msec 4 msec  7 192.168.59.9
 4 msec *  4 msec
```

Task 4.7 Solution

```
R1:
interface FastEthernet0/0
 xconnect 10.0.0.20 1 encapsulation mpls
 no shutdown

XR2:
interface GigabitEthernet0/4/0/1
l 2transport
 !
!
l2vpn
 pw-class ATOM
  encapsulation mpls
  !
 !
 xconnect group L2VPN
  p2p L2VPN_XC
```

```
   interface GigabitEthernet0/4/0/1
   neighbor 10.0.0.1 pw-id 1
    pw-class ATOM
   !
  !
 !
!
```

Task 4.7 Verification

```
R1#show mpls ldp neighbor 10.0.0.20
    Peer LDP Ident: 10.0.0.20:0; Local LDP Ident 10.0.0.1:0
    TCP connection: 10.0.0.20.39097 - 10.0.0.1.646
    State: Oper; Msgs sent/rcvd: 16/18; Downstream
    Up time: 00:00:10
    LDP discovery sources: Targeted Hello 10.0.0.1 -> 10.0.0.20, active, passive
    Addresses bound to peer LDP Ident:
      10.0.0.20 10.6.20.20  10.8.20.20
R1#show mpls l2transport vc detail
Local interface: Fa0/0 up, line protocol up, Ethernet up
 Destination address: 10.0.0.20, VC ID: 1, VC status: up
    Output interface: Fa1/0.17, imposed label stack {31 16012}

    Preferred path: not configured
    Default path: active
    Next hop: 10.1.7.7
  Create time: 00:01:32, last status change time: 00:00:33
  Signaling protocol: LDP, peer 10.0.0.20:0 up Targeted Hello: 10.0.0.1(LDP Id) -> 10.0.0.20, LDP is UP
    Status TLV support (local/remote)   : enabled/not supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local  dataplane  status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: Not sent
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 27, remote 16012
    Group ID: local 0, remote 83887104 MTU: local 1500, remote 1500
 Remote interface description: GigabitEthernet0_4_0_1
  Sequencing: receive disabled, send disabled
  Control Word: Off (configured: autosense)
  VC statistics:
    transit packet totals: receive 36, send 13
```

```
    transit byte totals:   receive 2762, send 1190
    transit packet drops:  receive 0, seq error 0, send 0
RP/0/3/CPU0:XR2#show mpls ldp neighbor 10.0.0.1
Thu Jun 21 22:01:08.059 UTC

Peer LDP Identifier: 10.0.0.1:0
  TCP connection: 10.0.0.1:646 - 10.0.0.20:39097
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 20/19
  Up time: 00:02:13
  LDP Discovery Sources: Targeted Hello (10.0.0.20 -> 10.0.0.1, active)
  Addresses bound to this peer:
    10.0.0.1         10.1.5.1         10.1.7.1
RP/0/3/CPU0:XR2#show l2vpn xconnect detail
Thu Jun 21 22:01:33.135 UTC
 Group L2VPN, XC L2VPN_XC, state is up
; Interworking none  AC: GigabitEthernet0/4/0/1, state is up
    Type Ethernet
    MTU 1500; XC ID 0x5000001; interworking none
    Statistics:
      packets: received 115, sent 23
      bytes: received 8440, sent 2128 PW: neighbor 10.0.0.1, PW ID 1, state is up ( established )
    PW class ATOM, XC ID 0x5000001
    Encapsulation MPLS, protocol LDP
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set

      MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        16012                          27
      Group ID     0x5000400                      0x0
      Interface    GigabitEthernet0/4/0/1         unknown
MTU          1500                           1500
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                            0x6
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
    ------------ ------------------------------ -----------------------------
MIB cpwVcIndex: 1
Create time: 21/06/2012 21:58:54 (00:02:38 ago)
Last time status changed: 21/06/2012 21:59:42 (00:01:50 ago)
```

```
Statistics:
  packets: received 23, sent 115
  bytes: received 2128, sent 8440
SW1#ping 255.255.255.255

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:
. Reply to request 1 from 172.16.101.10
, 1 ms Reply to request 1 from 172.16.102.10
, 1 ms
Reply to request 2 from 172.16.101.10, 1 ms
Reply to request 2 from 172.16.102.10, 1 ms
Reply to request 3 from 172.16.101.10, 1 ms
Reply to request 3 from 172.16.102.10, 1 ms
Reply to request 4 from 172.16.101.10, 8 ms
Reply to request 4 from 172.16.102.10, 8 ms
```

Task 4.8 Solution

```
R1:
ipv6 unicast-routing
!
vrf definition TWO
 address-family ipv6
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
!
router bgp 65001
 address-family vpnv6
  neighbor 10.0.0.20 activate
  neighbor 10.0.0.5 activate
  neighbor 10.0.0.5 route-reflector-client
 exit-address-family
 !
 address-family ipv6 vrf TWO
  network 2001:192:168::1/128
 exit-address-family

R5:
ipv6 unicast-routing
!
vrf definition TWO
```

```
 address-family ipv6
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
!
router bgp 65001
 address-family vpnv6
  neighbor 10.0.0.1 activate
 exit-address-family
 !
 address-family ipv6 vrf TWO
  network 2001:192:168::5/128 exit-
 address-family

R6:
ipv6 unicast-routing
!
vrf definition TWO address-
 family ipv6
 route-target export 65001:1
 route-target import 65001:1
 exit-address-family
!
router bgp 65001
 address-family vpnv6
  neighbor 10.0.0.20 activate
 exit-address-family
 !
 address-family ipv6 vrf TWO
  network 2001:192:168::6/128
 exit-address-family

XR2:
vrf TWO
 address-family ipv6 unicast
  import route-target
   65001:1
  !
  export route-target
   65001:1
  !
router bgp 65001
 address-family vpnv6 unicast
 !
 neighbor 10.0.0.1
  address-family vpnv6 unicast
```

```
   route-reflector-client
  !
 !
 neighbor 10.0.0.6
  address-family vpnv6 unicast
  !
 !
 vrf TWO
  address-family ipv6 unicast
   network 2001:192:168::20/128
```

Task 4.8 Verification

```
R5#show bgp vpnv6 unicast all
BGP table version is 8, local router ID is 10.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65001:1 (default for vrf TWO)
*>i2001:192:168::1/128
                    ::FFFF:10.0.0.1          0    100      0 i
*> 2001:192:168::5/128
                    ::                       0         32768 i*>i2001:192:168::6/128
                    ::FFFF:10.0.0.6          0    100      0 i
*>i2001:192:168::20/128
                    ::FFFF:10.0.0.20
                                             0    100      0 i
R5#show ipv6 cef vrf TWO 2001:192:168::6/128 detail
2001:192:168::6/128, epoch 0, flags rib defined all labels  recursive via 10.0.0.6 label 21
 nexthop 10.5.7.7 FastEthernet0/0.57 label 27
R5#ping vrf TWO 2001:192:168::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:192:168::6, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solutions 5.1 - 5.2 (pending update)

Task 5.1 Solution

```
R2:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.28
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.219
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
!
interface Tunnel0
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 tunnel mode mpls traffic-eng
 tunnel destination 34.0.0.7
 tunnel mpls traffic-eng path-option 1 explicit name INTER-AS
!
ip route 7.7.7.7 255.255.255.255 Tunnel0
!
ip explicit-path name INTER-AS enable
 next-address loose 46.0.0.4
 next-address loose 34.0.0.3
```

```
R3:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 mpls traffic-eng passive-interface nbr-te-id 46.0.0.4 nbr-if-addr 169.254.34.4
 ip rsvp bandwidth
!
interface FastEthernet0/0.37
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

R4:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.34
 mpls traffic-eng tunnels
 mpls traffic-eng passive-interface nbr-te-id 34.0.0.3 nbr-if-addr 169.254.34.3
 ip rsvp bandwidth
!
interface FastEthernet0/0.48
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

R7:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.37
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.719
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
```

```
R8:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.28
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
interface FastEthernet0/0.48
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

XR1:
router ospf 1
 area 0
  mpls traffic-eng
  !
 !
 mpls traffic-eng router-id Loopback0
!
rsvp
 interface GigabitEthernet0/1/0/0.719
 !
!
mpls traffic-eng
 interface GigabitEthernet0/1/0/0.719
 !
```

Task 5.1 Verification

```
R2#show mpls traffic-eng topology 46.0.0.4

<snip>
 link[1]: Point-to-Point, Nbr IGP Id: 2200.0003.0000.00, nbr_node_id:-1, gen:2
           frag_id 0, Intf Address:169.254.34.4, Nbr Intf Address:34.0.0.3
 TE metric:MaxLinkMetric, IGP metric:MaxLinkMetric
, attribute flags:0x0
          SRLGs: None
          physical_bw: 100000 (kbps), max_reservable_bw_global: 75000 (kbps)
          max_reservable_bw_sub: 0 (kbps)
```

```
                              Global Pool       Sub Pool
               Total Allocated   Reservable        Reservable
               BW (kbps)         BW (kbps)         BW (kbps)
               ---------------   -----------       ----------
        bw[0]:            0          75000                 0
        bw[1]:            0          75000                 0
        bw[2]:            0          75000                 0
        bw[3]:            0          75000                 0
        bw[4]:            0          75000                 0
        bw[5]:            0          75000                 0
        bw[6]:            0          75000                 0
        bw[7]:            0          75000                 0
```

R2#show mpls traffic-eng tunnels

```
P2P TUNNELS/LSPs:

Name: R2_t0                               (Tunnel0) Destination: 34.0.0.7
  Status:     Admin: up Oper: up     Path: valid       Signalling: connected

    path option 1, type explicit INTER-AS (Basis for Setup, path weight 20)

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute announce: disabled LockDown: disabled Loadshare: 0        bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled LockDown: disabled  Verbatim: disabled


InLabel  :  -
OutLabel : FastEthernet0/0.28, 20
Next Hop : 46.2.8.8
RSVP Signalling Info:
     Src 46.0.0.2, Dst 34.0.0.7, Tun_Id 0, Tun_Instance 10
  RSVP Path Info:
    My Address: 46.2.8.2 Explicit Route: 46.2.8.8 46.4.8.8 46.4.8.4 46.0.0.4
 34.0.0.3*
    Record  Route:
    Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record  Route:  46.2.8.8 169.254.34.4 34.3.7.3 34.3.7.7
```

```
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
History:
  Tunnel:
    Time since created: 4 minutes, 20 seconds
    Time since path change: 1 minutes, 25 seconds
    Number of LSP IDs (Tun_Instances) used: 10
  Current LSP: [ID: 10]
    Uptime: 1 minutes, 25 seconds



#B#R3#show mpls traffic-eng tunnels#B#

P2P TUNNELS/LSPs:

LSP Tunnel R2_t0 is signalled, connection is up
  InLabel  : FastEthernet0/0.34, 33
  Prev Hop : 169.254.34.4
  OutLabel : FastEthernet0/0.37, implicit-null
  Next Hop : 34.3.7.7
  RSVP Signalling Info:
       Src 46.0.0.2, Dst 34.0.0.7, Tun_Id 0, Tun_Instance 10
    RSVP Path Info:
      My Address: 34.3.7.3 Explicit Route: 34.3.7.7 34.0.0.7
Record   Route:  169.254.34.4 46.4.8.8 46.2.8.2

      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  34.3.7.7
      Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

#B#R2#traceroute 7.7.7.7#B#

Type escape sequence to abort.
Tracing the route to 7.7.7.7

  1 46.2.8.8 [MPLS: Label 20 Exp 0] 0 msec 0 msec 4 msec
  2 46.4.8.4 [MPLS: Label 32 Exp 0] 0 msec 4 msec 4 msec
  3 169.254.34.3 [MPLS: Label 33 Exp 0] 0 msec 4 msec 0 msec
  4 34.3.7.7 4 msec *  0 msec
```

Task 5.2 Solution

```
XR1:
explicit-path name INTER-AS
 index 1 next-address loose ipv4 unicast 34.0.0.3
 index 2 next-address loose ipv4 unicast 46.0.0.4
!
interface tunnel-te0
 ipv4 unnumbered Loopback0
 destination 46.0.0.8
 path-option 1 explicit name INTER-AS
!
router static
 address-family ipv4 unicast
  8.8.8.8/32 tunnel-te0
```

Task 5.2 Verification

```
RP/0/0/CPU0:XR1#show mpls traffic-eng topology 34.0.0.3
Thu Jun 21 22:16:02.160 UTC

 IGP Id: 34.0.0.3, MPLS TE Id: 34.0.0.3
 Router Node  (OSPF 1 area 0)
 Link[0]:Point-to-Point, Nbr IGP Id:46.0.0.4
, Nbr Node Id:-1, gen:71920       Frag Id:6, Intf Address:169.254.34.3
, Intf Id:0 Nbr Intf Address:46.0.0.4
, Nbr Intf Id:0 TE Metric:4294967295, IGP Metric:4294967295
, Attribute Flags:0x0
      Attribute Names:
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:100000 (kbps), Max Reservable BW Global:75000 (kbps)
      Max Reservable BW Sub:0 (kbps)
                                 Global Pool       Sub Pool
               Total Allocated   Reservable        Reservable
               BW (kbps)         BW (kbps)         BW (kbps)
               ---------------   -----------       ----------
        bw[0]:            0          75000              0
        bw[1]:            0          75000              0
        bw[2]:            0          75000              0
        bw[3]:            0          75000              0
        bw[4]:            0          75000              0
        bw[5]:            0          75000              0
        bw[6]:            0          75000              0
        bw[7]:            0          75000              0
```

```
RP/0/0/CPU0:XR1#show mpls traffic-eng tunnels

Thu Jun 21 22:18:34.646 UTC
Signalling Summary:
              LSP Tunnels Process: running
                     RSVP Process: running
                       Forwarding: enabled
          Periodic reoptimization: every 3600 seconds, next in 23 seconds
           Periodic FRR Promotion: every 300 seconds, next in 132 seconds
          Auto-bw enabled tunnels: 0 (disabled)

Name: tunnel-te0    Destination: 46.0.0.8
  Status:
    Admin:    up Oper:     up   Path:  valid  Signalling: connected

    path option 1,  type explicit INTER-AS (Basis for Setup, path weight 2)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps CT0

  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7  Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  History:
    Tunnel has been up for: 00:01:05 (since Thu Jun 21 22:17:29 UTC 2012)
    Current LSP:
      Uptime: 00:01:05 (since Thu Jun 21 22:17:29 UTC 2012)
    Prior LSP:
      ID: path option 1 [2]
      Removal Trigger: path error
 Path info (OSPF 1 area 0):
Hop0: 34.7.19.7
Hop1: 34.3.7.7
Hop2: 34.3.7.3
Hop3: 34.0.0.3
Hop4: 46.0.0.4
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
RP/0/0/CPU0:XR1#traceroute 8.8.8.8 source 34.0.0.19

Thu Jun 21 22:18:21.120 UTC
```

```
Type escape sequence to abort.
Tracing the route to 8.8.8.8

 1 34.7.19.7 [MPLS: Label 28 Exp 0] 6 msec  4 msec  4 msec
 2 34.3.7.3 [MPLS: Label 34 Exp 0] 3 msec   5 msec  2 msec
 3 169.254.34.4 [MPLS: Label 24 Exp 0] 3 msec   4 msec  4 msec
 4 46.4.8.8 4 msec  *  4 msec
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 3 v4

Full-Scale Lab 3 Solutions 6.1 - 6.2 (pending update)

Task 6.1 Solution

```
R1:
ip multicast-routing
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet1/0.15
 ip pim sparse-mode
!
interface FastEthernet1/0.17
 ip pim sparse-mode
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0

R5:
ip multicast-routing
!
interface FastEthernet0/0.15
 ip pim sparse-mode
!
interface FastEthernet0/0.57
 ip pim sparse-mode

R6:
ip multicast-routing
!
interface FastEthernet0/0.620
```

```
 ip pim sparse-mode

R7:
ip multicast-routing vrf ONE
!
interface FastEthernet0/0.17
 ip pim sparse-mode
!
interface FastEthernet0/0.57
 ip pim sparse-mode
!
interface Tunnel0
 ip vrf forwarding ONE
 ip address 78.0.0.7 255.255.255.0
 ip pim sparse-mode
 tunnel source 34.0.0.7
 tunnel destination 46.0.0.8

R8:
ip multicast-routing vrf ONE
!
interface FastEthernet0/0.820
 ip pim sparse-mode
!
interface Tunnel0
 ip vrf forwarding ONE
 ip address 78.0.0.8 255.255.255.0
 ip pim sparse-mode
 tunnel source 46.0.0.8
 tunnel destination 34.0.0.7
!
ip mroute vrf ONE 10.0.0.1 255.255.255.255 Tunnel0

XR2:
multicast-routing
 address-family ipv4
  interface all enable
```

Task 6.1 Verification

```
R5#show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
```

```
RP 10.0.0.1
 (?), v2    Info source: 10.0.0.1 (?), via bootstrap
, priority 0, holdtime 150
         Uptime: 00:00:12, expires: 00:02:15
```

R6#show ip pim rp mapping

```
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4  RP 10.0.0.1
 (?), v2    Info source: 10.0.0.1 (?), via bootstrap
, priority 0, holdtime 150
         Uptime: 00:00:03, expires: 00:02:25

R6#conf t
Enter configuration commands, one per line. End with CNTL/Z.R6(config)#int lo0
R6(config-if)#ip pim sparse-mode
%PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 10.0.0.6 on interface Loopback0
R6(config-if)#ip igmp join 224.6.6.6
R6(config-if)#end R6#
R1#show ip mroute 224.6.6.6
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
 (*, 224.6.6.6), 00:00:06/00:03:23, RP 10.0.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0  Outgoing interface list:
 FastEthernet1/0.17, Forward/Sparse, 00:00:06/00:03:23
```

Task 6.2 Solution

```
R1:
router bgp 65001
 address-family ipv4 mdt
  neighbor 10.0.0.5 activate
  neighbor 10.0.0.5 route-reflector-client
```

```
  neighbor 10.0.0.20 activate exit-
 address-family

R5:
vrf definition TWO
 address-family ipv4
 mdt default 239.255.255.1
!
ip multicast-routing vrf TWO
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet0/0.59
 ip pim dense-mode
 ip igmp join-group 224.9.9.9
!
router bgp 65001
 address-family ipv4 mdt
  neighbor 10.0.0.1 activate
 exit-address-family

R6:
vrf definition TWO
 address-family ipv4
 mdt default 239.255.255.1
!
ip multicast-routing vrf TWO
!
interface Loopback0
 ip pim sparse-mode
!
interface FastEthernet0/0.106
 ip pim dense-mode
 ip igmp join-group 224.10.10.10
!
router bgp 65001
 address-family ipv4 mdt
  neighbor 10.0.0.20 activate
 exit-address-family

R7:
ip mroute vrf ONE 10.0.0.6 255.255.255.255 Tunnel0

R8:
ip mroute vrf ONE 10.0.0.5 255.255.255.255 Tunnel0
```

```
XR2:
router bgp 65001
 !
 address-family ipv4 mdt
 !
 neighbor 10.0.0.1
  address-family ipv4 mdt
  !
 !
 neighbor 10.0.0.6
  !
  address-family ipv4 mdt
   route-reflector-client
  !
 !
!

SW1:
ip multicast-routing vrf RIP distributed
!
interface Vlan9
 ip pim dense-mode
!
interface Vlan59
 ip pim dense-mode

SW2:
ip multicast-routing vrf RIP
!
interface Vlan10
 ip pim dense-mode
!
interface Vlan106
 ip pim dense-mode
```

Task 6.2 Verification

```
R5#show bgp ipv4 mdt all
BGP table version is 3, local router ID is 10.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65001:1 (default for vrf TWO)*> 10.0.0.5/32      0.0.0.0
                               0 ?*>i10.0.0.6/32      10.0.0.6
                 0    100      0 ?
R5#show ip pim vrf TWO neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.0.0.6          Tunnel1                  00:01:17/00:01:26 v2    1 / DR S P G
192.168.59.9      FastEthernet0/0.59       00:00:48/00:01:25 v2    1 / DR S P G
R7#show ip mroute vrf ONE 239.255.255.1
<snip>

(*, 239.255.255.1), 00:02:13/00:02:53, RP 10.0.0.1, flags: S
  Incoming interface: FastEthernet0/0.17, RPF nbr 10.1.7.1
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:01:35/00:02:53
(10.0.0.5, 239.255.255.1)
, 00:01:14/00:03:25, flags: T
  Incoming interface: FastEthernet0/0.57, RPF nbr 10.5.7.5
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:01:14/00:02:53
(10.0.0.6, 239.255.255.1)
, 00:02:15/00:03:24, flags: T
  Incoming interface: Tunnel0, RPF nbr 78.0.0.8, Mroute
  Outgoing interface list:
    FastEthernet0/0.57, Forward/Sparse, 00:01:27/00:03:12
SW1#ping vrf RIP 224.10.10.10

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.10.10.10, timeout is 2 seconds:
Reply to request 0 from 192.168.106.6, 33 ms
SW2#ping vrf RIP 224.9.9.9

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.9.9.9, timeout is 2 seconds:
Reply to request 0 from 192.168.59.5, 20 ms
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Tasks (pending update)

Difficulty Rating (10 highest): 9

Lab Overview

The following scenario is a practice lab exam designed to test your skills at configuring Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco's CCIE Service Provider Version 3.0 Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab to complete all the configuration steps, take the time to research each networking technology and gain a deeper understanding of the principles behind its operation.

Lab Instructions

Before starting, ensure that the initial configuration scripts for this lab have been applied. If you have any questions related to the scenario solutions, visit our Online Community.

Refer to the attached diagrams for interface and protocol assignments. Upon completion, all devices in the Service Provider core should have full IP reachability to all networks in the core, and all customer devices should have full IP reachability to other sites belonging to the same customer, unless otherwise explicitly specified.

Lab Do’s and Don’ts

- Do not change or add any IP addresses from the initial configuration unless otherwise specified or required for troubleshooting.
- If additional IP addresses are needed but not specifically permitted by the task, use IP unnumbered.
- Do not change any interface encapsulations unless otherwise specified.
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified.
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified.
- Save your configurations often.

Grading

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to pass the exam. A section must work 100% with the requirements given to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Point Values

This lab is broken into 6 main technology sections, with point values for each section distributed as follows:

Section	Point Value
Bridging & Switching	3
Unicast Routing	42
MPLS	3

Section	Point Value
VPN	37
MPLS TE	7
Services	8

GOOD LUCK!

---

1. Bridging & Switching

1.1 Layer 2 Troubleshooting

- XR1 and XR2 are unable to communicate over their POS link.
- Modify the configuration to restore IPv4 and IPv6 connectivity between the devices over this link.
- Do not make any changes to XR1 to accomplish this.

Score: 3 Points

---

2. Unicast Routing

2.1 IS-IS for IPv4

- Configure IS-IS for IPv4 in AS 1000.
- XR1 should be in area 49.0019.
- XR2 should be in area 49.0020.
- Establish Level-2 adjacencies between R5 & XR1, R5 & XR2, and XR1 & XR2.
- Establish Level-1 adjacencies between R2 & R5 and R2 & XR2.
- Advertise the Loopback0 networks of R2, XR1, and XR2 into Level-2.
- Advertise the Loopback0 network of R2 into Level-1.

Score: 4 Points

2.2 IS-IS for IPv4 Path Selection

- Modify the network so that R2 uses R5 to reach the IPv4 Loopback0 networks of XR1 and XR2.
- R2 should use XR2 to reach the Loopback0 network of R5 and the rest of the Level-2 transit links.
- If R2 loses connectivity to either R5 or XR2, it should still be able to reach all these destinations.
- Do not use any access-lists to accomplish this.
- XR2's configuration should automatically account for any new addresses advertised into the Level-2 network in the future.

Score: 4 Points

2.3 IS-IS High Availability

- Configure R2 so that can detect a failure of the circuits going to both R5 and XR2 within 600 ms.
- Do not modify the IS-IS hello interval or multiplier to accomplish this.

Score: 3 Points

2.4 IS-IS for IPv6

- Configure IPv6 IS-IS routing on the devices in AS 1000.
- Use a single SPF calculation for both the IPv4 and IPv6 path selection.

Score: 4 Points

2.5 IS-IS for IPv6 Path Selection

- Configure the network so that R2's IPv6 traffic flows follow identical paths as the previously modified IPv4 flows.

Score: 4 Points

2.6 OSPF for IPv4 and IPv6

- Configure OSPFv2 and OSPFv3 on the devices in AS 2000.
- All transit links should be in area 0 for both the IPv4 and IPv6 processes.
- Advertise the Loopback0 IPv4 and IPv6 addresses into OSPFv2 and OSPFv3 respectively, but do not send hello packets out these interfaces.
- Optimize both the OSPFv2 and OSPFv3 databases so that unnecessary LSAs are removed from flooding.

Score: 3 Points

2.7 IPv4 Unicast BGP

- Configure IPv4 Unicast iBGP peerings in AS 1000 between R2 & R5, R2 & XR1, and R2 & XR2.
- Configure IPv4 Unicast iBGP peerings in AS 2000 between R1 & R3 and R1 & R4.
- Configure IPv4 Unicast EBGP peerings between R3 & R5 and R3 & XR1.
- Advertise the IPv4 Loopback0 networks of all of these devices into BGP.
- When complete, there should be full Inter-AS connectivity between all IPv4 Loopback0 networks.
- Do not advertise the Inter-AS transit links into IGP or BGP.

Score: 4 Points

2.8 IPv4 Unicast BGP Policy Enforcement

- You have been tasked with implementing a BGP policy for AS 1000 and 2000 that conforms to RFC 1998, *An Application of the BGP Community Attribute in Multi-home Routing*.
- Configure the edge routers of these ASes (R3, R5, and XR1) so that if they receive an IPv4 Unicast BGP route from an EBGP peer with a community value in the format ASN:YY, where ASN is the local AS number and YY is the signaled value, the Local Preference of the prefix is changed to the signaled value.
- Specifically, this policy should account for the following possible values being signaled:

Community	Local Pref
ASN:80	80
ASN:90	90
ASN:110	110
ASN:120	120

- Ensure that the community attribute is exchanged in all IPv4 Unicast BGP peering sessions.

Score: 4 Points

2.9 IPv4 Unicast BGP Policy Enforcement

- Using the previously created policy, configure R3 in such a way that the following verifications can be performed:

```
R5#show bgp ipv4 unicast regexp ^2000$

BGP table version is 12, local router ID is 10.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.1/32      10.0.35.3                             110
      0 2000 i *>i10.0.0.3/32
      10.0.0.19                0    100      0 2000 i * 10.0.35.3                0      80
      0 2000 i *>i10.0.0.4/32      10.0.0.19                      120
      0 2000 i
*                   10.0.35.3                             0 2000 i
R2#show bgp ipv4 unicast regexp ^2000$

BGP table version is 11, local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i10.0.0.1/32      10.0.0.5                 0    110
      0 2000 i
*>i10.0.0.3/32      10.0.0.19                0    100      0 2000 i
*>i10.0.0.4/32      10.0.0.19                     120
      0 2000 i
```

Score: 4 Points

2.10 IPv6 Unicast BGP

- Configure IPv6 Unicast iBGP peerings in AS 1000 between R2 & XR1, R5 & XR1, and XR1 & XR2.
- Configure IPv6 Unicast iBGP peerings in AS 2000 between R1 & R3 and R3 & R4.
- Configure IPv4 Unicast EBGP peerings between R3 & R5 and R3 & XR1.
- Advertise the IPv6 Loopback0 networks of all of these devices into BGP.
- When complete, there should be full Inter-AS connectivity between all IPv6 Loopback0 networks.
- Do not advertise the Inter-AS transit links into IGP or BGP.

Score: 4 Points

2.11 IPv6 Unicast BGP Traffic Engineering

- Modify the IPv6 Unicast BGP configuration in AS 1000 to allow for the following verification to occur:

```
R3#sh bgp ipv6 unicast regexp ^1000$
BGP table version is 13, local router ID is 10.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric
 LocPrf Weight Path*  2001:10::2/128    2001:10:0:35::5          20
             0 1000 i*>                   2001:10:0:193::19
                                                        10
             0 1000 i*> 2001:10::5/128    2001:10:0:193::19
                                                        10
             0 1000 i*                    2001:10:0:35::5          20
             0 1000 i*> 2001:10::19/128   2001:10:0:35::5          10
             0 1000 i*                    2001:10:0:193::19
                                                        20
             0 1000 i                          *> 2001:10::20/128   2001:10:0:35::5          10
             0 1000 i*                    2001:10:0:193::19
                                                        20
             0 1000 i
```

Score: 4 Points

---

3. MPLS

3.1 LDP

- Enable LDP on all transit links within the AS 1000 and AS 2000 core networks.
- Use the minimum configuration necessary to accomplish this.

Score: 3 Points

4. VPN

The network consists of two Core Carriers, AS 1000 and AS 2000. The Core Carriers connect to the Customer Carrier AS 3000 via VRF *FOO* on R1, R4, and XR2. All routers in AS 1000 and AS 2000 additionally have a Loopback interface that is part of VRF *FOO*. The Customer Carrier then connects to the final End Customer sites via VRF BAR on R6, R7, and R8. All routers in AS 3000 additionally have a Loopback interface that is part of VRF *BAR*. When this section is complete, all devices in AS 3000 should have reachability to each other, as well as the Loopbacks in VRF *FOO* in the core, and the final End Customer should have reachability to its sites along with the VRF *BAR* Loopbacks in AS 3000.

4.1 VPNv4 Unicast BGP

- Configure VPNv4 Unicast iBGP peerings in AS 1000 between R2 & XR2, R5 & XR2, and XR1 & XR2.
- Configure IPv6 Unicast iBGP peerings in AS 2000 between R1 & R4 and R3 & R4.
- Configure IPv4 Unicast EBGP peerings between R4 & XR2.
- Advertise the VRF *FOO* Loopbacks into VPNv4 BGP on these devices.
- AS 1000 should export these Loopbacks with the RT value 1000:1.
- AS 2000 should export these Loopbacks with the RT value 2000:1.
- Do not modify any previous IPv4 Unicast BGP configuration on R1, R2, R4, or XR2.
- Ensure that there is full reachability between all of the VRF *FOO* Loopbacks even if one of the Inter-AS links between AS 1000 and AS 2000 is down.
- VPNv4 traffic should take the most direct paths through AS 1000 and AS 2000.
- One static route is allowed to accomplish this task.

Score: 4 Points

4.2 IS-IS PE to CE Routing

- Configure IS-IS for routing on the PE-CE links connecting AS 2000 to the AS 3000 VRF *FOO* site.
- Advertise the Loopback0 network of R6 into IS-IS.
- When complete, R6 should have reachability to all the VRF *FOO* Loopbacks in AS 1000 and AS 2000.
- Ensure that R1 and R4 route over the MPLS core to reach each other’s Loopbacks in

VRF *FOO*, but both route toward R6 to reach R6’s Loopback.

Score: 4 Points

4.3 BGP PE to CE Routing

- Configure BGP for routing on the PE-CE links connecting AS 1000 to the AS 3000 VRF *FOO* site.
- Advertise the transit links and Loopback0 networks of R7 and R8 into BGP.
- When complete, R6, R7, and R8 should have reachability to all links in the AS 3000 sites as well as the VRF *FOO* Loopbacks in AS 1000 and AS 2000.

Score: 3 Points

4.4 CsC VPNv4 Unicast BGP

- Configure a full mesh of VPNv4 BGP peerings between the routers in AS 3000.
- Advertise their Loopback interfaces that are members of VRF *BAR*.
- Use Route Target import and export values of 3000:1.
- When complete, there should be a full mesh of connectivity between the three Loopbacks that are members of VRF *BAR*.
- Ensure that connectivity remains even if one of AS 1000’s links to AS 3000 goes down or if one of AS 2000’s links to AS 3000 goes down.
- Two static routes are allowed to accomplish this task.

Score: 4 Points

4.5 OSPF PE to CE Routing

- The End Customer sites that connect to AS 3000 are preconfigured for OSPFv2 routing.
- Configure R6, R7, and R8 in AS 3000 to use OSPF process 100 as the PE to CE routing protocol for these sites.
- Do not modify any of the OSPF `network` statements on the CE routers to accomplish this.
- When complete, SW1 and SW2 should have a full mesh of connectivity to each other’s sites as well as to the three Loopbacks that are members of VRF *BAR* on the AS 3000 routers.

- Ensure that reachability between the End Customer sites remains even if one of SW1's links to either R7 or R8 is down.

Score: 4 Points

4.6 VPNv4 High Availability

- Configure the network so that AS 1000 and AS 3000 can detect a failure of their Inter-AS links and begin to reconverge in three seconds.
- Do not make any changes to R7 or R8 to accomplish this.

Score: 3 Points

4.7 VPNv4 High Availability

- Configure the network so that AS 1000 and AS 2000 can detect a failure of their Inter-AS links and begin to reconverge in 15 0ms.
- R5 and XR1 should install backup VPNv4 paths in the FIB for faster convergence, according to the following verification. Note that the order of the path selection is not significant, but simply that a best route and backup route appear.

```
R5#show bgp vpnv4 unicast vrf FOO 172.16.0.6/32
BGP routing table entry for 10.0.0.5:1:172.16.0.6/32, version 324
Paths: (2 available, best #2, table FOO)
  Additional-path
  Not advertised to any peer
  2000, imported path from 10.0.0.4:1:172.16.0.6/32
    10.0.0.4 (metric 10) from 10.0.0.20 (10.0.0.20)
      Origin incomplete, metric 10, localpref 100, valid, internal, backup/repair

      Extended Community: RT:2000:1 , recursive-via-host
      mpls labels in/out nolabel/29
  2000, imported path from 10.0.0.1:1:172.16.0.6/32
    10.0.0.1 from 10.0.0.20 (10.0.0.20)      Origin incomplete, localpref 100, valid, internal, best

      Extended Community: RT:2000:1 , recursive-via-host
      mpls labels in/out nolabel/25
RP/0/0/CPU0:XR1#show bgp vpnv4 unicast vrf FOO 172.16.0.6/32
Sun Jun 24 11:38:24.752 UTC
BGP routing table entry for 172.16.0.6/32, Route Distinguisher: 10.0.0.19:1
Versions:
  Process           bRIB/RIB   SendTblVer
```

```
  Speaker                343        343
Last Modified: Jun 24 11:38:19.550 for 00:00:05
Paths: (2 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  2000
    10.0.0.1 (metric 40) from 10.0.0.20 (10.0.0.20)
      Received Label 25      Origin incomplete, localpref 100, valid, internal, best
, import-candidate,
imported
      Extended community: RT:2000:1
  Path #2: Received by speaker 0
  2000
    10.0.0.4 from 10.0.0.20 (10.0.0.20)
      Received Label 29      Origin incomplete, metric 10, localpref 100, valid, internal, backup
,
imported
      Extended community: RT:2000:1
```

Score: 4 Points

4.8 VPNv6 Unicast BGP

- Configure IPv6 EBGP peerings between R1 & R6, R4 & R6, R7 & XR2, and R8 & XR2.
- Do not add any additional BGP peerings besides these.
- Advertise the IPv6 Loopbacks and IPv6 transit links in AS 3000 into IPv6 BGP.
- Use the same RT import and export policy as defined for VPNv4.
- Core routers in AS 1000 and AS 2000 are preconfigured with IPv6 Loopbacks in VRF FOO; advertise these into BGP.
- When complete, R6, R7, and R8 should have IPv6 reachability to all the IPv6 links in AS 3000, as well as the IPv6 VRF FOO Loopbacks in AS 1000 and AS 2000.

Score: 4 Points

4.9 L2TPv3

- Configure L2TPv3 between R1 and R5 to form an L2VPN between R7 and SW1.
- Do not modify any configuration on R7 to accomplish this.
- When complete, you should be able to perform the following verifications:

```
SW1#show ip route ospf
     7.0.0.0/32 is subnetted, 1 subnets
O       7.7.7.7 [110/2] via 79.0.0.7, 00:02:55, Vlan59
SW1#ping 7.7.7.7 source 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 9.9.9.9
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/30/34 ms
SW1#traceroute 7.7.7.7


Type escape sequence to abort.
Tracing the route to 7.7.7.7

  1 79.0.0.7 16 msec *  16 msec
```

Score: 3 Points

4.10 AToM

- Configure AToM between R2 and XR2 to form an L2VPN between R8 and SW2.
- Do not modify any configuration on SW2 to accomplish this.
- When complete, you should be able to perform the following verifications:

```
SW2#traceroute vrf VLAN100 100.0.0.8

Type escape sequence to abort.
Tracing the route to 100.0.0.8

  1 100.0.0.8 16 msec *  12 msec
SW2#traceroute vrf VLAN200 200.0.0.8


Type escape sequence to abort.
Tracing the route to 200.0.0.8
```

```
1 200.0.0.8 16 msec *  16 msec
```

Score: 4 Points

---

5. MPLS TE

5.1 MPLS Traffic Engineering

- Configure AS 1000 to support MPLS Traffic Engineering.
- All transit interfaces in the core should support TE reservations up to 50 Mbps, but no more than 15 Mbps reserved per tunnel.

Score: 3 Points

5.2 Inter-Area MPLS Traffic Engineering

- Configure an MPLS TE tunnels R2 to XR1.
- R2 should route traffic to XR1’s Loopback0 via a TE tunnel toward XR2.
- Do not use static routing to accomplish this.

Score: 4 Points

---

6. Services

6.1 Multicast MPLS VPN

- Enable PIM Sparse Mode on all interfaces in the global routing tables of AS 1000, 2000, and 3000.
- Enable PIM Sparse Mode on the VRF *FOO* Loopback interfaces in AS 1000 and 2000.
- Configure R6 to advertise its Loopback0 interface as the BSR and RP candidate.
- Configure IPv4 MDT BGP in AS 1000 and 2000 to follow the same topology as your previously created VPNv4 and VPNv6 BGP peerings.
- Use the default MDT address of 232.0.0.1 and an MDT data range of 232.255.255.0/24.

- When complete, all routers in AS 1000, 2000, and 3000 should agree that R6 is the RP for VRF *FOO*, and a full mesh of MDT tunnels should be established between the routers in AS 1000 and 2000.
- Static multicast routing is allowed to accomplish this.

Score: 4 Points

6.2 Multicast MPLS VPN

- Configure R6, R7, and R8 to join the multicast group 239.0.0.X on their Loopback0 interfaces, where X is the router number.
- Configure R1, R2, R3, R4, and R5 to join the multicast group 239.0.0.X on their VRF *FOO* Loopback1 interfaces, where X is the router number.
- When complete, R6, R7, and R8 should be able to ping all 239.0.0.X group addresses and get a response from the Loopback of the router joined to that group address.

Score: 4 Points

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solution 1.1 (pending update)

Task 1.1 Solution

```
XR2:
no interface POS0/7/0/0
interface POS0/7/0/0
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface POS0/7/0/0.1920 point-to-point
 ipv4 address 10.19.20.20 255.255.255.0
 ipv6 address 2001:10:19:20::20/64
 pvc 192
```

Task 1.1 Verification

```
RP/0/3/CPU0:XR2#show ip int brief
Sun Jun 24 17:58:58.108 UTC

Interface                        IP-Address      Status                Protocol
Loopback0                        10.0.0.20       Up                    Up
MgmtEth0/3/CPU0/0                unassigned      Up                    Up
MgmtEth0/3/CPU0/1                unassigned      Up                    Up
MgmtEth0/3/CPU0/2                unassigned      Down                  Down
GigabitEthernet0/4/0/0           unassigned      Up                    Up
GigabitEthernet0/4/0/0.205       10.0.205.20     Up                    Up
GigabitEthernet0/4/0/0.220       10.0.220.20     Up                    Up
GigabitEthernet0/4/0/1           unassigned      Up                    Up
GigabitEthernet0/4/0/2           unassigned      Up                    Up
GigabitEthernet0/4/0/3           unassigned      Up                    Up
POS0/7/0/0                       10.19.20.20     Up                    Down

RP/0/3/CPU0:XR2#config t
```

```
Sun Jun 24 17:59:03.590 UTC
RP/0/3/CPU0:XR2(config)#no interface POS0/7/0/0
RP/0/3/CPU0:XR2(config)#interface POS0/7/0/0
RP/0/3/CPU0:XR2(config-if)# encapsulation frame-relay
RP/0/3/CPU0:XR2(config-if)# frame-relay intf-type dce
RP/0/3/CPU0:XR2(config-if)#!
RP/0/3/CPU0:XR2(config-if)#interface POS0/7/0/0.1920 point-to-point
RP/0/3/CPU0:XR2(config-subif)# ipv4 address 10.19.20.20 255.255.255.0
RP/0/3/CPU0:XR2(config-subif)# ipv6 address 2001:10:19:20::20/64
RP/0/3/CPU0:XR2(config-subif)# pvc 192RP/0/3/CPU0:XR2(config-fr-vc)#commit
LC/0/7/CPU0:Jun 24 17:59:07.238 : ifmgr[173]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line
protocol on Interface POS0/7/0/0, changed state to Down
LC/0/7/CPU0:Jun 24 17:59:07.247 : ifmgr[173]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line
protocol on Interface POS0/7/0/0, changed state to Up
RP/0/3/CPU0:Jun 24 17:59:09.360 : config[65734]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'xr2'. Use 'show configuration commit changes
1000000176' to view the changes. RP/0/3/CPU0:XR2(config-fr-vc)#end

RP/0/3/CPU0:Jun 24 17:59:09.401 : config[65734]: %MGBL-SYS-5-CONFIG_I : Configured
from console by xr2
RP/0/3/CPU0:XR2#show ip int brief
Sun Jun 24 17:59:14.030 UTC

Interface                      IP-Address      Status              Protocol
Loopback0                      10.0.0.20       Up                  Up
MgmtEth0/3/CPU0/0              unassigned      Up                  Up
MgmtEth0/3/CPU0/1              unassigned      Up                  Up
MgmtEth0/3/CPU0/2              unassigned      Down                Down
GigabitEthernet0/4/0/0         unassigned      Up                  Up
GigabitEthernet0/4/0/0.205     10.0.205.20     Up                  Up
GigabitEthernet0/4/0/0.220     10.0.220.20     Up                  Up
GigabitEthernet0/4/0/1         unassigned      Up                  Up
GigabitEthernet0/4/0/2         unassigned      Up                  Up
GigabitEthernet0/4/0/3         unassigned      Up                  Up
POS0/7/0/0                     unassigned      Up                  Up
POS0/7/0/0.1920                10.19.20.20     Up                  Up
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solutions 2.1 - 2.11 (pending update)

Task 2.1 Solution

```
R2:
router isis 1000
 is-type level-1
 net 49.0020.0000.0000.0002.00
 passive-interface loopback0
!
interface FastEthernet0/0.25
 ip router isis 1000
!
interface FastEthernet0/0.220
 ip router isis 1000

R5:
router isis 1000
 net 49.0020.0000.0000.0005.00
 passive-interface loopback0
!
interface FastEthernet0/0.25
```

```
 ip router isis 1000
 isis circuit-type level-1
!
interface FastEthernet0/0.205
 ip router isis 1000
 isis circuit-type level-2
!
interface Loopback0
 isis circuit-type level-2

XR1:
router isis 1000
 is-type level-2-only
 net 49.0019.0000.0000.0019.00
 interface Loopback0
  passive
  address-family ipv4 unicast
 !
 interface GigabitEthernet0/1/0/0.195
  address-family ipv4 unicast
 !
 interface POS0/6/0/0.1920
  address-family ipv4 unicast

XR2:
router isis 1000
 net 49.0020.0000.0000.0020.00
 interface Loopback0
  passive
  circuit-type level-2-only
  address-family ipv4 unicast
 !
 interface GigabitEthernet0/4/0/0.205
  circuit-type level-2-only
  address-family ipv4 unicast
 !
 interface GigabitEthernet0/4/0/0.220
  circuit-type level-1
  address-family ipv4 unicast
 !
 interface POS0/7/0/0.1920
  circuit-type level-2-only
  address-family ipv4 unicast
 !
```

```
!
```

Task 2.1 Verification

```
R2#show isis neighbors

System Id       Type Interface    IP Address      State Holdtime Circuit Id
R5              L1   Fa0/0.25     10.0.25.5       UP    26       R2.01
XR2             L1   Fa0/0.220    10.0.220.20     UP    9        XR2.01

R2#show ip route isis
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.220.20 to network 0.0.0.0

i*L1  0.0.0.0/0 [115/10] via 10.0.220.20, 00:00:52, FastEthernet0/0.220
                [115/10] via 10.0.25.5, 00:00:52, FastEthernet0/0.25
R5#show isis neighbors

System Id       Type Interface    IP Address      State Holdtime Circuit Id
R2              L1   Fa0/0.25     10.0.25.2       UP    8        R2.01
XR1             L2   Fa0/0.195    10.0.195.19     UP    8        XR1.01
XR2             L2   Fa0/0.205    10.0.205.20     UP    9        XR2.03
R5#show ip route isis
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
i L1     10.0.0.2/32 [115/10] via 10.0.25.2, 00:02:35, FastEthernet0/0.25
```

```
i L2     10.0.0.19/32 [115/10] via 10.0.195.19, 00:00:00, FastEthernet0/0.195
i L2     10.0.0.20/32 [115/10] via 10.0.205.20, 00:02:48, FastEthernet0/0.205
i L1     10.0.220.0/24 [115/20] via 10.0.25.2, 00:02:35, FastEthernet0/0.25
i L2     10.19.20.0/24 [115/20] via 10.0.205.20, 00:00:00, FastEthernet0/0.205
                       [115/20] via 10.0.195.19, 00:00:00, FastEthernet0/0.195
RP/0/3/CPU0:XR2#show isis neighbors
Sun Jun 24 18:09:06.297 UTC

IS-IS 1000 neighbors:
System Id      Interface         SNPA           State Holdtime Type IETF-NSF
R2             Gi0/4/0/0.220     0018.18ce.eb00 Up    22       L1   Capable
R5             Gi0/4/0/0.205     0001.975b.6c00 Up    29       L2   Capable
XR1            PO0/7/0/0.1920    *PtoP*         Up    29       L2   Capable

Total neighbor count: 3
RP/0/3/CPU0:XR2#show route ipv4 unicast isis
Sun Jun 24 18:09:08.963 UTC

i L1 10.0.0.2/32 [115/10] via 10.0.220.2, 00:03:07, GigabitEthernet0/4/0/0.220
i L2 10.0.0.5/32 [115/10] via 10.0.205.5, 00:03:17, GigabitEthernet0/4/0/0.205
i L2 10.0.0.19/32 [115/10] via 10.19.20.19, 00:05:48, POS0/7/0/0.1920
i L1 10.0.25.0/24 [115/20] via 10.0.220.2, 00:03:07, GigabitEthernet0/4/0/0.220
i L2 10.0.195.0/24 [115/20] via 10.19.20.19, 00:00:36, POS0/7/0/0.1920
                   [115/20] via 10.0.205.5, 00:00:36, GigabitEthernet0/4/0/0.205
RP/0/0/CPU0:XR1#show isis neighbors
Sun Jun 24 18:09:25.291 UTC

IS-IS 1000 neighbors:
System Id      Interface         SNPA           State Holdtime Type IETF-NSF
R5             Gi0/1/0/0.195     0001.975b.6c00 Up    22       L2   Capable
XR2            PO0/6/0/0.1920    *PtoP*         Up    23       L2   Capable

Total neighbor count: 2
RP/0/0/CPU0:XR1#show route ipv4 unicast isis

Sun Jun 24 18:09:32.290 UTC

i L2 10.0.0.2/32 [115/20] via 10.19.20.20, 00:00:54, POS0/6/0/0.1920
                 [115/20] via 10.0.195.5, 00:00:54, GigabitEthernet0/1/0/0.195
i L2 10.0.0.5/32 [115/10] via 10.0.195.5, 00:00:54, GigabitEthernet0/1/0/0.195
i L2 10.0.0.20/32 [115/10] via 10.19.20.20, 00:06:18, POS0/6/0/0.1920
i L2 10.0.25.0/24 [115/20] via 10.0.195.5, 00:00:54, GigabitEthernet0/1/0/0.195
i L2 10.0.205.0/24 [115/20] via 10.19.20.20, 00:00:54, POS0/6/0/0.1920
                   [115/20] via 10.0.195.5, 00:00:54, GigabitEthernet0/1/0/0.195
```

```
i L2 10.0.220.0/24 [115/20] via 10.19.20.20, 00:06:08, POS0/6/0/0.1920
```

Task 2.2 Solution

```
R5:
router isis 1000
 redistribute isis ip level-2 into level-1 route-map ISIS_ROUTE_LEAKING
!
ip prefix-list ISIS_ROUTE_LEAKING seq 5 permit 10.0.0.19/32
ip prefix-list ISIS_ROUTE_LEAKING seq 10 permit 10.0.0.20/32
!
route-map ISIS_ROUTE_LEAKING permit 10
 match ip address prefix-list ISIS_ROUTE_LEAKING

XR1:
prefix-set XR1_XR2_LOOPBACKS
  10.0.0.19/32,
  10.0.0.20/32
end-set
!
route-policy ISIS_ROUTE_LEAKING
  if not destination in XR1_XR2_LOOPBACKS then
    pass
endif
end-policy
!
router isis 1000
 address-family ipv4 unicast
  propagate level 2 into level 1 route-policy ISIS_ROUTE_LEAKING
 !
!
```

Task 2.2 Verification

```
R2#show ip route isis
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.220.20 to network 0.0.0.0

i*L1  0.0.0.0/0 [115/10] via 10.0.220.20, 00:07:27, FastEthernet0/0.220
                [115/10] via 10.0.25.5, 00:07:27, FastEthernet0/0.25
      10.0.0.0/8 is variably subnetted, 11 subnets, 2 masksi ia
     10.0.0.5/32 [115/148] via 10.0.220.20, 00:00:02, FastEthernet0/0.220  i ia
     10.0.0.19/32 [115/148] via 10.0.25.5, 00:00:17, FastEthernet0/0.25  i ia
     10.0.0.20/32 [115/148] via 10.0.25.5, 00:00:17, FastEthernet0/0.25  i ia
     10.0.195.0/24
       [115/158] via 10.0.220.20, 00:00:02, FastEthernet0/0.220i ia
     10.0.205.0/24
       [115/148] via 10.0.220.20, 00:00:02, FastEthernet0/0.220i ia
     10.19.20.0/24
           [115/148] via 10.0.220.20, 00:00:02, FastEthernet0/0.220
```

Task 2.3 Solution

```
R2:
interface FastEthernet0/0.25
 bfd interval 200 min_rx 200 multiplier 3
!
interface FastEthernet0/0.220
 bfd interval 200 min_rx 200 multiplier 3
!
router isis 1000
 bfd all-interfaces

R5:
interface FastEthernet0/0.25
 bfd interval 200 min_rx 200 multiplier 3
 isis bfd

XR2:
router isis 1000
 interface GigabitEthernet0/4/0/0.220
  bfd minimum-interval 200
  bfd multiplier 3
  bfd fast-detect ipv4
```

Task 2.3 Verification

```
R2#show bfd neighbors details

NeighAddr                              LD/RD     RH/RS     State     Int
10.0.25.5                               2/1      Up        Up        Fa0/0.25
Session state is UP and using echo function with 200 ms interval.
OurAddr: 10.0.25.2
Local Diag: 0, Demand mode: 0, Poll bit: 0 MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(26)
Rx Count: 22, Rx Interval (ms) min/max/avg: 1/992/821 last: 92 ms ago
Tx Count: 27, Tx Interval (ms) min/max/avg: 1/984/844 last: 784 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF ISIS
Uptime: 00:00:17
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
```

```
             My Discr.: 1                - Your Discr.: 2
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 200000

NeighAddr                             LD/RD     RH/RS     State     Int
10.1.220.20                            1/1048580 Up        Up        Fa0/0.220
Session state is UP and using echo function with 200 ms interval.

OurAddr: 10.0.220.2
Local Diag: 0, Demand mode: 0, Poll bit: 0 MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3

Received MinRxInt: 2000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 2000(30)
Rx Count: 3, Rx Interval (ms) min/max/avg: 1/1960/980 last: 572 ms ago
Tx Count: 31, Tx Interval (ms) min/max/avg: 760/992/875 last: 572 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF ISIS
Uptime: 00:00:00
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 1048580          - Your Discr.: 1
             Min tx interval: 2000000    - Min rx interval: 2000000
             Min Echo interval: 1000
```

Task 2.4 Solution

```
R2:
ipv6 unicast-routing
!
interface FastEthernet0/0.25
 ipv6 router isis 1000
!
interface FastEthernet0/0.220
 ipv6 router isis 1000

R5:
ipv6 unicast-routing
!
interface FastEthernet0/0.25
 ipv6 router isis 1000
!
```

```
interface FastEthernet0/0.195
 ipv6 router isis 1000
!
interface FastEthernet0/0.205
 ipv6 router isis 1000

XR1:
router isis 1000
 address-family ipv6 unicast
  single-topology
 !
 interface Loopback0
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/1/0/0.195
  address-family ipv6 unicast
  !
 !
 interface POS0/6/0/0.1920
  address-family ipv6 unicast

XR2:
router isis 1000
 address-family ipv6 unicast
  single-topology
 !
 interface Loopback0
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/4/0/0.205
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/4/0/0.220
  address-family ipv6 unicast
  !
 !
 interface POS0/7/0/0.1920
  address-family ipv6 unicast
  !
 !
```

```
!
```

Task 2.4 Verification

```
R2#show ipv6 route isis
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I1  ::/0 [115/10]
     via FE80::201:97FF:FE5B:6C00, FastEthernet0/0.25
     via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220
R5#show ipv6 route isis
IPv6 Routing Table - default - 15 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I1  2001:10::2/128 [115/10]
     via FE80::218:18FF:FECE:EB00, FastEthernet0/0.25
I2  2001:10::19/128 [115/10]
     via FE80::2D0:79FF:FE03:F87E, FastEthernet0/0.195
I2  2001:10::20/128 [115/10]
     via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.205
I1  2001:10:0:220::/64 [115/20]
     via FE80::218:18FF:FECE:EB00, FastEthernet0/0.25
I2  2001:10:19:20::/64 [115/20]
     via FE80::2D0:79FF:FE03:F87E, FastEthernet0/0.195
     via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.205
RP/0/0/CPU0:XR1#show route ipv6 unicast isis
Sun Jun 24 18:19:07.625 UTC

i L2 2001:10::2/128
      [115/20] via fe80::9ca0:71ff:fe0f:b9ad, 00:01:14, POS0/6/0/0.1920
      [115/20] via fe80::201:97ff:fe5b:6c00, 00:01:14, GigabitEthernet0/1/0/0.195
i L2 2001:10::5/128
      [115/10] via fe80::201:97ff:fe5b:6c00, 00:01:35, GigabitEthernet0/1/0/0.195
i L2 2001:10::20/128
      [115/10] via fe80::9ca0:71ff:fe0f:b9ad, 00:01:24, POS0/6/0/0.1920
```

```
i L2 2001:10:0:25::/64
      [115/20] via fe80::201:97ff:fe5b:6c00, 00:01:35, GigabitEthernet0/1/0/0.195
i L2 2001:10:0:205::/64
      [115/20] via fe80::9ca0:71ff:fe0f:b9ad, 00:01:24, POS0/6/0/0.1920
      [115/20] via fe80::201:97ff:fe5b:6c00, 00:01:24, GigabitEthernet0/1/0/0.195
i L2 2001:10:0:220::/64
      [115/20] via fe80::9ca0:71ff:fe0f:b9ad, 00:01:24, POS0/6/0/0.1920
RP/0/3/CPU0:XR2#show route ipv6 unicast isis

Sun Jun 24 18:19:20.384 UTC

i L1 2001:10::2/128
      [115/10] via fe80::218:18ff:fece:eb00, 00:01:31, GigabitEthernet0/4/0/0.220
i L2 2001:10::5/128
      [115/10] via fe80::201:97ff:fe5b:6c00, 00:01:31, GigabitEthernet0/4/0/0.205
i L2 2001:10::19/128
      [115/10] via fe80::158a:b5ff:fe74:5710, 00:01:36, POS0/7/0/0.1920
i L1 2001:10:0:25::/64
      [115/20] via fe80::218:18ff:fece:eb00, 00:01:31, GigabitEthernet0/4/0/0.220
i L2 2001:10:0:195::/64
      [115/20] via fe80::158a:b5ff:fe74:5710, 00:01:31, POS0/7/0/0.1920
      [115/20] via fe80::201:97ff:fe5b:6c00, 00:01:31, GigabitEthernet0/4/0/0.205
```

Task 2.5 Solution

```
R5:
router isis 1000
 address-family ipv6
  redistribute isis level-2 into level-1 distribute-list IPV6_ISIS_ROUTE_LEAKING
 exit-address-family
!
ipv6 prefix-list IPV6_ISIS_ROUTE_LEAKING seq 5 permit 2001:10::19/128
ipv6 prefix-list IPV6_ISIS_ROUTE_LEAKING seq 10 permit 2001:10::20/128

XR2:
prefix-set IPV6_XR1_XR2_LOOPBACKS
  2001:10::19/128,
  2001:10::20/128
end-set
!
route-policy IPV6_ISIS_ROUTE_LEAKING
  if not destination in IPV6_XR1_XR2_LOOPBACKS then
    pass
```

```
  endif
end-policy
!
router isis 1000
 address-family ipv6 unicast
  propagate level 2 into level 1 route-policy IPV6_ISIS_ROUTE_LEAKING
 !
!
end
```

Task 2.5 Verification

```
R2#show ipv6 route isis
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I1  ::/0 [115/10]
     via FE80::201:97FF:FE5B:6C00, FastEthernet0/0.25
     via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220 IA
  2001:10::5/128 [115/20]
   via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220 IA
  2001:10::19/128 [115/20]
   via FE80::201:97FF:FE5B:6C00, FastEthernet0/0.25 IA
  2001:10::20/128 [115/20]
   via FE80::201:97FF:FE5B:6C00, FastEthernet0/0.25 IA
  2001:10:0:195::/64 [115/30]
   via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220 IA
  2001:10:0:205::/64 [115/20]
   via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220 IA
  2001:10:19:20::/64 [115/20]
     via FE80::2D0:79FF:FE03:F9F8, FastEthernet0/0.220
```

Task 2.6 Solution

```
R1:
ipv6 unicast-routing
!
```

```
interface Loopback0
 ip ospf 2000 area 0
 ipv6 ospf 2000 area 0
!
interface FastEthernet0/0.13
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
interface FastEthernet0/0.14
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
router ospf 2000
 passive-interface Loopback0
!
ipv6 router ospf 2000 passive-
 interface Loopback0

R3:
ipv6 unicast-routing
!
interface Loopback0
 ip ospf 2000 area 0
 ipv6 ospf 2000 area 0
!
interface FastEthernet0/0.13
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
interface FastEthernet0/0.34
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
router ospf 2000
 passive-interface Loopback0
!
ipv6 router ospf 2000
 passive-interface Loopback0
```

```
R4:
ipv6 unicast-routing
!
interface Loopback0
 ip ospf 2000 area 0
 ipv6 ospf 2000 area 0
!
 interface FastEthernet0/0.14
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
interface FastEthernet0/0.34
 ip ospf network point-to-point
 ip ospf 2000 area 0
 ipv6 ospf network point-to-point
 ipv6 ospf 2000 area 0
!
router ospf 2000
 passive-interface Loopback0
!
ipv6 router ospf 2000
 passive-interface Loopback0
```

Task 2.6 Verification

```
R4#show ip route ospf
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O        10.0.0.1/32 [110/2] via 10.0.14.1, 00:00:02, FastEthernet0/0.14
O        10.0.0.3/32 [110/2] via 10.0.34.3, 00:00:02, FastEthernet0/0.34
O        10.0.13.0/24 [110/2] via 10.0.34.3, 00:00:02, FastEthernet0/0.34
```

```
                      [110/2] via 10.0.14.1, 00:00:02, FastEthernet0/0.14
R4#show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:10::1/128 [110/1]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.14
O   2001:10::3/128 [110/1]
     via FE80::250:80FF:FE83:8600, FastEthernet0/0.34
O   2001:10:0:13::/64 [110/2]
     via FE80::250:80FF:FE83:8600, FastEthernet0/0.34
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.14
R4#show ip ospf neighbor

Neighbor ID      Pri   State          Dead Time   Address        Interface
10.0.0.3           0   FULL/ -        00:00:30    10.0.34.3
FastEthernet0/0.34
10.0.0.1           0   FULL/ -        00:00:31    10.0.14.1
FastEthernet0/0.14
R4#show ipv6 ospf neighbor



Neighbor ID      Pri   State          Dead Time   Interface ID   Interface
172.16.0.3         0   FULL/ -        00:00:36    8
FastEthernet0/0.34
172.16.0.1         0   FULL/ -        00:00:34    12
FastEthernet0/0.14
```

Task 2.7 Solution

```
R1:
router bgp 2000
 no bgp default ipv4-unicast
 neighbor 10.0.0.3 remote-as 2000
 neighbor 10.0.0.3 update-source Loopback0
 neighbor 10.0.0.4 remote-as 2000
 neighbor 10.0.0.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.0.0.3 activate
```

```
  neighbor 10.0.0.3 route-reflector-client
  neighbor 10.0.0.4 activate
  neighbor 10.0.0.4 route-reflector-client
 exit-address-family

R2:
router bgp 1000
 no bgp default ipv4-unicast
 neighbor 10.0.0.5 remote-as 1000
 neighbor 10.0.0.5 update-source Loopback0
 neighbor 10.0.0.19 remote-as 1000
 neighbor 10.0.0.19 update-source Loopback0
 neighbor 10.0.0.20 remote-as 1000
 neighbor 10.0.0.20 update-source Loopback0
 !
 address-family ipv4 neighbor 10.0.0.5 activate
  neighbor 10.0.0.5 route-reflector-client
  neighbor 10.0.0.19 activate
  neighbor 10.0.0.19 route-reflector-client
  neighbor 10.0.0.20 activate
  neighbor 10.0.0.20 route-reflector-client
 exit-address-family

R3:
router bgp 2000
 no bgp default ipv4-unicast
 neighbor 10.0.0.1 remote-as 2000
 neighbor 10.0.0.1 update-source Loopback0
 neighbor 10.0.35.5 remote-as 1000
 neighbor 10.0.193.19 remote-as 1000
 !
 address-family ipv4
  network 10.0.0.1 mask 255.255.255.255
  network 10.0.0.3 mask 255.255.255.255
  network 10.0.0.4 mask 255.255.255.255
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 next-hop-self
  neighbor 10.0.35.5 activate
  neighbor 10.0.193.19 activate
 exit-address-family

R4:
router bgp 2000
 no bgp default ipv4-unicast
 neighbor 10.0.0.1 remote-as 2000
 neighbor 10.0.0.1 update-source Loopback0
```

```
 !
 address-family ipv4
  neighbor 10.0.0.1 activate
 exit-address-family

R5:
router bgp 1000
 no bgp default ipv4-unicast
 neighbor 10.0.0.2 remote-as 1000
 neighbor 10.0.0.2 update-source Loopback0
 neighbor 10.0.35.3 remote-as 2000
 !
 address-family ipv4
  network 10.0.0.2 mask 255.255.255.255
  network 10.0.0.5 mask 255.255.255.255
  network 10.0.0.19 mask 255.255.255.255
  network 10.0.0.20 mask 255.255.255.255
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 next-hop-self
  neighbor 10.0.35.3 activate
 exit-address-family

XR1:
route-policy PASS
 pass
end-policy
!
router bgp 1000
 address-family ipv4 unicast
  network 10.0.0.2/32
  network 10.0.0.5/32
  network 10.0.0.19/32
  network 10.0.0.20/32
 !
 neighbor 10.0.0.2
  remote-as 1000
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
 !
 neighbor 10.0.193.3
  remote-as 2000
  address-family ipv4 unicast
   route-policy PASS out
   route-policy PASS in
```

```
XR2:
router bgp 1000
 address-family ipv4 unicast
 !
 neighbor 10.0.0.2
  remote-as 1000
  update-source Loopback0
  address-family ipv4 unicast
```

Task 2.7 Verification

```
R2#show bgp ipv4 unicast
BGP table version is 9, local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.0.0.1/32      10.0.0.19                2    100      0 2000 i
*>i                 10.0.0.5                 2    100      0 2000 i
r i10.0.0.2/32      10.0.0.19               20    100      0 i
r>i                 10.0.0.5                10    100      0 i
* i10.0.0.3/32      10.0.0.19                0    100      0 2000 i
*>i                 10.0.0.5                 0    100      0 2000 i
* i10.0.0.4/32      10.0.0.19                2    100      0 2000 i
*>i                 10.0.0.5                 2    100      0 2000 i
r i10.0.0.5/32      10.0.0.19               10    100      0 i
r>i                 10.0.0.5                 0    100      0 i
r>i10.0.0.19/32     10.0.0.19                0    100      0 i
r i                 10.0.0.5                10    100      0 i
r i10.0.0.20/32     10.0.0.19               10    100      0 i
r>i                 10.0.0.5                10    100      0 i

R2#tclsh
R2(tcl)#foreach X {
+>(tcl)#10.0.0.1
+>(tcl)#10.0.0.2
+>(tcl)#10.0.0.3
+>(tcl)#10.0.0.4
+>(tcl)#10.0.0.5
+>(tcl)#10.0.0.19
+>(tcl)#10.0.0.20                            +>(tcl)#} { ping $X source lo0 }
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.4, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.5, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.19, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.20, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 2.8 Solution

```
R1:
router bgp 2000
 address-family ipv4
  neighbor 10.0.0.3 send-community
  neighbor 10.0.0.4 send-community

R2:
router bgp 1000
 address-family ipv4
  neighbor 10.0.0.5 send-community
  neighbor 10.0.0.19 send-community
```

```
  neighbor 10.0.0.20 send-community

R3:
router bgp 2000 address-
 family ipv4
  neighbor 10.0.0.1 send-community
  neighbor 10.0.35.5 send-community
  neighbor 10.0.193.19 send-community
  neighbor 10.0.35.5 route-map RFC_1998 in
  neighbor 10.0.193.19 route-map RFC_1998 in
 exit-address-family
!
ip bgp-community new-format
!
ip community-list standard 2000:80 permit 2000:80
ip community-list standard 2000:90 permit 2000:90
ip community-list standard 2000:110 permit 2000:110
ip community-list standard 2000:120 permit 2000:120
!
route-map RFC_1998 permit 10
 match community 2000:80
 set local-preference 80
route-map RFC_1998 permit 20
 match community 2000:90
 set local-preference 90
route-map RFC_1998 permit 30
 match community 2000:110
 set local-preference 110
route-map RFC_1998 permit 40
 match community 2000:120
 set local-preference 120
route-map RFC_1998 permit 1000

R4:
router bgp 2000
 address-family ipv4
  neighbor 10.0.0.1 send-community

R5:
router bgp 1000
 address-family ipv4
  neighbor 10.0.35.3 route-map RFC_1998 in
  neighbor 10.0.0.2  send-community
  neighbor 10.0.35.3 send-community
 exit-address-family
!
```

```
ip bgp-community new-format
!
ip community-list standard 1000:80 permit 1000:80
ip community-list standard 1000:90 permit 1000:90
ip community-list standard 1000:110 permit 1000:110
ip community-list standard 1000:120 permit 1000:120
!
route-map RFC_1998 permit 10
 match community 1000:80
 set local-preference 80
route-map RFC_1998 permit 20
 match community 1000:90
 set local-preference 90
route-map RFC_1998 permit 30
 match community 1000:110
 set local-preference 110
route-map RFC_1998 permit 40
 match community 1000:120
 set local-preference 120
route-map RFC_1998 permit 1000

XR1:
policy-global
  myASN '1000'
end-global
!
route-policy RFC_1998
  if community matches-every ($myASN:80) then
    set local-preference 80
  endif
  if community matches-every ($myASN:90) then
    set local-preference 90
  endif
  if community matches-every ($myASN:110) then
    set local-preference 110
  endif
  if community matches-every ($myASN:120) then
    set local-preference 120
  endif
  pass end-
policy
!
router bgp 1000
 neighbor 10.0.193.3
  address-family ipv4 unicast
   send-community-ebgp
```

```
  route-policy RFC_1998 in
```

Task 2.9 Solution

```
R3:
router bgp 2000
 address-family ipv4
  neighbor 10.0.35.5 route-map TO_R5 out
  neighbor 10.0.193.19 route-map TO_XR1 out
 exit-address-family
!
ip prefix-list R1_LOOPBACK seq 5 permit 10.0.0.1/32
ip prefix-list R3_LOOPBACK seq 5 permit 10.0.0.3/32
ip prefix-list R4_LOOPBACK seq 5 permit 10.0.0.4/32
!
route-map TO R5 permit 10
 match ip address prefix-list R1 LOOPBACK
 set community 1000:110 route-
map TO_R5 permit 20
 match ip address prefix-list R3_LOOPBACK
 set community 1000:80
route-map TO_R5 permit 1000
!
route-map TO_XR1 permit 10
 match ip address prefix-list R4 LOOPBACK
 set community 1000:120
route-map TO XR1 permit 1000
```

Task 2.9 Verification

```
RP/0/0/CPU0:XR1#sh bgp ipv4 unicast 10.0.0.1/32
Sun Jun 24 19:49:23.874 UTC
BGP routing table entry for 10.0.0.1/32
Versions:
  Process           bRIB/RIB  SendTblVer
Speaker                   10          10
Last Modified: Jun 24 19:48:40.550 for 00:00:43
Paths: (2 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  2000
```

```
    10.0.0.5 (metric 10) from 10.0.0.2 (10.0.0.5)      Origin IGP, metric 2, localpref 110
, valid, internal, best Community: 1000:110
      Originator: 10.0.0.5, Cluster list: 10.0.0.2
  Path #2: Received by speaker 0
  2000
    10.0.193.3 from 10.0.193.3 (10.0.0.3)
      Origin IGP, metric 2, localpref 100, valid, external
```

R5#sh bgp ipv4 unicast 10.0.0.3/32

```
BGP routing table entry for 10.0.0.3/32, version 11
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     4
  2000
    10.0.0.19 (metric 10) from 10.0.0.2 (10.0.0.2)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 10.0.0.19, Cluster list: 10.0.0.2
  2000
    10.0.35.3 from 10.0.35.3 (10.0.0.3)      Origin IGP, metric 0, localpref 80
, valid, external ommunity: 1000:80
```

R5#sh bgp ipv4 unicast 10.0.0.4/32

```
BGP routing table entry for 10.0.0.4/32, version 12
Paths: (2 available, best #1, table default)
  Advertised to update-groups: 4
     2000
  10.0.0.19 (metric 10) from 10.0.0.2 (10.0.0.2)      Origin IGP, metric 2, localpref 120
, valid, internal, best Community: 1000:120

      Originator: 10.0.0.19, Cluster list: 10.0.0.2
  2000
    10.0.35.3 from 10.0.35.3 (10.0.0.3)
      Origin IGP, metric 2, localpref 100, valid, external
```

Task 2.10 Solution

```
R1:
router bgp 2000
 neighbor 2001:10::3 remote-as 2000
 neighbor 2001:10::3 update-source loopback0
 !
 address-family ipv6 unicast
  network 2001:10::1/128
  neighbor 2001:10::3 activate
 exit-address-family
```

```
R2:
router bgp 1000
 neighbor 2001:10::19 remote-as 1000
 neighbor 2001:10::19 update-source loopback0
 !
 address-family ipv6 unicast
  network 2001:10::2/128
  neighbor 2001:10::19 activate

R3:
router bgp 2000
 neighbor 2001:10::1 remote-as 2000
 neighbor 2001:10::1 update-source loopback0
 neighbor 2001:10::4 remote-as 2000
 neighbor 2001:10::4 update-source loopback0
 neighbor 2001:10:0:193::19 remote-as 1000
 neighbor 2001:10:0:35::5 remote-as 1000
 !
 address-family ipv6 unicast
  network 2001:10::3/128
  neighbor 2001:10::1 activate
  neighbor 2001:10::1 route-reflector-client
  neighbor 2001:10::1 next-hop-self
  neighbor 2001:10::4 activate
  neighbor 2001:10::4 route-reflector-client
  neighbor 2001:10::4 next-hop-self
  neighbor 2001:10:0:193::19 activate
  neighbor 2001:10:0:35::5 activate
 exit-address-family

R4:
router bgp 2000
 neighbor 2001:10::3 remote-as 2000
 neighbor 2001:10::3 update-source loopback0
 !
 address-family ipv6 unicast
  network 2001:10::4/128
  neighbor 2001:10::3 activate
 exit-address-family

R5:
router bgp 1000
 neighbor 2001:10::19 remote-as 1000
 neighbor 2001:10::19 update-source loopback0
 neighbor 2001:10:0:35::3 remote-as 2000
```

```
 !
 address-family ipv6 unicast
  network 2001:10::5/128
  neighbor 2001:10::19 activate
  neighbor 2001:10:0:35::3 activate

XR1:
router bgp 1000
 address-family ipv6 unicast
  network 2001:10::19/128
 !
 neighbor 2001:10::2
  remote-as 1000
  update-source loopback0
  address-family ipv6 unicast
   next-hop-self
   route-reflector-client
 !
 neighbor 2001:10::5
  remote-as 1000
  update-source loopback0
  address-family ipv6 unicast
   next-hop-self
   route-reflector-client
 !
 neighbor 2001:10::20
 remote-as 1000
 update-source loopback0
 address-family ipv6 unicast
  next-hop-self
  route-reflector-client
 !
 neighbor 2001:10:0:193::3
  remote-as 2000
  address-family ipv6 unicast
   route-policy PASS out
   route-policy PASS in

XR2:
router bgp 1000
 address-family ipv6 unicast
  network 2001:10::20/128
 !
 neighbor 2001:10::19
  remote-as 1000
  update-source Loopback0
```

```
  address-family ipv6 unicast
```

Task 2.10 Verification

```
R2#show bgp ipv6 unicast
BGP table version is 8, local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i2001:10::1/128   2001:10::19                   100      0 2000 i
*> 2001:10::2/128   ::                       0         32768 i
*>i2001:10::3/128   2001:10::19              0    100      0 2000 i
*>i2001:10::4/128   2001:10::19                   100      0 2000 i
*>i2001:10::5/128   2001:10::5               0    100      0 i
*>i2001:10::19/128  2001:10::19              0    100      0 i
*>i2001:10::20/128  2001:10::20              0    100      0 i

R2#tclsh
R2(tcl)#foreach X {
+>(tcl)#2001:10::1
+>(tcl)#2001:10::2
+>(tcl)#2001:10::3
+>(tcl)#2001:10::4
+>(tcl)#2001:10::5
+>(tcl)#2001:10::19
+>(tcl)#2001:10::20+>(tcl)#} { ping $X source lo0 }



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::1, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::2, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::3, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::4, timeout is 2 seconds:
```

```
Packet sent with a source address of 2001:10::2 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::5, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/12 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::19, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10::20, timeout is 2 seconds:
Packet sent with a source address of 2001:10::2!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/20 ms
```

Task 2.11 Solution

```
R5:
router bgp 1000
 address-family ipv6
  neighbor 2001:10:0:35::3 route-map IPV6_TO_R3 out
!
ipv6 prefix-list R2_R5_IPV6_LOOPBACKS seq 5 permit 2001:10::2/128
ipv6 prefix-list R2_R5_IPV6_LOOPBACKS seq 10 permit 2001:10::5/128
!
route-map IPV6_TO_R3 permit 10
 match ipv6 address prefix-list R2_R5_IPV6_LOOPBACKS
 set metric 20
!
route-map IPV6_TO_R3 permit 20
 set metric 10

XR1:
prefix-set XR1_XR2_IPV6_LOOPBACKS
 2001:10::19/128,
 2001:10::20/128
end-set
!
route-policy IPV6_TO_R3
  if destination in XR1_XR2_IPV6_LOOPBACKS then
    set med 20
  else
```

```
    set med 10 endif
end-policy
!
router bgp 1000
 address-family ipv6 unicast
 !
 neighbor 2001:10:0:193::3
  address-family ipv6 unicast
   route-policy IPV6_TO_R3 out
  !
 !
!
```

Task 2.11 Verification

```
R3#show bgp ipv6 unicast 2001:10::2/128
BGP routing table entry for 2001:10::2/128, version 11
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1          2
  1000
    2001:10:0:35::5 (FE80::201:97FF:FE5B:6C00) from 2001:10:0:35::5 (10.0.0.5)      Origin IGP,
metric 20
, localpref 100, valid, external
  1000
    2001:10:0:193::19 (FE80::2D0:79FF:FE03:F87E) from 2001:10:0:193::19 (10.0.0.19)      Origin IGP,
metric 10
, localpref 100, valid, external, best
R3#show bgp ipv6 unicast 2001:10::19/128
BGP routing table entry for 2001:10::19/128, version 10
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     1          2
  1000
    2001:10:0:35::5 (FE80::201:97FF:FE5B:6C00) from 2001:10:0:35::5 (10.0.0.5)      Origin IGP,
metric 10
, localpref 100, valid, external, best
  1000
    2001:10:0:193::19 (FE80::2D0:79FF:FE03:F87E) from 2001:10:0:193::19 (10.0.0.19)      Origin IGP,
metric 20
, localpref 100, valid, external
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solution 3.1 (pending update)

Task 3.1 Solution

```
R1:
router ospf 2000
 mpls ldp autoconfig

R2:
router isis 1000
 mpls ldp autoconfig

R3:
router ospf 2000
 mpls ldp autoconfig

R4:
router ospf 2000
 mpls ldp autoconfig

R5:
router isis 1000
 mpls ldp autoconfig

XR1:
router isis 1000
 address-family ipv4 unicast
  mpls ldp auto-config
 !
!
mpls ldp

XR2:
router isis 1000
 address-family ipv4 unicast
```

```
  mpls ldp auto-config
 !
!
mpls ldp
```

Task 3.1 Verification

```
RP/0/3/CPU0:XR2#show mpls ldp neighbor brief
Sun Jun 24 20:15:44.101 UTC

Peer                GR  NSR  Up Time     Discovery  Address  IPv4 Label
-----------------  --  ---  ----------  ---------  -------  ----------
10.0.0.2:0         N    N    00:00:10           1        3          10
10.0.0.5:0         N    N    00:00:10           1        5          10
10.0.0.19:0        N    N    00:00:08           1        4          10
RP/0/3/CPU0:XR2#show mpls forwarding
Sun Jun 24 20:15:51.000 UTC
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16000  Pop         10.0.0.19/32       PO0/7/0/0.1920 10.19.20.19   0
16001  Pop         10.0.0.5/32        Gi0/4/0/0.205 10.0.205.5     63
16002  Pop         10.0.195.0/24      Gi0/4/0/0.205 10.0.205.5     0
       Pop         10.0.195.0/24      PO0/7/0/0.1920 10.19.20.19   0
16003  Pop         10.0.0.2/32        Gi0/4/0/0.220 10.0.220.2     44
16004  Pop         10.0.25.0/24       Gi0/4/0/0.220 10.0.220.2     0
R3#show mpls ldp neighbor
    Peer LDP Ident: 10.0.0.1:0; Local LDP Ident 10.0.0.3:0 TCP connection: 10.0.0.1.646 - 10.0.0.3.28843
        State: Oper; Msgs sent/rcvd: 13/11; Downstream
        Up time: 00:01:48
        LDP discovery sources:
          FastEthernet0/0.13, Src IP addr: 10.0.13.1
        Addresses bound to peer LDP Ident:
          10.0.13.1            10.0.14.1  10.0.0.1
    Peer LDP Ident: 10.0.0.4:0; Local LDP Ident 10.0.0.3:0
        TCP connection: 10.0.0.4.55920 - 10.0.0.3.646
        State: Oper; Msgs sent/rcvd: 13/10; Downstream
        Up time: 00:01:45
        LDP discovery sources:
          FastEthernet0/0.34, Src IP addr: 10.0.34.4
        Addresses bound to peer LDP Ident:
          10.0.14.4       10.0.34.4       10.0.0.4
R3#show mpls forwarding-table
```

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	Pop Label	10.0.0.1/32	0	Fa0/0.13	10.0.13.1
17	Pop Label	10.0.0.4/32	0	Fa0/0.34	10.0.34.4
18	Pop Label	10.0.14.0/24	0	Fa0/0.13	10.0.13.1
	Pop Label	10.0.14.0/24	0	Fa0/0.34	10.0.34.4

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solutions 4.1 - 4.10 (pending update)

Task 4.1 Solution

```
R1:
vrf definition FOO
 address-family ipv4
  route-target export 2000:1
  route-target import 1000:1
  route-target import 2000:1
!
router bgp 2000
 address-family vpnv4
  neighbor 10.0.0.4 activate
 exit-address-family
 !
 address-family ipv4 vrf FOO
  network 172.16.0.1 mask 255.255.255.255
 exit-address-family

R2:
vrf definition FOO address-
 family ipv4
```

```
  route-target export 1000:1
  route-target import 1000:1
  route-target import 2000:1
!
router bgp 1000
 address-family vpnv4
  neighbor 10.0.0.20 activate
 exit-address-family
 !
 address-family ipv4 vrf FOO
  network 172.16.0.2 mask 255.255.255.255
 exit-address-family

R3:
vrf definition FOO
 address-family ipv4
  route-target export 2000:1
  route-target import 1000:1
  route-target import 2000:1
!
router bgp 2000
 neighbor 10.0.0.4 remote-as 2000
 neighbor 10.0.0.4 update-source Loopback0
 !
 address-family vpnv4
  neighbor 10.0.0.4 activate
 exit-address-family
 !
 address-family ipv4
  neighbor 10.0.35.5 send-label
  neighbor 10.0.193.19 send-label
 exit-address-family
 !
 address-family ipv4 vrf FOO
  network 172.16.0.3 mask 255.255.255.255
 exit-address-family
!
! NOTE: Labels are stripped from route-map
! unless "set label" is used
!
route-map TO_R5 permit 10
 set mpls-label
route-map TO_R5 permit 20
 set mpls-label
route-map TO_R5 permit 1000
 set mpls-label
```

```
route-map TO_XR1 permit 10
 set mpls-label
route-map TO_XR1 permit 1000
 set mpls-label
!
! Redistribute remote loopbacks so they get LDP labels
!
router ospf 2000
 redistribute bgp 2000 subnets route-map BGP_TO_IGP
!
ip prefix-list REMOTE_LSP_DESTINATIONS seq 5 permit 10.0.0.2/32
ip prefix-list REMOTE_LSP_DESTINATIONS seq 10 permit 10.0.0.5/32
ip prefix-list REMOTE_LSP_DESTINATIONS seq 15 permit 10.0.0.19/32
ip prefix-list REMOTE_LSP_DESTINATIONS seq 20 permit 10.0.0.20/32
!
route-map BGP_TO_IGP permit 10
 match ip address prefix-list REMOTE_LSP_DESTINATIONS

R4:
vrf definition FOO
 address-family ipv4
  route-target export 2000:1
  route-target import 1000:1
  route-target import 2000:1
!
router bgp 2000
 neighbor 10.0.0.3 remote-as 2000
 neighbor 10.0.0.3 update-source Loopback0
 neighbor 10.0.0.20 remote-as 1000
 neighbor 10.0.0.20 update-source Loopback0
 neighbor 10.0.0.20 ebgp-multihop
 !
 address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 route-reflector-client
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 route-reflector-client
  neighbor 10.0.0.20 activate
  neighbor 10.0.0.20 next-hop-unchanged
 exit-address-family
 !
 address-family ipv4 vrf FOO
  network 172.16.0.4 mask 255.255.255.255
 exit-address-family

R5:
```

```
vrf definition FOO
 address-family ipv4
  route-target export 1000:1
  route-target import 1000:1
  route-target import 2000:1
!
router bgp 1000
 neighbor 10.0.0.20 remote-as 1000
 neighbor 10.0.0.20 update-source loopback0
 !
 address-family ipv4
  neighbor 10.0.35.3 send-label
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.20 activate
 exit-address-family
 !
 address-family ipv4 vrf FOO
  network 172.16.0.5 mask 255.255.255.255
 exit-address-family
!
router isis 1000
 redistribute bgp 1000 level-1 route-map BGP_TO_IGP
!
ip prefix-list REMOTE_LSP_DESTINATIONS seq 5 permit 10.0.0.1/32
ip prefix-list REMOTE_LSP_DESTINATIONS seq 10 permit 10.0.0.3/32
ip prefix-list REMOTE_LSP_DESTINATIONS seq 15 permit 10.0.0.4/32
!
route-map BGP_TO_IGP permit 10
 match ip address prefix-list REMOTE_LSP_DESTINATIONS

XR1:
vrf FOO
 address-family ipv4 unicast
  import route-target
   1000:1
   2000:1
  !
  export route-target
   1000:1
  !
 !
!
router bgp 1000
 address-family vpnv4 unicast
```

```
 !
 address-family ipv4 unicast
  allocate-label all
 !
 neighbor 10.0.193.3
  no address-family ipv4 unicast
  address-family ipv4 labeled-unicast
   send-community-ebgp
   route-policy RFC_1998 in
   route-policy PASS out
 !
 neighbor 10.0.0.20
  remote-as 1000
  update-source loopback0
  address-family vpnv4 unicast
!
vrf FOO
  rd 10.0.0.19:1
  address-family ipv4 unicast
   network 172.16.0.19/32
!
prefix-set REMOTE_LSP_DESTINATIONS
  10.0.0.1/32,
  10.0.0.3/32,
  10.0.0.4/32
end-set
!
route-policy BGP_TO_IGP
  if destination in REMOTE_LSP_DESTINATIONS then
    pass
  endif
end-policy
!
router isis 1000
 address-family ipv4 unicast
  redistribute bgp 1000 route-policy BGP_TO_IGP
 !
!
router static
 address-family ipv4 unicast
  10.0.193.3/32 GigabitEthernet0/1/0/0.193

XR2:
vrf FOO
 address-family ipv4 unicast
  import route-target
```

```
   1000:1
   2000:1
  !
  export route-target
   1000:1
  !
 !
!
route-policy PASS
  pass end-
policy
!
router bgp 1000
 address-family vpnv4 unicast
 !
 neighbor 10.0.0.2
  address-family vpnv4 unicast
   route-reflector-client
  !
 neighbor 10.0.0.5
  remote-as 1000
  update-source loopback0
  address-family vpnv4 unicast
   route-reflector-client
  !
 neighbor 10.0.0.19
  remote-as 1000
  update-source loopback0
  address-family vpnv4 unicast
   route-reflector-client
  !
 neighbor 10.0.0.4
  remote-as 2000
  ebgp-multihop
  update-source loopback0
  address-family vpnv4 unicast
   next-hop-unchanged
   route-policy PASS in
   route-policy PASS out
!
vrf FOO
  rd 10.0.0.20:1
  address-family ipv4 unicast
```

```
   network 172.16.0.20/32
```

Task 4.1 Verification

```
R1#sh bgp vpnv4 unicast vrf FOO
BGP table version is 14, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.0.0.1:1 (default for vrf FOO)
*> 172.16.0.1/32    0.0.0.0                  0         32768 i
*>i172.16.0.2/32    10.0.0.2                 0    100      0 1000 i
*>i172.16.0.3/32    10.0.0.3                 0    100      0 i
*>i172.16.0.4/32    10.0.0.4                 0    100      0 i
*>i172.16.0.5/32    10.0.0.5                 0    100      0 1000 i
*>i172.16.0.19/32   10.0.0.19                0    100      0 1000 i
*>i172.16.0.20/32   10.0.0.20                0    100      0 1000 i
RP/0/3/CPU0:XR2#show bgp vpnv4 unicast vrf FOO
Sun Jun 24 20:21:18.233 UTC
BGP router identifier 10.0.0.20, local AS number 1000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0
BGP main routing table version 14
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.0.0.20:1 (default for vrf FOO)
*> 172.16.0.1/32      10.0.0.1                              0 2000 i
*>i172.16.0.2/32      10.0.0.2                 0    100      0 i
*> 172.16.0.3/32      10.0.0.3                              0 2000 i
*> 172.16.0.4/32      10.0.0.4                 0             0 2000 i
*>i172.16.0.5/32      10.0.0.5                 0    100      0 i
*>i172.16.0.19/32     10.0.0.19                0    100      0 i
*> 172.16.0.20/32     0.0.0.0                  0         32768 i

Processed 7 prefixes, 7 paths
R1#traceroute vrf FOO 172.16.0.2

Type escape sequence to abort.
```

```
Tracing the route to 172.16.0.2
 1 10.0.13.3 [MPLS: Labels 20/22 Exp 0] 0 msec 4 msec 0 msec
 2 10.0.35.5 [MPLS: Labels 16/22 Exp 0] 0 msec 0 msec 0 msec
  3 172.16.0.2 4 msec * 0 msec

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0.35R3(config-subif)#shutdown
R3(config-subif)#
%BGP-5-ADJCHANGE: neighbor 10.0.35.5 Down Interface flap
%BGP_SESSION-5-ADJCHANGE: neighbor 10.0.35.5 IPv4 Unicast topology base removed
from session    Interface flap
%BGP-5-ADJCHANGE: neighbor 2001:10:0:35::5 Down Interface flap
%BGP_SESSION-5-ADJCHANGE: neighbor 2001:10:0:35::5 IPv6 Unicast topology base
removed from session  Interface flap
R1#traceroute vrf FOO 172.16.0.2

Type escape sequence to abort.
Tracing the route to 172.16.0.2
 1 10.0.13.3 [MPLS: Labels 20/22 Exp 0] 0 msec 0 msec 4 msec
 2 10.0.193.19 [MPLS: Labels 16005/22 Exp 0] 0 msec 4 msec 4 msec

  3 10.19.20.20 [MPLS: Labels 16003/22 Exp 0] 4 msec 0 msec 0 msec
  4 172.16.0.2 4 msec * 0 msec
```

Task 4.2 Solution

```
R1:
interface FastEthernet0/0.16
 ip router isis 3000
!
router isis 3000
 vrf FOO
 net 00.0000.0000.0001.00
 redistribute bgp 2000
 !
 ! Prevent route feedback of PE to CE redistribution
 !
 distance 201 ip
 !
 ! Prefer to route via CE link to reach CE's Loopback
 !
 distance 115 0.0.0.0 255.255.255.255 1
```

```
!
access-list 1 permit 172.16.0.6
!
router bgp 2000
 address-family ipv4 vrf FOO
  network 172.16.0.1 mask 255.255.255.255
  redistribute isis 3000 level-1-2
 exit-address-family

R4:
interface FastEthernet0/0.46
 ip router isis 3000
!
router isis 3000
 vrf FOO
 net 00.0000.0000.0004.00
 redistribute bgp 2000
 !
 ! Prevent route feedback of PE to CE redistribution
 !
 distance 201 ip
 !
 ! Prefer to route via CE link to reach CE's Loopback
 !
 distance 115 0.0.0.0 255.255.255.255 1
!
access-list 1 permit 172.16.0.6
!
router bgp 2000
 address-family ipv4 vrf FOO
  network 172.16.0.4 mask 255.255.255.255
  redistribute isis 3000 level-1-2
 exit-address-family

R6:
interface FastEthernet0/0.16
 ip router isis 3000
!
interface FastEthernet0/0.46
 ip router isis 3000
!
router isis 3000
 net 00.0000.0000.0006.00
```

```
 passive-interface Loopback0
```

Task 4.2 Verification

```
R6#show ip route isis
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
i L2     172.16.0.1/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                       [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.2/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                       [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.3/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                       [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.4/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                       [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.5/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                       [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.19/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                        [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16
i L2     172.16.0.20/32 [115/10] via 172.16.46.4, 00:00:00, FastEthernet0/0.46
                        [115/10] via 172.16.16.1, 00:00:00, FastEthernet0/0.16



R6#tclsh
R6(tcl)#foreach X {
+>(tcl)#172.16.0.1
+>(tcl)#172.16.0.2
+>(tcl)#172.16.0.3
+>(tcl)#172.16.0.4
+>(tcl)#172.16.0.5
+>(tcl)#172.16.0.19
+>(tcl)#172.16.0.20+>(tcl)#} { ping $X}

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.4, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.5, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.19, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.20, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R6(tcl)#
R1#show ip route vrf FOO

Routing Table: FOO
Codes: L - local, 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, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 11 subnets, 2 masks
C        172.16.0.1/32 is directly connected, Loopback1
B        172.16.0.2/32 [200/0] via 10.0.0.2, 00:11:28
B        172.16.0.3/32 [200/0] via 10.0.0.3, 00:13:22B        172.16.0.4/32 [200/0]
 via 10.0.0.4, 00:13:22
B        172.16.0.5/32 [200/0] via 10.0.0.5, 00:11:28i L1     172.16.0.6/32 [115/10]
 via 172.16.16.6, 00:01:19, FastEthernet0/0.16
B        172.16.0.19/32 [200/0] via 10.0.0.19, 00:10:58
B        172.16.0.20/32 [200/0] via 10.0.0.20, 00:11:28
C        172.16.16.0/24 is directly connected, FastEthernet0/0.16
```

```
L        172.16.16.1/32 is directly connected, FastEthernet0/0.16
i L1     172.16.46.0/24 [201/20] via 172.16.16.6, 00:01:19, FastEthernet0/0.16
R1#traceroute vrf FOO 172.16.0.4

Type escape sequence to abort.
Tracing the route to 172.16.0.4
 1 172.16.0.4 4 msec * 0 msec
R1#traceroute vrf FOO 172.16.0.6

Type escape sequence to abort.
Tracing the route to 172.16.0.6
 1 172.16.16.6 4 msec * 0 msec
```

Task 4.3 Solution

```
R7:
router bgp 3000
 no bgp default ipv4-unicast
 neighbor 172.16.0.8 remote-as 3000
 neighbor 172.16.0.8 update-source loopback0
 neighbor 172.16.207.20 remote-as 1000
 !
 address-family ipv4
  network 172.16.78.0 mask 255.255.255.0
  network 172.16.207.0 mask 255.255.255.0
  network 172.16.0.7 mask 255.255.255.255
  neighbor 172.16.0.8 activate
  neighbor 172.16.207.20 activate

R8:
router bgp 3000
 neighbor 172.16.0.7 remote-as 3000
 neighbor 172.16.0.7 update-source loopback0
 neighbor 172.16.208.20 remote-as 1000
 !
 address-family ipv4
  neighbor 172.16.0.7 activate
  neighbor 172.16.208.20 activate
  network 172.16.78.0 mask 255.255.255.0
  network 172.16.208.0 mask 255.255.255.0
  network 172.16.0.8 mask 255.255.255.255
```

```
XR2:
router bgp 1000
 vrf FOO
  neighbor 172.16.207.7
   remote-as 3000
   address-family ipv4 unicast
    route-policy PASS out
    route-policy PASS in
  !
  neighbor 172.16.208.8
   remote-as 3000
   address-family ipv4 unicast
    route-policy PASS out
    route-policy PASS in
```

Task 4.3 Verification

```
R7#show ip bgp
BGP table version is 18, local router ID is 172.16.0.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.1/32    172.16.207.20                          0 1000 2000 i
* i                 172.16.208.20            0    100      0 1000 2000 i
*> 172.16.0.2/32    172.16.207.20                          0 1000 i
* i                 172.16.208.20            0    100      0 1000 i
*> 172.16.0.3/32    172.16.207.20                          0 1000 2000 i
* i                 172.16.208.20            0    100      0 1000 2000 i
*> 172.16.0.4/32    172.16.207.20                          0 1000 2000 i
* i                 172.16.208.20            0    100      0 1000 2000 i
*> 172.16.0.5/32    172.16.207.20                          0 1000 i
* i                 172.16.208.20            0    100      0 1000 i
*> 172.16.0.6/32    172.16.207.20                          0 1000 2000 ?
* i                 172.16.208.20            0    100      0 1000 2000 ?
*>  172.16.0.7/32   0.0.0.0                  0         32768 i
r>i172.16.0.8/32    172.16.0.8               0    100      0 i
*> 172.16.0.19/32   172.16.207.20                          0 1000 i
* i                 172.16.208.20            0    100      0 1000 i
*> 172.16.0.20/32   172.16.207.20            0             0 1000 i
   Network          Next Hop            Metric LocPrf Weight Path
* i                 172.16.208.20            0    100      0 1000 i
*> 172.16.16.0/24   172.16.207.20                          0 1000 2000 ?
```

```
* i                 172.16.208.20           0    100      0 1000 2000 ?
*> 172.16.46.0/24   172.16.207.20                           0 1000 2000 ?
* i                 172.16.208.20           0    100      0 1000 2000 ?
* i172.16.78.0/24   172.16.0.8              0    100      0 i
*>                  0.0.0.0                 0         32768 i
*> 172.16.207.0/24  0.0.0.0                 0         32768 i
r>i172.16.208.0/24  172.16.0.8              0    100      0 i
R7#ping 172.16.0.6



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 4.4 Solution

```
R1:
interface FastEthernet0/0.16
 mpls ip

R4:
interface FastEthernet0/0.46
 mpls ip

R6:
vrf definition BAR
 address-family ipv4
  route-target both 3000:1
!
router bgp 3000
 no bgp default ipv4-unicast
  neighbor 172.16.0.7 remote-as 3000
  neighbor 172.16.0.7 update-source loopback0
  neighbor 172.16.0.8 remote-as 3000
  neighbor 172.16.0.8 update-source loopback0
!
address-family vpnv4
 neighbor 172.16.0.7 activate
 neighbor 172.16.0.8 activate
!
address-family ipv4 vrf BAR
 network 192.168.0.6 mask 255.255.255.255
```

```
!
interface FastEthernet0/0.16
 mpls ip
!
interface FastEthernet0/0.46
 mpls ip

R7:
interface FastEthernet0/0.78
 mpls ip
!
ip vrf BAR
 route-target both 3000:1
!
router bgp 3000
 no bgp default ipv4-unicast
 neighbor 172.16.0.6 remote-as 3000
 neighbor 172.16.0.6 update-source loopback0
 !
 address-family ipv4 unicast
  neighbor 172.16.207.20 send-label
  neighbor 172.16.0.8 send-label
 !
 address-family vpnv4
  neighbor 172.16.0.6 activate
  neighbor 172.16.0.8 activate
 !
 address-family ipv4 vrf BAR
  network 192.168.0.7 mask 255.255.255.255

R8:
interface FastEthernet0/0.78
 mpls ip
!
ip vrf BAR
 route-target both 3000:1
!
router bgp 3000
 no bgp default ipv4-unicast
 neighbor 172.16.0.6 remote-as 3000
 neighbor 172.16.0.6 update-source loopback0
 !
 address-family ipv4 unicast
  neighbor 172.16.0.7 send-label
  neighbor 172.16.208.20 send-label
 !
```

```
 address-family vpnv4
  neighbor 172.16.0.6 activate
  neighbor 172.16.0.7 activate
 !
 address-family ipv4 vrf BAR
  network 192.168.0.8 mask 255.255.255.255

XR2:
router bgp 1000
 vrf FOO
  address-family ipv4 unicast
   allocate-label all
  !
  neighbor 172.16.207.7
   no address-family ipv4 unicast
   address-family ipv4 labeled-unicast
    route-policy PASS in
    route-policy PASS out
   !
  !
  neighbor 172.16.208.8
   no address-family ipv4 unicast
   address-family ipv4 labeled-unicast route-
    policy PASS in
    route-policy PASS out
!
router static
 vrf FOO
   address-family ipv4 unicast
    172.16.207.7/32 GigabitEthernet0/4/0/0.207
    172.16.208.8/32 GigabitEthernet0/4/0/0.208
```

Task 4.4 Verification

```
RP/0/3/CPU0:XR2#sh bgp vrf FOO ipv4 labeled-unicast summary
Sun Jun 24 22:10:43.866 UTC
BGP VRF FOO, state: Active
BGP Route Distinguisher: 10.0.0.20:1
VRF ID: 0x60000001
BGP router identifier 10.0.0.20, local AS number 1000
BGP table state: Active
Table ID: 0xe0000001
BGP main routing table version 110
```

```
<snip>

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
172.16.207.7      0  3000      65      81      110    0    0 00:00:57          5
172.16.208.8      0  3000      70      82      110    0    0 00:00:51          5
```

RP/0/3/CPU0:XR2#sh bgp vrf FOO ipv4 labeled-unicast

```
Sun Jun 24 22:10:47.081 UTC
BGP VRF FOO, state: Active
BGP Route Distinguisher: 10.0.0.20:1
VRF ID: 0x60000001
BGP router identifier 10.0.0.20, local AS number 1000
BGP table state: Active
Table ID: 0xe0000001
BGP main routing table version 110

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.0.0.20:1 (default for vrf FOO)
*> 172.16.0.1/32      10.0.0.1                               0 2000 i
*>i172.16.0.2/32      10.0.0.2                 0    100      0 i
*> 172.16.0.3/32      10.0.0.3                               0 2000 i
*> 172.16.0.4/32      10.0.0.4                 0             0 2000 i
*>i172.16.0.5/32      10.0.0.5                 0    100      0 i
*> 172.16.0.6/32      10.0.0.1                               0 2000 ?
*                     10.0.0.4                10             0 2000 ?
*> 172.16.0.7/32      172.16.207.7             0             0 3000 i
*                     172.16.208.8                           0 3000 i
*> 172.16.0.8/32      172.16.207.7                           0 3000 i
*                     172.16.208.8             0             0 3000 i
*>i172.16.0.19/32     10.0.0.19                0    100      0 i
*> 172.16.0.20/32     0.0.0.0                  0         32768 i
*> 172.16.16.0/24     10.0.0.4                20             0 2000 ?
*> 172.16.46.0/24     10.0.0.1                               0 2000 ?
*> 172.16.78.0/24     172.16.207.7             0             0 3000 i
*                     172.16.208.8             0             0 3000 i
*> 172.16.207.0/24    172.16.207.7             0             0 3000 i
*                     172.16.208.8                           0 3000 i
*> 172.16.208.0/24    172.16.207.7                           0 3000 i
*                     172.16.208.8             0             0 3000 i

Processed 15 prefixes, 21 paths
```

R6#show bgp vpnv4 unicast vrf BAR

```
BGP table version is 6, local router ID is 172.16.0.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 172.16.0.6:1 (default for vrf BAR)
*> 192.168.0.6/32   0.0.0.0                  0         32768 i
*>i192.168.0.7/32   172.16.0.7               0    100      0 i
*>i192.168.0.8/32   172.16.0.8               0    100      0 i
R6#ping vrf BAR 192.168.0.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R6#ping vrf BAR 192.168.0.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R6#traceroute vrf BAR 192.168.0.7

Type escape sequence to abort.
Tracing the route to 192.168.0.7

1 172.16.46.4 [MPLS: Labels 31/18 Exp 0] 0 msec
  172.16.16.1 [MPLS: Labels 31/18 Exp 0] 4 msec
  172.16.46.4 [MPLS: Labels 31/18 Exp 0] 4 msec 2 10.0.13.3 [MPLS: Labels 22/16009/18
 Exp 0] 0 msec   10.0.34.3 [MPLS: Labels 22/16009/18
 Exp 0] 4 msec   10.0.13.3 [MPLS: Labels 22/16009/18
 Exp 0] 4 msec 3 10.0.35.5 [MPLS: Labels 18/16009/18
 Exp 0] 0 msec 4 msec 4 msec
4 10.0.205.20 [MPLS: Labels 16009/18 Exp 0] 4 msec 4 msec 4 msec
5 192.168.0.7 0 msec *  0 msec
```

Task 4.5 Solution

```
R6:
router ospf 100 vrf BAR
 redistribute bgp 3000 subnets
 network 192.168.0.0 0.0.255.255 area 106
!
router bgp 3000
```

```
 address-family ipv4 vrf BAR
  redistribute ospf 100 vrf BAR
 exit-address-family

R7:
router ospf 100 vrf BAR
 area 79 virtual-link 192.168.0.9
 redistribute bgp 3000 subnets
 network 192.168.79.0 0.0.0.255 area 79
!
router bgp 3000
 address-family ipv4 vrf BAR
  redistribute ospf 100 vrf BAR
 exit-address-family

R8:
router ospf 100 vrf BAR
 area 89 virtual-link 192.168.0.9
 redistribute bgp 3000 subnets
 network 192.168.89.0 0.0.0.255 area 89
!
router bgp 3000
 address-family ipv4 vrf BAR
  redistribute ospf 100 vrf BAR
 exit-address-family

SW1:
router ospf 100 vrf BAR
 capability vrf-lite
 area 79 virtual-link 192.168.0.7
 area 89 virtual-link 192.168.0.8
```

Task 4.5 Verification

```
SW1#show ip route vrf BAR

Routing Table: BAR
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

O IA 192.168.106.0/24 [110/2] via 192.168.89.8, 00:00:14, Vlan89
                      [110/2] via 192.168.79.7, 00:00:14, Vlan79
C    192.168.89.0/24 is directly connected, Vlan89
C    192.168.79.0/24 is directly connected, Vlan79
     192.168.0.0/32 is subnetted, 5 subnets
O E2    192.168.0.8 [110/1] via 192.168.89.8, 00:00:04, Vlan89
                    [110/1] via 192.168.79.7, 00:00:04, Vlan79
C       192.168.0.9 is directly connected, Loopback1
O IA    192.168.0.10 [110/3] via 192.168.89.8, 00:00:14, Vlan89
                     [110/3] via 192.168.79.7, 00:00:14, Vlan79
O E2    192.168.0.6 [110/1] via 192.168.89.8, 00:00:04, Vlan89
                    [110/1] via 192.168.79.7, 00:00:04, Vlan79
O E2    192.168.0.7 [110/1] via 192.168.89.8, 00:00:06, Vlan89
                    [110/1] via 192.168.79.7, 00:00:06, Vlan79
SW1#traceroute vrf BAR 192.168.0.10

Type escape sequence to abort.
Tracing the route to 192.168.0.10
   1 192.168.79.7
 0 msec 192.168.89.8
 8 msec
     192.168.79.7 0 msec
   2 172.16.208.20 0 msec
     172.16.207.20 9 msec
     172.16.208.20 8 msec
   3 10.0.220.2 0 msec 8 msec 0 msec
   4 10.0.25.5 9 msec 0 msec 8 msec
   5 10.0.35.3 0 msec 9 msec 0 msec
   6 10.0.13.1 0 msec 8 msec 0 msec
   7 192.168.106.6 9 msec 0 msec 8 msec
   8 192.168.106.10 0 msec *  9 msec
```

Task 4.6 Solution

```
XR2:
router bgp 1000
 vrf FOO
  neighbor 172.16.207.7
   timers 1 3
  !
```

```
 neighbor 172.16.208.8
  timers 1 3
```

Task 4.6 Verification

```
RP/0/3/CPU0:XR2#show bgp vrf FOO ipv4 labeled-unicast neighbors | in "neighbor is|Hold"
Sun Jun 24 22:23:16.770 UTC
BGP neighbor is 172.16.207.7, vrf FOO  Hold time is 180, keepalive interval is 60 seconds
BGP neighbor is 172.16.208.8, vrf FOO  Hold time is 180, keepalive interval is 60 seconds
RP/0/3/CPU0:XR2#clear bgp vrf FOO *
Sun Jun 24 22:26:09.083 UTC
RP/0/3/CPU0:Jun 24 22:26:09.195 : bgp[139]: %ROUTING-BGP-5-ADJCHANGE : neighbor
172.16.207.7 Down - User clear requested (CEASE notification sent - administrative
reset) (VRF: FOO)
RP/0/3/CPU0:Jun 24 22:26:09.199 : bgp[139]: %ROUTING-BGP-5-ADJCHANGE : neighbor
172.16.208.8 Down - User clear requested (CEASE notification sent - administrative
reset) (VRF: FOO)
RP/0/3/CPU0:XR2#RP/0/3/CPU0:Jun 24 22:26:10.018 : bgp[139]: %ROUTING-BGP-5-
ADJCHANGE : neighbor 172.16.207.7 Up (VRF: FOO)
RP/0/3/CPU0:Jun 24 22:26:10.260 : bgp[139]: %ROUTING-BGP-5-ADJCHANGE : neighbor
172.16.208.8 Up (VRF: FOO)
RP/0/3/CPU0:XR2#show bgp vrf FOO ipv4 labeled-unicast neighbors | in ""neighbor is|Hold"
Sun Jun 24 22:26:18.009 UTC
BGP neighbor is 172.16.207.7, vrf FOO  Hold time is 3, keepalive interval is 1 seconds
BGP neighbor is 172.16.208.8, vrf FOO  Hold time is 3, keepalive interval is 1 seconds
```

Task 4.7 Solution

```
R3:
interface FastEthernet0/0.35
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet0/0.193
 bfd interval 50 min_rx 50 multiplier 3
!
router bgp 2000
 neighbor 10.0.35.5 fall-over bfd
 neighbor 10.0.193.19 fall-over bfd

R5:
```

```
interface FastEthernet0/0.35
 bfd interval 50 min_rx 50 multiplier 3
!
router bgp 1000
 neighbor 10.0.35.3 fall-over bfd
 !
 address-family vpnv4
  bgp additional-paths install
  bgp recursion host

XR1:
router bgp 1000
 bfd minimum-interval 50
 bfd multiplier 3
 neighbor 10.0.193.3
  bfd fast-detect
 exit
 !
 address-family vpnv4 unicast
  additional-paths install backup
```

Task 4.7 Verification

```
RP/0/0/CPU0:XR1#show bfd session
Sun Jun 24 23:25:50.267 UTC
Interface            Dest Addr           Local det time(int*mult)      State
                                           Echo            Async
-------------------- --------------- ---------------- ---------------- ---------
Gi0/1/0/0.193        10.0.193.3      150ms(50ms*3)    6s(2s*3)         UP
R5#show bgp vpnv4 unicast vrf FOO
BGP table version is 240, local router ID is 10.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path
, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.0.0.5:1 (default for vrf FOO)
*>i172.16.0.1/32    10.0.0.1                      100      0 2000 i
*>i172.16.0.2/32    10.0.0.2                  0   100      0 i
*>i172.16.0.3/32    10.0.0.3                      100      0 2000 i
*>i172.16.0.4/32    10.0.0.4                  0   100      0 2000 i
*> 172.16.0.5/32    0.0.0.0                   0         32768 i   *b
i172.16.0.6/32    10.0.0.4                 10   100      0 2000 ?
```

```
*>i                 10.0.0.1                      100      0 2000 ?
*>i172.16.0.7/32    10.0.0.20                0    100      0 3000 i
*>i172.16.0.8/32    10.0.0.20                     100      0 3000 i
*>i172.16.0.19/32   10.0.0.19                0    100      0 i
*>i172.16.0.20/32   10.0.0.20                0    100      0 i
*>i172.16.16.0/24   10.0.0.4                20    100      0 2000 ?
*>i172.16.46.0/24   10.0.0.1                      100      0 2000 ?
*>i172.16.78.0/24   10.0.0.20                0    100      0 3000 i
   Network          Next Hop            Metric LocPrf Weight Path
*>i172.16.207.0/24  10.0.0.20               0    100      0 3000 i
*>i172.16.208.0/24  10.0.0.20                     100      0 3000 i
```

Task 4.8 Solution

```
R1:
vrf definition FOO
 address-family ipv6
 route-target export 2000:1
 route-target import 1000:1
 route-target import 2000:1
!
router bgp 2000
 address-family vpnv6
  neighbor 10.0.0.4 activate
 exit-address-family
 !
 address-family ipv6 vrf FOO
  no synchronization
  neighbor 2001:172:16:16::6 remote-as 3000
  neighbor 2001:172:16:16::6 as-override
  network 2001:172:16::1/128
 exit-address-family

R2:
vrf definition FOO address-family ipv6
 route-target export 1000:1
 route-target import 1000:1
 route-target import 2000:1
!
router bgp 1000
 address-family vpnv6
  neighbor 10.0.0.20 activate
 exit-address-family
```

```
 !
 address-family ipv6 vrf FOO
  no synchronization
  network 2001:172:16::2/128
 exit-address-family

R3:
vrf definition FOO
 address-family ipv6
 route-target export 2000:1
 route-target import 1000:1
 route-target import 2000:1
!
router bgp 2000
 address-family vpnv6
  neighbor 10.0.0.4 activate exit-address-
 family
 !
 address-family ipv6 vrf FOO
  no synchronization
  network 2001:172:16::3/128 exit-address-
 family

R4:
vrf definition FOO
 address-family ipv6
 route-target export 2000:1
 route-target import 1000:1
 route-target import 2000:1
!
router bgp 2000
 address-family vpnv6 neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 route-reflector-client
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 route-reflector-client
  neighbor 10.0.0.20 activate
  neighbor 10.0.0.20 next-hop-unchanged
 exit-address-family
 !
 address-family ipv6 vrf FOO
  no synchronization
  neighbor 2001:172:16:46::6 remote-as 3000
  neighbor 2001:172:16:46::6 as-override
  network 2001:172:16::4/128
 exit-address-family
```

```
R5:
vrf definition FOO
 address-family ipv6
 route-target export 1000:1
 route-target import 1000:1
 route-target import 2000:1
!
router bgp 1000
 address-family vpnv6
  neighbor 10.0.0.20 activate
 exit-address-family
 !
 address-family ipv6 vrf FOO
  no synchronization
  network 2001:172:16::5/128
 exit-address-family

R6:
ipv6 unicast-routing
!
router bgp 3000
 neighbor 2001:172:16:46::4 remote-as 2000
 neighbor 2001:172:16:16::1 remote-as 2000
 !
 address-family ipv6 unicast
  neighbor 2001:172:16:46::4 activate
  neighbor 2001:172:16:16::1 activate
  network  2001:172:16::6/128
  network 2001:172:16:16::/64
  network 2001:172:16:46::/64

R7:
ipv6 unicast-routing
!
router bgp 3000
 neighbor 2001:172:16:207::20 remote-as 1000
 !
 address-family ipv6 unicast
  neighbor 2001:172:16:207::20 activate
  network  2001:172:16::7/128
  network 2001:172:16:78::/64
  network 2001:172:16:207::/64

R8:
ipv6 unicast-routing
!
```

```
router bgp 3000
 neighbor 2001:172:16:208::20 remote-as 1000
 !
 address-family ipv6 unicast
  neighbor 2001:172:16:208::20 activate
  network  2001:172:16::8/128
  network 2001:172:16:78::/64
  network 2001:172:16:208::/64

XR1:
vrf FOO
 address-family ipv6 unicast
  import route-target
   1000:1
   2000:1
  !
  export route-target
   1000:1
  !
 !
router bgp 1000
 address-family vpnv6 unicast
 !
 neighbor 10.0.0.20
  address-family vpnv6 unicast
  !
 !
 vrf FOO
  address-family ipv6 unicast
   network 2001:172:16::19/128

XR2:
vrf FOO
 address-family ipv6 unicast
  import route-target
   1000:1
   2000:1
  !
  export route-target
   1000:1
  !
 !
router bgp 1000
 address-family vpnv6 unicast
 !
 neighbor 10.0.0.2
```

```
 address-family vpnv6 unicast
  route-reflector-client
!
neighbor 10.0.0.4
 address-family vpnv6 unicast
  route-policy PASS in
  route-policy PASS out
  next-hop-unchanged
!
neighbor 10.0.0.5
 address-family vpnv6 unicast
  route-reflector-client
!
neighbor 10.0.0.19
 address-family vpnv6 unicast
  route-reflector-client
!
vrf FOO
 address-family ipv6 unicast
  network 2001:172:16::20/128
!
neighbor 2001:172:16:207::7
 remote-as 3000
  address-family ipv6 unicast route-
   policy PASS in
  route-policy PASS out
  as-override
!
neighbor 2001:172:16:208::8
 remote-as 3000
  address-family ipv6 unicast
  route-policy PASS in
  route-policy PASS out
  as-override
```

Task 4.8 Verification

```
R6#show ipv6 route bgp
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:172:16::1/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::2/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::3/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::4/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::5/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::7/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::8/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::19/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16::20/128 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16:78::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16:207::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16
B   2001:172:16:208::/64 [20/0]
     via FE80::202:7EFF:FE84:8400, FastEthernet0/0.16

R6#tclsh
R6(tcl)#foreach X {
+>(tcl)#2001:172:16::1
+>(tcl)#2001:172:16::2
+>(tcl)#2001:172:16::3
+>(tcl)#2001:172:16::4
+>(tcl)#2001:172:16::5
+>(tcl)#2001:172:16::7
+>(tcl)#2001:172:16::8
+>(tcl)#2001:172:16::19
+>(tcl)#2001:172:16::20
+>(tcl)#2001:172:16:78::7
+>(tcl)#2001:172:16:78::8
+>(tcl)#2001:172:16:207::7
+>(tcl)#2001:172:16:208::8+>(tcl)#} { ping $X }


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::19, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16::20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16:78::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16:78::8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:172:16:207::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2001:172:16:208::8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
```

Task 4.9 Solution

```
R1:
username ROUTER7 password 0 CHAPPASS
!
pseudowire-class L2TPV3_PPP_TO_ETH
 encapsulation l2tpv3
 interworking ip
 ip local interface Loopback0
!
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ROUTER1
 clock rate 64000
 xconnect 10.0.0.5 79 pw-class L2TPV3_PPP_TO_ETH
 no shutdown

R5:
pseudowire-class L2TPV3_PPP_TO_ETH
 encapsulation l2tpv3
 interworking ip
 ip local interface Loopback0
!
interface FastEthernet0/0.59
 encapsulation dot1Q 59
 xconnect 10.0.0.1 79 pw-class L2TPV3_PPP_TO_ETH

SW1:
interface Vlan59
 ip ospf network point-to-point
```

Task 4.9 Verification

```
R1#show xconnect all detail
```

```
Legend:     XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up        DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby   HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                         S1 Segment 2                         S2
------+--------------------------------+--+--------------------------------+--
UP     ac   Se2/0(PPP)                   UP l2tp 10.0.0.5:79                  UP

            Interworking: ip                     Session ID: 1689243931
                                                 Tunnel ID: 2339390597
                                                 Protocol State: UP
                                                 Remote Circuit State: UP
                                                 pw-class: L2TPV3_PPP_TO_ETH
```

Task 4.10 Solution

```
R2:
frame-relay switching
!
pseudowire-class ATOM_FR_TO_ETH
 encapsulation mpls
 interworking ip
!
interface Serial2/0
 encapsulation frame-relay
 clock rate 64000
 frame-relay intf-type dce
 no shutdown
!
connect VLAN100 Serial2/0 100 l2transport
 xconnect 10.0.0.19 100 pw-class ATOM_FR_TO_ETH
!
connect VLAN200 Serial2/0 200 l2transport
 xconnect 10.0.0.19 200 pw-class ATOM_FR_TO_ETH

XR1:
interface GigabitEthernet0/1/0/1
 no shutdown
!
interface GigabitEthernet0/1/0/1.100 l2transport
 dot1q vlan 100
!
interface GigabitEthernet0/1/0/1.200 l2transport
```

```
 dot1q vlan 200
!
l2vpn
 pw-class ATOM_FR_TO_ETH
  encapsulation mpls
  !
 !
 xconnect group ATOM_TO_R2
  p2p VLAN100
   interface GigabitEthernet0/1/0/1.100
   neighbor 10.0.0.2 pw-id 100
    pw-class ATOM_FR_TO_ETH
   !
   interworking ipv4
  !
  p2p VLAN200
   interface GigabitEthernet0/1/0/1.200
   neighbor 10.0.0.2 pw-id 200
    pw-class ATOM_FR_TO_ETH
   !
   interworking ipv4
  !
 !
!

R8:
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial0/0.100 point-to-point
 ip address 100.0.0.8 255.255.255.0
 frame-relay interface-dlci 100
!
interface Serial0/0.200 point-to-point
 ip address 200.0.0.8 255.255.255.0
 frame-relay interface-dlci 200
```

Task 4.10 Verification

```
RP/0/0/CPU0:XR1#show l2vpn xconnect
Sun Jun 24 23:43:21.891 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
```

```
LU = Local Up, RU = Remote Up, CO = Connected, SB = Standby

XConnect                    Segment 1                   Segment 2
Group      Name       ST    Description           ST    Description           ST
------------------------    -------------------------   ------------------------
ATOM_TO_R2 VLAN100    UP    Gi0/1/0/1.100         UP    10.0.0.2       100    UP

--------------------------------------------------------------------------------
ATOM_TO_R2 VLAN200    UP    Gi0/1/0/1.200         UP    10.0.0.2       200    UP

--------------------------------------------------------------------------------
R8#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:

Reply to request 0 from 172.16.208.20, 4 msReply to request 0 from 200.0.0.10, 92 ms
Reply to request 0 from 100.0.0.10, 80 ms

Reply to request 0 from 172.16.78.7, 4 ms
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solutions 5.1 - 5.2 (pending update)

Task 5.1 Solution

```
R2:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.25
 mpls traffic-eng tunnels
 ip rsvp bandwidth 50000 15000
!
interface FastEthernet0/0.220
 mpls traffic-eng tunnels
 ip rsvp bandwidth 50000 15000
!
router isis 1000
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

R5:
mpls traffic-eng tunnels
!
interface FastEthernet0/0.25
 mpls traffic-eng tunnels
 ip rsvp bandwidth 50000 15000
!
interface FastEthernet0/0.195
 mpls traffic-eng tunnels
 ip rsvp bandwidth 50000 15000
!
interface FastEthernet0/0.205
```

```
 mpls traffic-eng tunnels
 ip rsvp bandwidth 50000 15000
!
router isis 1000
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
 mpls traffic-eng level-2

XR1:
router isis 1000
 address-family ipv4 unicast
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  metric-style wide
 !
!
rsvp
 interface POS0/6/0/0
  bandwidth 50000 15000
 !
 interface GigabitEthernet0/1/0/0.195
  bandwidth 50000 15000
 !
!
mpls traffic-eng
!
mpls traffic-eng interface POS0/6/0/0
 !
 interface GigabitEthernet0/1/0/0.195
 !
!

XR2:
router isis 1000
 address-family ipv4 unicast
  mpls traffic-eng level-1-2
  mpls traffic-eng router-id Loopback0
  metric-style wide
 !
!
rsvp
 interface POS0/7/0/0
  bandwidth 50000 15000
 !
 interface GigabitEthernet0/4/0/0.205
```

```
  bandwidth 50000 15000
 !
 interface GigabitEthernet0/4/0/0.220
  bandwidth 50000 15000
 !
!
mpls traffic-eng
!
mpls traffic-eng
 interface POS0/7/0/0
 !
 interface GigabitEthernet0/4/0/0.205
 !
 interface GigabitEthernet0/4/0/0.220
 !
!
```

Task 5.1 Verification

```
R2#show mpls traffic-eng topology brief
My_System_id: 0000.0000.0002.00 (isis  level-1)

Signalling error holddown: 10 sec Global Link Generation 8

IGP Id: 0000.0000.0002.00, MPLS TE Id:10.0.0.2 Router Node  (isis  level-1)
      link[0]: Broadcast, DR: 0000.0000.0002.01, nbr node id:1, gen:2
          frag id 0, Intf Address:10.0.25.2
          TE metric:10, IGP metric:10, attribute flags:0x0
          SRLGs: None

IGP Id: 0000.0000.0005.00, MPLS TE Id:10.0.0.5 Router Node  (isis  level-1)
      link[0]: Broadcast, DR: 0000.0000.0002.01, nbr node id:1, gen:4
          frag id 0, Intf Address:10.0.25.5
          TE metric:10, IGP metric:10, attribute flags:0x0
          SRLGs: None

IGP Id: 0000.0000.0020.00, MPLS TE Id:10.0.0.20 Router Node (isis   level-1)
      link[0]: Broadcast, DR: 0000.0000.0020.01, nbr node id:3, gen:8
          frag id 0, Intf Address:10.0.220.20, Nbr Intf Address:10.0.220.20
          TE metric:10, IGP metric:10, attribute flags:0x0
          SRLGs: None

<snip>
RP/0/0/CPU0:XR1#show mpls traffic-eng topology summary
```

```
Sun Jun 24 23:46:42.633 UTC
My_System_id: 0000.0000.0019.00 (IS-IS 1000 level-2)
My_BC_Model_Type: RDM

Signalling error holddown: 10 sec Global Link Generation 13

IS-IS 1000  level 2
  Local System Id:          0000.0000.0019
  TE router ID configured:  10.0.0.19
  in use:                   10.0.0.19

    IGP Id: 0000.0000.0005.00, MPLS TE Id: 10.0.0.5 Router Node
        2 links

    IGP Id: 0000.0000.0019.00, MPLS TE Id: 10.0.0.19 Router Node
        1 links

    IGP Id: 0000.0000.0020.00, MPLS TE Id: 10.0.0.20 Router Node
        1 links

    IGP Id: 0000.0000.0019.01, Network Node
        2 links

    IGP Id: 0000.0000.0020.03, Network Node
        2 links

    Total: 5 nodes (3 router, 2 network), 8 links

Grand Total: 5 nodes (3 router, 2 network)  8 links
```

Task 5.2 Solution

```
R2:
ip explicit-path name INTER_AREA_TE enable
 next-address loose 10.0.0.20
!
interface Tunnel0
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 tunnel mode mpls traffic-eng
 tunnel destination 10.0.0.19
 tunnel mpls traffic-eng autoroute destination
 tunnel mpls traffic-eng path-option 1 explicit name INTER_AREA_TE
```

Task 5.2 Verification

```
R2#show ip route 10.0.0.19
Routing entry for 10.0.0.19/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:  * directly connected, via Tunnel0
      Route metric is 0, traffic share count is 1
R2#traceroute 10.0.0.19

Type escape sequence to abort.
Tracing the route to 10.0.0.19
 1 10.0.220.20 [MPLS: Label 16031 Exp 0] 4 msec 4 msec 0 msec

  2 10.0.205.5 [MPLS: Label 28 Exp 0] 4 msec 0 msec 0 msec
  3 10.0.195.19 68 msec *  4 msec
```

CCIE Service Provider Lab Workbook v4.0 - CCIE Service Provider Full-Scale Lab 4 v4

Full-Scale Lab 4 Solutions 6.1 - 6.2 (pending update)

Task 6.1 Solution

```
R1:
ip multicast-routing
ip multicast-routing vrf FOO
!
interface FastEthernet0/0.13
 ip pim sparse-mode
!
interface FastEthernet0/0.14
 ip pim sparse-mode
!
interface FastEthernet0/0.16
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
interface Loopback1
 ip pim sparse-mode
!
vrf definition FOO
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.255.255.0 0.0.0.255
!
ip pim ssm default
!
router bgp 2000
 address-family ipv4 mdt
```

```
  neighbor 10.0.0.4 activate
 exit-address-family

R2:
ip multicast-routing
ip multicast-routing vrf FOO
!
interface FastEthernet0/0.25
 ip pim sparse-mode
!
interface FastEthernet0/0.220
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
interface Loopback1 ip pim sparse-mode
!
vrf definition FOO
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.255.255.0 0.0.0.255
!
ip pim ssm default
!
router bgp 1000
 address-family ipv4 mdt
  neighbor 10.0.0.20 activate
 exit-address-family
!
ip mroute 10.0.0.19 255.255.255.255 10.0.220.20

R3:
ip multicast-routing
ip multicast-routing vrf FOO
!
interface FastEthernet0/0.13
 ip pim sparse-mode
!
interface FastEthernet0/0.34
 ip pim sparse-mode
!
interface FastEthernet0/0.35
 ip pim sparse-mode
!
interface FastEthernet0/0.193
```

```
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
interface Loopback1
 ip pim sparse-mode
!
vrf definition FOO
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.255.255.0 0.0.0.255
!
ip pim ssm default
!
router bgp 2000
 address-family ipv4 mdt
  neighbor 10.0.0.4 activate
 exit-address-family

R4:
ip multicast-routing
ip multicast-routing vrf FOO
!
interface FastEthernet0/0.14
 ip pim sparse-mode
!
interface FastEthernet0/0.34
 ip pim sparse-mode
!
interface FastEthernet0/0.46
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
interface Loopback1
 ip pim sparse-mode
!
vrf definition FOO
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.255.255.0 0.0.0.255
!
ip pim ssm default
!
```

```
router bgp 2000
 address-family ipv4 mdt
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 route-reflector-client
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 route-reflector-client
  neighbor 10.0.0.20 activate
 exit-address-family

R5:
ip multicast-routing
ip multicast-routing vrf FOO
!
interface FastEthernet0/0.25
 ip pim sparse-mode
!
interface FastEthernet0/0.35
 ip pim sparse-mode
!
interface FastEthernet0/0.195
 ip pim sparse-mode
!
interface FastEthernet0/0.205
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
interface Loopback1
 ip pim sparse-mode
!
vrf definition FOO
 address-family ipv4
 mdt default 232.0.0.1
 mdt data 232.255.255.0 0.0.0.255
!
ip pim ssm default
!
router bgp 1000
 address-family ipv4 mdt
  neighbor 10.0.0.20 activate
 exit-address-family

R6:
ip multicast-routing
!
```

```
interface FastEthernet0/0.16
 ip pim sparse-mode
!
interface FastEthernet0/0.46
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode
!
ip pim bsr-candidate Loopback0
ip pim rp-candidate Loopback0

R7:
ip multicast-routing
!
interface FastEthernet0/0.78
 ip pim sparse-mode
!
interface FastEthernet0/0.207
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode

R8:
ip multicast-routing
!
interface FastEthernet0/0.78
 ip pim sparse-mode
!
interface FastEthernet0/0.208
 ip pim sparse-mode
!
interface Loopback0
 ip pim sparse-mode

XR1:
multicast-routing
 address-family ipv4
  interface all enable
 !
 vrf FOO
  address-family ipv4
   mdt source Loopback0
   mdt data 232.255.255.0/24
   mdt default ipv4 232.0.0.1 interface all enable
```

```
!
router bgp 1000
 address-family ipv4 mdt
 !
 neighbor 10.0.0.20
  address-family ipv4 mdt

XR2:
multicast-routing
 address-family ipv4
  interface all enable
 !
 vrf FOO
  address-family ipv4
   mdt source Loopback0
   mdt data 232.255.255.0/24
   mdt default ipv4 232.0.0.1
   interface all enable
!
router bgp 1000
 address-family ipv4 mdt
 !
 neighbor 10.0.0.2
  address-family ipv4 mdt
   route-reflector-client
!
neighbor 10.0.0.4
 address-family ipv4 mdt
  route-policy PASS in
  route-policy PASS out
!
neighbor 10.0.0.5
 address-family ipv4 mdt
  route-reflector-client
!
 neighbor 10.0.0.19 address-
  family ipv4 mdt
   route-reflector-client
```

Task 6.1 Verification

```
RP/0/0/CPU0:XR1#show bgp ipv4 mdt
Mon Jun 25 00:09:54.007 UTC
BGP router identifier 10.0.0.19, local AS number 1000
```

```
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 8
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10.0.0.1:1
*>i10.0.0.1/96      10.0.0.4                      100      0 2000 ?
Route Distinguisher: 10.0.0.2:1
*>i10.0.0.2/96      10.0.0.2                 0    100      0 ?
Route Distinguisher: 10.0.0.3:1
*>i10.0.0.3/96      10.0.0.4                      100      0 2000 ?
Route Distinguisher: 10.0.0.4:1
*>i10.0.0.4/96      10.0.0.4                 0    100      0 2000 ?
Route Distinguisher: 10.0.0.5:1
*>i10.0.0.5/96      10.0.0.5                 0    100      0 ?
Route Distinguisher: 10.0.0.19:1
*> 10.0.0.19/96     0.0.0.0                                0 i
Route Distinguisher: 10.0.0.20:1
*>i10.0.0.20/96     10.0.0.20                     100      0 i

Processed 7 prefixes, 7 paths
R1#sh ip pim vrf FOO neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
172.16.16.6       FastEthernet0/0.16       00:03:21/00:01:20 v2    1 /  DR S P G
10.0.0.4          Tunnel1                  00:00:37/00:01:36 v2    1 /  S P G
10.0.0.2          Tunnel1                  00:01:07/00:00:36 v2    1 /  S P G
10.0.0.20         Tunnel1                  00:01:33/00:01:23 v2    1 /  DR G
10.0.0.5          Tunnel1                  00:01:36/00:01:36 v2    1 /  S P G
10.0.0.3          Tunnel1                  00:01:36/00:01:36 v2    1 /  S P G
10.0.0.19         Tunnel1                  00:01:37/00:01:29 v2    1 /  G
R1#show ip pim vrf FOO rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4 RP 172.16.0.6
 (?), v2 Info source: 172.16.0.6 (?), via bootstrap
, priority 0, holdtime 150
```

```
        Uptime: 00:03:29, expires: 00:01:58
```

Task 6.2 Solution

```
R1:
interface Loopback1
 ip igmp join-group 239.0.0.1

R2:
interface Loopback1
 ip igmp join-group 239.0.0.2

R3:
interface Loopback1
 ip igmp join-group 239.0.0.3

R4:
interface Loopback1
 ip igmp join-group 239.0.0.4

R5:
interface Loopback1
 ip igmp join-group 239.0.0.5

R6:
interface Loopback0
 ip igmp join-group 239.0.0.6

R7:
interface Loopback0
 ip igmp join-group 239.0.0.7

R8:
interface Loopback0
 ip igmp join-group 239.0.0.8
```

Task 6.2 Verification

```
R6#ping 239.0.0.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.1, timeout is 2 seconds:
```

```
Reply to request 0 from 172.16.0.1, 8 ms
Reply to request 0 from 172.16.0.1, 28 ms
Reply to request 0 from 172.16.0.1, 28 ms
```
R6#ping 239.0.0.2

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.2, timeout is 2 seconds:

Reply to request 0 from 172.16.0.2, 20 ms
Reply to request 0 from 172.16.0.2, 40 ms
```
R6#ping 239.0.0.3

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.3, timeout is 2 seconds:

Reply to request 0 from 172.16.0.3, 4 ms
Reply to request 0 from 172.16.0.3, 4 ms
```
R6#ping 239.0.0.4

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.4, timeout is 2 seconds:

Reply to request 0 from 172.16.0.4, 4 ms
Reply to request 0 from 172.16.0.4, 4 ms
```
R6#ping 239.0.0.5

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.5, timeout is 2 seconds:

Reply to request 0 from 172.16.0.5, 4 ms
Reply to request 0 from 172.16.0.5, 4 ms
```
R6#ping 239.0.0.6

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.6, timeout is 2 seconds:

Reply to request 0 from 172.16.0.6, 8 ms
Reply to request 0 from 172.16.0.6, 8 ms
Reply to request 0 from 172.16.0.6, 8 ms
```
R6#ping 239.0.0.7

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.7, timeout is 2 seconds:

Reply to request 0 from 172.16.207.7, 4 ms
```

```
Reply to request 0 from 172.16.207.7, 4 ms
R6#ping 239.0.0.8


Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.0.0.8, timeout is 2 seconds:

Reply to request 0 from 172.16.208.8, 4 ms
Reply to request 0 from 172.16.208.8, 4 ms
```