1. Basic Initialization

    1.1. Load the provided initial configs, which contain basic IPv4 & IPv6 addressing per the diagram. Once complete, ensure that all devices can ping their directly connected neighbors with both IPv4 & IPv6.

2. Core Routing

    2.1. Configure OSPFv2 and OSPFv3 on all transit links that connect R2, R3, XR2, & XR3. Advertise their IPv4 and IPv6 Loopback0 interfaces into OSPFv2 and OSPFv3 respectively. Once complete you should have full IPv4 and IPv6 connectivity between these devices.

    2.2. Configure IS-IS Level 2 on all transit links that connect R1, R2, XR1, & XR2. Advertise their IPv4 and IPv6 Loopback0 interfaces into IS-IS respectively. Once complete you should have full IPv4 and IPv6 connectivity between these devices.

    2.3. Do not advertise unnecessary LSAs in the OSPF or IS-IS domains.

    2.4. Configure redistribution where necessary to allow for IPv4 & IPv6 reachability between R1, R2, R3, XR1, XR2, & XR3. Ensure that a single link or node failure does not break connectivity between the OSPF and IS-IS domains.

    2.5. Configure MPLS on all links on all routers in the core. Advertise the minimum number of labels necessary to form a full mesh of LDP tunnels between the 6 core routers. Protect against an IGP process failure causing a black hole on any link in the MPLS core. In the event of a link failure, MPLS information should be cached for 5 minutes on the core devices.

    2.6. Core routers are in BGP AS 123, R9 is in BGP AS 9, and XR4 is in AS 24. Configure R2 and XR2 to peer BGP with all routers in the core using AS 123. R9 and XR4 should peer VPNv4 & VPNv6 BGP. XR3 and XR4 should peer IPv4 Unicast BGP. XR4 should peer VPNv4 & VPNv6 BGP with R2 and XR2.

3. MPLS L3VPN

3.1. CE router R8 is in BGP AS 8. R8 should peer BGP with its MPLS L3VPN providers AS 9 and AS 123. Advertise R8's IPv4 and IPv6 Loopback0 addresses to the MPLS providers.

3.2. CE router R10 is in EIGRP AS 10. R10 should peer EIGRP with its MPLS L3VPN provider R2. Advertise R10's IPv4 and IPv6 Loopback0 addresses to the MPLS providers.

3.3. R4, R5, and R6 are in Customer Site 1. R7 is in Customer Site 2. Configure OSPF area 1 in Customer Site 1 and to its MPLS L3VPN provider. Configure OSPF area 2 in Customer Site 2 and to its MPLS L3VPN provider.

3.4. Establish IPv4 and IPv6 connectivity between R8 and R10. R8 should prefer to route to R9 for both IPv4 and IPv6 traffic.

3.5. Establish IPv4 and IPv6 connectivity between Customer Site 1 and Customer Site 2. Traffic between R6 and R7 should be load balanced between all available PE-CE connections.

4. MPLS TE

4.1. Configure an MPLS TE tunnel so that R5's traffic sent to the MPLS service provider is routed from R1 to XR1 to XR2 to XR2, and then load balanced between R3 and XR3.

5. MPLS L2VPN

5.1. Configure new IPv4 addresses 192.168.0.4/24 on R4's layer 2 link to R7, and address 192.168.0.8/24 on R8's layer 2 link to R5. R5 and R7 should peer L2VPN BGP to establish direct layer 3 connectivity between these addresses on R4 and R8.

6. Multicast

6.1. Configure R7 to listen for the multicast group 227.7.7.7. R6 should be able to ping this address and get a response from R7.

1. Basic Initialization

    1.1. Load the expanded lab initial configs onto devices R1, R3, XR3, XR4, and R11 – R20, which contain basic IPv4 & IPv6 addressing per the diagram. Once complete, ensure that all devices can ping their directly connected neighbors with both IPv4 & IPv6.

2. Carrier Supporting Carrier (CSC)

    2.1. R14 and R19 are the final CE routers that will be using the CSC network for transport. R14 is dual homed to its MPLS L3VPN provider via R12 and R13. R19's MPLS L3VPN provider is R17. Configure EIGRP AS 1419 on these devices, and advertise their IPv4 and IPv6 Loopback0 interfaces.

    2.2. R11, R12, R13, R16, R17, and R18 are in BGP AS 1000. Use IS-IS Level 1 routing on all links and Loopback0 interfaces in AS 1000 to provide IGP transport for both IPv4 and IPv6 within the two sites.

    2.3. Configure BGP as follows to provide CSC transport:

        2.3.1. R11 should peer IPv4 Unicast BGP with XR4
        2.3.2. R16 should peer IPv4 Unicast BGP with R1
        2.3.3. R12, R13, & R17 should peer full mesh VPNv4 and VPNv6 BGP

    2.4. Redistribute wherever necessary. Once the CSC network is completed, you should have both IPv4 and IPv6 connectivity between R14 and R19, with R14 load balancing traffic between both R12 and R13.

3. L3VPN Extranet

    3.1. R20 is hosting shared services for AS 123's L3VPN customers. Configure Extranet routing using BGP so that R6, R7, R8, & R10 are all able to reach the IPv4 and IPv6 Loopback0 addresses of R20. Traffic should not leak between R8/R10's site and R6/R7's site. Use only a single BGP peering on R20 to XR3 to accomplish this.

4. L3VPN Internet Access

    4.1. R3 connects to the Internet via R15. Configure the network so that R6, R7, R8, and R10 can all ping the IPv4 Loopback0 address of R15, while following these restrictions:

        4.1.1. Do not modify any routing configuration on R15.

        4.1.2. R3's link to R15 should remain in the global routing table.

        4.1.3. Traffic should not leak between R8/R10's site and R6/R7's site.

5. Unified MPLS

5.1. Remove the redistribution of OSPFv2 and IPv4 IS-IS on both R2 and XR2.

5.2. Modify your BGP peerings in AS 123 as follows:

5.2.1. R2 and XR2 should be route reflectors for IPv4 unicast to R1, R3, XR1, and XR3.

5.2.2. Advertise the IPv4 Loopback0 networks of all six of these routers into IPv4 Unicast BGP.

5.2.3. Once complete, any of the L3VPN traffic transiting over the core should still be successful, e.g. R6 to R7 IPv4 and IPv6 transport.

6. LISP

6.1. Modify the Customer 1 and Customer 2 sites PE-CE routing as follows:

6.1.1. Remove the VRF aware OSPFv2 process for Customer 1 & 2 on R1, R3, XR1, and XR3.

6.1.2. Configure R4, R5, and R7 with static default routes to their attached PE routers. Advertise these default routes into OSPFv2 on R4 and R5. Configure R20 with a static default route to XR3.

6.1.3. Advertise the following links into the VRF aware BGP process:

6.1.3.1. R1’s link to R5
6.1.3.2. R3’s link to R7
6.1.3.3. XR1’s link to R4
6.1.3.4. XR3’s link to R7
6.1.3.5. XR3’s link to R20

6.1.4. Ensure that you can ping IPv4 from R4, R5, & R7 to R20.

6.2. Configure LISP on R4, R5, R7 & R20 as follows:
6.2.1. R20 will be the Map Server and Map Resolver (MS/MR)
6.2.2. R4, R5, & R7 with be the Ingress and Egress Tunnel Routers (xTRs)
6.2.3. R4 and R5 should register their links to the PE’s as the Routing Locators (RLOCs) to R20 as “SITE1”.
6.2.4. R7 should register its links to both PEs as RLOCs to R20 as “SITE2”.
6.2.5. Once complete, R6 and R7 should have IP reachability to each other’s Loopback0 networks.

6.3. Modify the LISP configuration so that R4 accepts twice as much traffic for Site 1 as R5.

7. MPLS over GRE

7.1. Create a new Loopback1 interface on R5 and R7 with addresses 1.5.5.5/32 and 1.7.7.7/32. Configure a GRE tunnel between them sourced and unnumbered from Loopback0. Enable a new EIGRP process with AS 57 on the tunnel and the new Loopbacks. Enable LDP on the tunnel. Once complete you should have an LSP between the new Loopbacks.

8. L2VPN

8.1. Configure new IPv4 addresses 192.168.0.4/24 on R4's layer 2 link to R7, and address 192.168.0.8/24 on R8's layer 2 link to R5. Configure a point-to-point L2VPN circuit between R5 and R7 to transport the traffic between R4 and R8. Once complete, R4 and R8 should be able to ping each other over the layer 2 circuit.

8.2. Configure new IPv4 addresses 172.16.0.2/24, 172.16.0.9/24, and 172.16.0.22/24 on R2, R9, and XR2's additional links per the L2VPN diagram.

8.3. Configure BGP L2VPN peerings as follows:

8.3.1. R1 to R3
8.3.2. R2 to R3
8.3.3. R3 to XR3
8.3.4. XR1 to XR3

8.4. Establish a full mesh of pseudowires between PEs R1, R2, and XR1. Use BGP for signaling the VPLS membership.

9. MPLS Traffic Engineering

9.1. Enable OSPFv2 area 0 on all links between R1, R2, XR1, and XR2.

9.2. Configure an MPLS TE tunnel from R3 to XR1's Loopback using any available dynamic path in the core that has 25Mbps of bandwidth available. Dynamically route XR1's Loopback via the tunnel.
fs

9.3. Configure an MPLS TE tunnel from XR3 to XR2's Loopback so that it follows the path of XR3 > R3 > R2 > XR2. If this path is unavailable, fall back to any other available path. Use static routing out the tunnel to reach ***R1***. Once complete you should be able to ping from XR3's interface in the Customer Site 2 VRF to R1's interface in the Customer Site 1 VRF.

9.4. Modify R3's tunnel to XR1 so that it routes from R3 > R2 > XR2 > XR1. Do not use an explicit path for this or change any IGP metrics.

9.5. Configure R2 to protect R3's tunnel to XR1 in the case that R2's link to XR2 goes down. If this failure occurs, it should be detected within 500ms and traffic should re-route from R2 to R1 to XR2.

10. fsMulticast

10.1. Revert your configs to the VIRL file “csc.working.virl”

10.2. Enable multicast routing in VRF A on R2, R8, R10 & XR1. Use R2 RP for this customer. Use the BGP MDT AFI to advertise that R2 and XR1 are participating in multicast routing for customer A. Enable PIM SSM in the core where necessary to transport multicast traffic. Join the multicast group 228.8.8.8 on R8’s Loopback0. Once complete, R10 should be able to ping this address when sourcing traffic from its own Loopback0 interface.

10.3. Enable multicast routing in VRF B on R1, R3, R4, R5, R6, R7, XR1, & XR3. Use R7’s Loopback0 as the BSR and Candidate RP. Configure MLDP with R2 as the root of the tree and XR2 as the backup root of the tree for customer VRF B. Join the multicast group 226.6.6.6 on R6’s Loopback0. Once complete, R7 should be able to ping this address when sourcing traffic from its own Loopback0 interface.

1. Recently there was a circuit outage between R1 and R5, and failover did not properly occur to Customer Site 1's backup circuit via R4. Modify the network so that if R5's link to R1 is down, Customer Sites 1 & 2 maintain IP reachability to each other.

2. Network monitoring has indicated abnormally high utilization on the link between R2 and R3. Modify the network to restore R3's ability to load share traffic in the core between R2 and XR2.

3. After the outage for Customer Site 1 was resolved, network monitoring has indicated that the circuit from R4 to XR1 is no longer being used for load sharing traffic to and from Customer Site 1. Resolve so that traffic from R6 to R7 is load shared on both R4 and R5's circuits to the MPLS provider.

4. After a maintenance window in the core, the customer at R8's site has told you that their routing policy is no longer in effect. Resolve the issue to that R8 prefers to use the circuit to R9 to reach R10, and uses the circuit to XR1 only as a backup.

5. R14's site has reported an outage during a planned maintenance window on the circuit to R12. Resolve the issue so that failover to R14's circuit to R13 properly occurs if the circuit to R12 is down.

1. Customer Site 2 is unable to reach Customer Site 1. Resolve the reachability issue and match the following output when complete. Do not modify any interface configurations to accomplish this.

```
R7#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32
  Known via "ospf 1", distance 110, metric 5, type intra area
  Last update from 10.7.13.13 on GigabitEthernet2.713, 00:01:11 ago
  Routing Descriptor Blocks:
  * 10.7.13.13, from 6.6.6.6, 00:01:11 ago, via GigabitEthernet2.713
      Route metric is 5, traffic share count is 1

R7#traceroute 6.6.6.6 source 7.7.7.7
Type escape sequence to abort.
Tracing the route to 6.6.6.6
VRF info: (vrf in name/id, vrf out name/id)
  1 10.7.13.13 2 msec 1 msec 1 msec
  2  *  *
    10.2.13.2 [MPLS: Labels 16/34 Exp 0] 6 msec
  3 10.1.5.1 [MPLS: Label 34 Exp 0] 3 msec 3 msec 3 msec
  4 10.1.5.5 14 msec 6 msec 5 msec
  5 10.5.6.6 5 msec *  4 msec
```

2. After a maintenance window in AS 1000, customer sites R14 and R19 are unable to reach each other. Resolve the problem so that R14 and R19 can ping each other’s Loopback0 interfaces.

3. After an outage of the R2 core route reflector, R19 and R14 were unable to forward traffic to each other. Resolve the problem in the core so that if R2 is down, traffic for the CSC attached customers still forwards successfully.

4. After a circuit outage between AS 8 and AS 9, AS 8 lost IP reachability to its other sites. Resolve this issue so that if R8’s link to R9 is down, R8 can still ping R10’s Loopback0. Do not modify any BGP configuration to accomplish this.

5. After a circuit outage between R13 and R14, R14 lost reachability to its remote site. Solve the issue so that if the link between R13 and R14 is down, R14 still has IP reachability to R19.