Advanced Routing

Case Study v15.1

Requirements:

General

1. Use the Vmware virtual machine ROUTECS151 that is available in LMS (see the top of the LMS web page for the unit). Only use this VM for your case study!!! I have tested the VM using VMware Workstation. You will be able to run the VM on any operating system that supports VMware. The routers have already been configured so all you have to do is start them using the web browser GUI. To uncompress the VM you will require a password which is “ROUTECS151”.
2. What you learn in this case study will be examined in the Practical Exam and Final Exam. I'm happy to help you with the case study but I will not do it for you. You are permitted to work with other students to complete the case study but you are ultimately responsible for knowing the material.
3. Define the router ID's in each routing protocol where possible.
4. Be sure to verify that your router configurations are working correctly by using the appropriate show and debug commands. Your lab exercises will provide some of the appropriate commands but you will find many more in the videos and lecture slides. You will also need to do some research on the Cisco website. You need to start developing good testing and research skills because I will not be there to help you once you graduate. :-)

1.0. IP Addressing

1. Using the 10.0.0.0/8 network, subnet the network to allow for 2040 usable subnets. Using subnet #1162, subnet the network to allow for 30 usable subnets. Using your answer from the previous calculation, subnet the subnet #18 to allow for 6 usable subnets. **Hint:** if done correctly, the subnet mask that is required for any of the final subnets will be a /27.

2. Use subnet #2 from the final subnet calculation from above for the frame-relay network between R8, R11 & R12. Use the last usable IP address from this subnet and assign it to the S2/0 interface on R8. Use the first usable IP address from this subnet on R11's S2/0 interface and the second usable IP address on R12's S2/0 interface.

2.0. WAN Technologies

2.1. Frame Relay Hub-and-Spoke

Using only physical router interfaces, configure a Frame Relay hub-and-spoke network between R1, R2, and R5 with R1 as the hub. Traffic from R2 destined for R5 should transit R1, and vice versa. All routers are permitted to ping their own Frame Relay interface. Use only the DLCIs specified in the diagram. Do NOT use any dynamic layer 3 to layer 2 mappings over these Frame Relay connections (i.e. turn off inverse arp). You are required to use the frame-relay map statement to statically map the IP and the DLCI of each of the connections.

Verification

R1# show frame-relay map

```
Serial2/0 (up): ip 191.1.125.1 dlci 102(0x66,0x1860), static,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.5 dlci 105(0x69,0x1890), static,
              broadcast,
              CISCO, status defined, active
```

R2# show frame-relay map

```
Serial2/0 (up): ip 191.1.125.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.2 dlci 201(0xC9,0x3090), static,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.5 dlci 201(0xC9,0x3090), static,
              CISCO, status defined, active
```

R5# show frame-relay map

```
Serial2/0 (up): ip 191.1.125.1 dlci 501(0x1F5,0x7C50), static,
              broadcast,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.2 dlci 501(0x1F5,0x7C50), static,
              CISCO, status defined, active
Serial2/0 (up): ip 191.1.125.5 dlci 501(0x1F5,0x7C50), static,
              CISCO, status defined, active
```

R1#ping 191.1.125.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.1.125.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/38/50 ms
```

R1#ping 191.1.125.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.1.125.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/17/18 ms
```

R1#ping 191.1.125.5

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.1.125.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/18 ms
```

When R1 pings its own IP address, these packets will be sent to R2 and redirected back. This can be seen in the traceroute below.

R1# traceroute 191.1.125.1

```
Type escape sequence to abort.
Tracing the route to 191.1.125.1
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.125.2 15 msec 17 msec 17 msec
  2 191.1.125.1 35 msec 35 msec 34 msec
```

R1# traceroute 191.1.125.2

```
Type escape sequence to abort.
Tracing the route to 191.1.125.2
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.125.2 18 msec 17 msec 17 msec
```

R1# traceroute 191.1.125.5

```
Type escape sequence to abort.
Tracing the route to 191.1.125.5
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.125.5 17 msec 17 msec 13 msec
```

R2# traceroute 191.1.125.5

```
Type escape sequence to abort.
Tracing the route to 191.1.125.5
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.125.1 17 msec 14 msec 18 msec
  2 191.1.125.5 35 msec 34 msec 31 msec
```

R2# traceroute 191.1.125.2

```
Type escape sequence to abort.
Tracing the route to 191.1.125.2
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.125.1 15 msec 17 msec 18 msec
  2 191.1.125.2 30 msec 34 msec 36 msec
```

2.2. Hub-and-Spoke

Using only physical interfaces configure a Frame Relay hub-and-spoke network between R8, R11, and R12 with R8 as the hub. All routers are permitted to ping their own Frame Relay interface. Use only the DLCIs specified in the diagram. Do NOT use any dynamic layer 3 to layer 2 mappings over these Frame Relay connections (i.e. turn off inverse arp). You are required to use the frame-relay map statement to statically map the IP and the DLCI of each of the connections. Use the verification statements from section 2.1 as a guide to verify full connectivity of your Frame Relay configured interfaces.

2.3 Point-to-Point

Configure the Frame Relay connection between R6 and BBR1 using PVC 61 (i.e. DLCI 61) on R6's main Serial interface. Do NOT use any dynamic layer 3 to layer 2 mappings over this Frame Relay connection. Router R6 is permitted to ping its own Frame Relay interface.

Verification

```
R6#show frame-relay map
Serial2/0 (up): ip 54.1.3.254 dlci 61(0x3D,0xCD0), static,
              broadcast,
              CISCO, status defined, active
Serial2/0 (up): ip 54.1.3.6 dlci 61(0x3D,0xCD0), static,
              CISCO, status defined, active

R6#traceroute 54.1.3.254
Type escape sequence to abort.
Tracing the route to 54.1.3.254
VRF info: (vrf in name/id, vrf out name/id)
  1 54.1.3.254 17 msec 19 msec 32 msec

R6#traceroute 54.1.3.6
Type escape sequence to abort.
Tracing the route to 54.1.3.6
VRF info: (vrf in name/id, vrf out name/id)
  1 54.1.3.254 17 msec 18 msec 17 msec
  2 54.1.3.6 30 msec 34 msec 34 msec
```

3. Interior Gateway Routing

3.0 OSPFv2 General Requirements

- All routers running OSPF are to automatically use 1GB as their reference bandwidth for their route calculations.

- On routers R1, R2, R5, R8, R11, R12 you are required to use the *ip ospf* command on the interface to assign the interface to the correct area (see the CCNPv7 OSPF 3.2 Lab on how to do this). All other routers running OSPF are to use the network statement under the router ospf process to assign the interface to an OSPF.

- Advertise the Loopback 0 interfaces on all routers running OSPF but do not use the network statement or the *ip ospf* statement under the interface to accomplish this. Use the redistribute statement with a router-map named REDISTRIBUTE-LOOPBACK0 to match only the Loopback 0 interface. You should be able to apply the same statements to any router without changing anything.

3.1. OSPF Frame Relay

- Configure OSPF area 0 on the Frame Relay segment between R1, R2, and R5 using the *ip ospf network point-to-multipoint* statement on each routers S2/0 interface.

Verification

R1# show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.2.2         0   FULL/  -        00:01:48    191.1.125.2     Serial2/0
150.1.5.5         0   FULL/  -        00:01:51    191.1.125.5     Serial2/0
```

R1# show ip ospf interface s2/0

```
Serial2/0 is up, line protocol is up
  Internet Address 191.1.125.1/24, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 150.1.1.1, Network Type POINT_TO_MULTIPOINT, Cost: 5000
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           5000      no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:18
  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 2, Adjacent neighbor count is 2
    Adjacent with neighbor 150.1.2.2
    Adjacent with neighbor 150.1.5.5
  Suppress hello for 0 neighbor(s)
```

R1# show ip route ospf

```
Gateway of last resort is not set
      150.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
O E2     150.1.2.0/24 [110/20] via 191.1.125.2, 00:07:12, Serial2/0
O E2     150.1.5.0/24 [110/20] via 191.1.125.5, 00:07:24, Serial2/0
      191.1.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        191.1.125.2/32 [110/5000] via 191.1.125.2, 00:32:23, Serial2/0
O        191.1.125.5/32 [110/5000] via 191.1.125.5, 00:32:33, Serial2/0
```

R5# sh ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.1.1         0   FULL/  -        00:01:52    191.1.125.1     Serial2/0
```

R5# show ip route ospf

```
Gateway of last resort is not set
      150.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
O E2     150.1.1.0/24 [110/20] via 191.1.125.1, 00:13:44, Serial2/0
O E2     150.1.2.0/24 [110/20] via 191.1.125.1, 00:12:54, Serial2/0
      191.1.0.0/16 is variably subnetted, 12 subnets, 2 masks
O        191.1.125.1/32 [110/3906] via 191.1.125.1, 00:02:59, Serial2/0
O        191.1.125.2/32 [110/8906] via 191.1.125.1, 00:02:03, Serial2/0
```

- Configure OSPF area 48 on the Frame Relay segment between R8, R11, and R12 using the *ip ospf network point-to-multipoint* statement on each routers S2/0 interface. Use the previous show commands to verify your frame relay configurations on R8, R11 and R12.

3.2. OSPF

- Configure OSPF area 5 on R5.
- Configure OSPF area 13 on R1 and R3.
- Configure OSPF area 23 on R2 and R3.
- Configure OSPF area 27 on R2 and R7 (do NOT advertise the loopback interfaces 125 to 134 with OSPF).
- Configure OSPF area 34 on R3 and R4
- Configure OSPF area 45 on R4 and R5.
- Configure OSPF area 48 on R4 and R8.
- Configure OSPF area 90 on R4, R5, R9 and R10 (do NOT advertise the loopback interfaces starting with the 10 network with OSPF).

Verification

Verify that redistributed Loopback0 prefixes are announced as external prefixes.

R1# show ip route ospf | include E2

```
O E2     150.1.2.0/24 [110/20] via 191.1.125.2, 00:44:00, Serial2/0
O E2     150.1.3.0/24 [110/20] via 191.1.13.3, 00:36:17, Serial2/1
O E2     150.1.4.0/24 [110/20] via 191.1.125.5, 00:21:41, Serial2/0
O E2     150.1.5.0/24 [110/20] via 191.1.125.5, 00:44:00, Serial2/0
O E2     150.1.7.0/24 [110/20] via 191.1.125.2, 00:29:42, Serial2/0
O E2     150.1.9.0/24 [110/20] via 191.1.125.5, 00:04:15, Serial2/0
O E2     150.1.10.0/24 [110/20] via 191.1.125.5, 00:02:13, Serial2/0
```

R8# show ip route ospf | include E2

```
O E2     150.1.4.0/24 [110/20] via 191.1.48.4, 00:25:03, Ethernet0/0
O E2     150.1.11.0/24 [110/20] via 10.129.228.129, 01:20:30, Serial2/0
O E2     150.1.12.0/24 [110/20] via 10.129.228.130, 01:20:10, Serial2/0
```

Verify that redistributed Loopback0 prefixes are announced as external prefixes.

R1# show ip route ospf

```
Gateway of last resort is not set
      150.1.0.0/16 is variably subnetted, 9 subnets, 2 masks
O E2     150.1.2.0/24 [110/20] via 191.1.125.2, 00:52:55, Serial2/0
O E2     150.1.3.0/24 [110/20] via 191.1.13.3, 00:45:12, Serial2/1
O E2     150.1.4.0/24 [110/20] via 191.1.125.5, 00:30:36, Serial2/0
O E2     150.1.5.0/24 [110/20] via 191.1.125.5, 00:52:55, Serial2/0
O E2     150.1.7.0/24 [110/20] via 191.1.125.2, 00:38:37, Serial2/0
O E2     150.1.9.0/24 [110/20] via 191.1.125.5, 00:13:10, Serial2/0
O E2     150.1.10.0/24 [110/20] via 191.1.125.5, 00:11:08, Serial2/0
      191.1.0.0/16 is variably subnetted, 18 subnets, 2 masks
O IA     191.1.5.0/24 [110/5100] via 191.1.125.5, 00:52:55, Serial2/0
O IA     191.1.7.0/24 [110/5200] via 191.1.125.2, 00:38:42, Serial2/0
O IA     191.1.10.0/24 [110/5200] via 191.1.125.5, 00:11:03, Serial2/0
O IA     191.1.23.0/24 [110/8906] via 191.1.125.2, 00:43:29, Serial2/0
O IA     191.1.27.0/24 [110/5100] via 191.1.125.2, 00:42:51, Serial2/0
O IA     191.1.40.0/24 [110/5200] via 191.1.125.5, 00:11:03, Serial2/0
O IA     191.1.45.0/24 [110/5100] via 191.1.125.5, 00:30:51, Serial2/0
O IA     191.1.49.0/24 [110/5200] via 191.1.125.5, 00:13:15, Serial2/0
O IA     191.1.50.0/24 [110/5100] via 191.1.125.5, 00:30:41, Serial2/0
O IA     191.1.59.0/24 [110/5100] via 191.1.125.5, 00:30:31, Serial2/0
O IA     191.1.77.0/24 [110/5200] via 191.1.125.2, 00:38:42, Serial2/0
O        191.1.125.2/32 [110/5000] via 191.1.125.2, 00:52:55, Serial2/0
O        191.1.125.5/32 [110/5000] via 191.1.125.5, 00:52:55, Serial2/0
O IA     191.1.177.0/24 [110/5200] via 191.1.125.2, 00:38:42, Serial2/0
```

R8# show ip route ospf

```
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O        10.129.###.###/32 [110/1953] via 10.129.###.###, 01:08:03, Serial2/0
O        10.129.###.###/32 [110/1953] via 10.129.###.###, 01:08:03, Serial2/0
      150.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
O E2     150.1.4.0/24 [110/20] via 191.1.48.4, 00:29:47, Ethernet0/0
O E2     150.1.11.0/24 [110/20] via 10.129.###.###, 01:25:14, Serial2/0
O E2     150.1.12.0/24 [110/20] via 10.129.###.###, 01:24:54, Serial2/0
```

3.3. OSPF

- Traffic from R8 to the OSPF area 27 network 191.1.7.0/24 should transit the serial 2/0 link between R3 & R4 and should transit the link between R3 and R2. In the case that the link between R3 & R4 is down the traffic should transit the Ethernet link between R4 & R5. Use a route-map AREA-27-POLICY to implement your policy routing solution. **Hint:** part of this is accomplished with Virtual Links and using policy routing on router R4. Create the virtual-links first before implementing policy routing.

Verification of Virutal Links

Verify the virtual-links and new OSPF neighbors - policy routing had NOT been implemented at this time.

R4# show ip ospf nei

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.5.5         0   FULL/  -           -        191.1.45.5      OSPF_VL1
150.1.3.3         0   FULL/  -           -        191.1.34.3      OSPF_VL0
150.1.3.3         0   FULL/  -        00:00:33    191.1.34.3      Serial2/0
150.1.5.5         1   FULL/BDR        00:00:39    191.1.45.5      Ethernet0/0
150.1.8.8         1   FULL/BDR        00:00:30    191.1.48.8      Ethernet0/1
150.1.9.9         1   FULL/BDR        00:00:31    191.1.49.9      Ethernet0/3
150.1.10.10       1   FULL/BDR        00:00:39    191.1.40.10     Ethernet0/2
```

R4# show ip ospf

```
 Routing Process "ospf 1" with ID 150.1.4.4
 Start time: 3d13h, Time elapsed: 02:14:07.743
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an area border and autonomous system boundary router
 Redistributing External Routes from,
    connected, includes subnets in redistribution
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
```

```
Retransmission pacing timer 66 msecs
Number of external LSA 11. Checksum Sum 0x05BB27
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 5. 5 normal 0 stub 0 nssa
Number of areas transit capable is 2
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 1000 mbps
   Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:02:18.393 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 56. Checksum Sum 0x1DC6AA
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 37
        Flood list length 0
   Area 34
        Number of interfaces in this area is 1
        This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 00:06:58.693 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 45. Checksum Sum 0x185C3B
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
   Area 45
        Number of interfaces in this area is 1
        This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 00:02:18.393 ago
        SPF algorithm executed 5 times
        Area ranges are
        Number of LSA 46. Checksum Sum 0x176C32
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
   Area 48
        Number of interfaces in this area is 1
        Area has no authentication
```

```
        SPF algorithm last executed 00:03:17.577 ago
        SPF algorithm executed 6 times
        Area ranges are
        Number of LSA 35. Checksum Sum 0x141C6F
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 90
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:06:58.693 ago
        SPF algorithm executed 8 times
        Area ranges are
        Number of LSA 56. Checksum Sum 0x1FBC4D
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

R8# show ip route ospf

```
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.129.###.###/32 [110/1953] via 10.129.###.###, 00:13:31, Serial2/0
O       10.129.###.###/32 [110/1953] via 10.129.###.###, 00:13:31, Serial2/0
      150.1.0.0/16 is variably subnetted, 12 subnets, 2 masks
O E2     150.1.1.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.2.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.3.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.4.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.5.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.7.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.9.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.10.0/24 [110/20] via 191.1.48.4, 00:13:31, Ethernet0/0
O E2     150.1.11.0/24 [110/20] via 10.129.228.129, 00:13:31, Serial2/0
O E2     150.1.12.0/24 [110/20] via 10.129.228.130, 00:13:31, Serial2/0
      191.1.0.0/16 is variably subnetted, 19 subnets, 2 masks
O IA     191.1.5.0/24 [110/300] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.7.0/24 [110/9306] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.10.0/24 [110/300] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.13.0/24 [110/8012] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.23.0/24 [110/11818] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.27.0/24 [110/9206] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.34.0/24 [110/7912] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.40.0/24 [110/200] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.45.0/24 [110/200] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.49.0/24 [110/200] via 191.1.48.4, 00:13:21, Ethernet0/0
O IA     191.1.50.0/24 [110/300] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.59.0/24 [110/300] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.77.0/24 [110/9306] via 191.1.48.4, 00:12:16, Ethernet0/0
```

```
O        191.1.125.1/32 [110/4106] via 191.1.48.4, 00:12:16, Ethernet0/0
O        191.1.125.2/32 [110/9106] via 191.1.48.4, 00:12:16, Ethernet0/0
O        191.1.125.5/32 [110/200] via 191.1.48.4, 00:12:16, Ethernet0/0
O IA     191.1.177.0/24 [110/9306] via 191.1.48.4, 00:12:16, Ethernet0/0
```

R8# traceroute 191.1.7.7

```
Type escape sequence to abort.
Tracing the route to 191.1.7.7
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.48.4 6 msec 0 msec 0 msec
  2 191.1.45.5 1 msec 0 msec 0 msec
  3 191.1.125.1 17 msec 18 msec 15 msec
  4 191.1.125.2 34 msec 34 msec 35 msec
  5 191.1.27.7 35 msec 34 msec 34 msec
```

Verification of Policy Routing

R8# traceroute 191.1.7.7

```
Type escape sequence to abort.
Tracing the route to 191.1.7.7
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.48.4 4 msec 0 msec 1 msec
  2 191.1.34.3 8 msec 9 msec 9 msec
  3 191.1.23.2 26 msec 24 msec 25 msec
  4 191.1.27.7 25 msec 26 msec 26 msec
```

Traffic to the 191.1.7.0 network originating from other routers will use the route in the routing table and will not be policy routed.

R11# traceroute 191.1.7.7

```
Type escape sequence to abort.
Tracing the route to 191.1.7.7
VRF info: (vrf in name/id, vrf out name/id)
  1 10.129.###.### 14 msec 17 msec 18 msec
  2 191.1.48.4 17 msec 17 msec 18 msec
  3 191.1.45.5 18 msec 17 msec 13 msec
  4 191.1.125.1 34 msec 34 msec 31 msec
  5 191.1.125.2 52 msec 49 msec 53 msec
  6 191.1.27.7 53 msec 53 msec 52 msec
```

Shutdown the S2/0 interface on router R4 to verify that the traffic originating from router R8 will take the route via router R5.

R8# traceroute 191.1.7.7

```
Type escape sequence to abort.
Tracing the route to 191.1.7.7
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.48.4 1 msec 1 msec 0 msec
  2 191.1.45.5 0 msec 1 msec 0 msec
  3 191.1.125.1 20 msec 17 msec 17 msec
  4 191.1.125.2 35 msec 34 msec 35 msec
  5 191.1.27.7 35 msec 34 msec 35 msec
```

3.4. OSPF Filtering and Summarization

- On router R7 advertise the loopback interfaces 125 to 134 as OSPF E2 using the existing route-map REDISTRIBUTE-LOOPBACK0 with an ACL that only matches on the source IP address. The ACL should contain the minimal number of statements to accomplish this.
- Summarize the above networks. Do NOT over summarize the networks or under summarize the networks. Router R2 should see the summarized routes.
- Since R7's only connection to the rest of the routing domain is through R2 it does not need specific routing information about the rest of your network. Configure the network so that R2 filters all routing advertisements to R7 with the exception of a default route. **HINT:** see the verification output.
- Summarize the networks that start with 10 that originate from the OSPF area 90. Do NOT over summarize the networks or under summarize the networks. Routers running OSPF that are not connected to Area 90 should see the summarized routes.

Verification

R7# show ip ospf | begin Area 27

```
        Area 27
            Number of interfaces in this area is 4
            It is a NSSA area
            Area has no authentication
            SPF algorithm last executed 00:33:53.399 ago
            SPF algorithm executed 5 times
            Area ranges are
            Number of LSA 11. Checksum Sum 0x05753D
            Number of opaque link LSA 0. Checksum Sum 0x000000
            Number of DCbitless LSA 0
            Number of indication LSA 0
            Number of DoNotAge LSA 0
            Flood list length 0
```

R7# show ip route ospf

```
Gateway of last resort is 191.1.27.2 to network 0.0.0.0

O*N2  0.0.0.0/0 [110/1] via 191.1.27.2, 00:00:46, Ethernet0/0
```

R4# show ip route | include 150.1.7.0

```
O E2     150.1.7.0/24 [110/20] via 191.1.45.5, 00:36:41, Ethernet0/0
```

Verify summarization is working correctly on R7 and R2. See lab exercises for commands.

3.5. OSPF Authentication

- After a recent network security audit you have been informed that your OSPF network is susceptible to attack via the injection of false routing information. In order to prevent this problem from happening in the future configure your network so that all OSPF area 0 adjacencies are authenticated with an MD5 hash of the password CISCO123. **Hint:** Do NOT forget that your virtual-links require authentication also.
- All non-area 0 adjacencies should be authenticated with the clear-text password CCNP1234.

Verification

Verify that authentication has been enabled for all adjacencies.

R4# show ip ospf | begin Area

```
     Routing Process "ospf 1" with ID 150.1.4.4
     Start time: 3d13h, Time elapsed: 09:39:58.395
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     Supports Link-local Signaling (LLS)
     Supports area transit capability
     Supports NSSA (compatible with RFC 3101)
     Event-log enabled, Maximum number of events: 1000, Mode: cyclic
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        connected, includes subnets in redistribution
     Router is not originating router-LSAs with maximum metric
     Initial SPF schedule delay 5000 msecs
     Minimum hold time between two consecutive SPFs 10000 msecs
     Maximum wait time between two consecutive SPFs 10000 msecs
     Incremental-SPF disabled
     Minimum LSA interval 5 secs
     Minimum LSA arrival 1000 msecs
     LSA group pacing timer 240 secs
     Interface flood pacing timer 33 msecs
     Retransmission pacing timer 66 msecs
     Number of external LSA 16. Checksum Sum 0x098736
     Number of opaque AS LSA 0. Checksum Sum 0x000000
     Number of DCbitless external and opaque AS LSA 0
```

```
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 5. 5 normal 0 stub 0 nssa
Number of areas transit capable is 2
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 1000 mbps
   Area BACKBONE(0)
       Number of interfaces in this area is 2
       Area has message digest authentication
       SPF algorithm last executed 00:01:50.507 ago
       SPF algorithm executed 4 times
       Area ranges are
       Number of LSA 55. Checksum Sum 0x1BAB90
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 32
       Flood list length 0
   Area 34
       Number of interfaces in this area is 1
       This area has transit capability: Virtual Link Endpoint
       Area has simple password authentication
       SPF algorithm last executed 00:01:50.508 ago
       SPF algorithm executed 4 times
       Area ranges are
       Number of LSA 46. Checksum Sum 0x1707EE
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 45
       Number of interfaces in this area is 1
       This area has transit capability: Virtual Link Endpoint
       Area has simple password authentication
       SPF algorithm last executed 00:01:50.507 ago
       SPF algorithm executed 4 times
       Area ranges are
       Number of LSA 51. Checksum Sum 0x1844E8
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 48
       Number of interfaces in this area is 1
       Area has simple password authentication
       SPF algorithm last executed 00:00:18.403 ago
       SPF algorithm executed 5 times
       Area ranges are
       Number of LSA 32. Checksum Sum 0x106337
```

```
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 90
        Number of interfaces in this area is 2
        Area has simple password authentication
        SPF algorithm last executed 00:02:00.516 ago
        SPF algorithm executed 3 times
        Area ranges are
           10.2##.0.0/## Active(101) Advertise
           *** Output Omitted ***
        Number of LSA 54. Checksum Sum 0x1E577E
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

R4# show ip ospf virtual-links

```
 Virtual Link OSPF_VL1 to router 150.1.5.5 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 45, via interface Ethernet0/0
 Topology-MTID    Cost    Disabled     Shutdown      Topology Name
        0           100       no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency State FULL (Hello suppressed)
    Index 1/6, 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
  Cryptographic authentication enabled
    Youngest key id is 1
Virtual Link OSPF_VL0 to router 150.1.3.3 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 34, via interface Serial2/0
 Topology-MTID    Cost    Disabled     Shutdown      Topology Name
        0           7812      no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
    Adjacency State FULL (Hello suppressed)
    Index 2/7, 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
  Cryptographic authentication enabled
    Youngest key id is 1
```

Verify that we still have all OSPF neighbors.

R4# show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.5.5         0   FULL/  -           -        191.1.45.5      OSPF_VL1
150.1.3.3         0   FULL/  -           -        191.1.34.3      OSPF_VL0
150.1.3.3         0   FULL/  -        00:00:35    191.1.34.3      Serial2/0
150.1.5.5         1   FULL/DR         00:00:34    191.1.45.5      Ethernet0/0
150.1.8.8         1   FULL/DR         00:00:33    191.1.48.8      Ethernet0/1
150.1.9.9         1   FULL/DR         00:00:38    191.1.49.9      Ethernet0/3
150.1.10.10       1   FULL/DR         00:00:35    191.1.40.10     Ethernet0/2
```

3.6. Default Routing

R3 is the only connection between the OSPF domain and the other routing domains. In order to minimize the amount of memory necessary to maintain the routing table throughout the OSPF domain configure the network so that all routers in the OSPF network send their traffic towards R3 if they do not have a longer match in their routing table. In order to prevent the unnecessary forwarding of traffic that will eventually be dropped ensure that R3 only advertises this default route if it has an active connection to either BBR2 or BBR3**.**

Requirements: Create a prefix-list to permit the 192.10.1.0/24 and another prefix-list to permit the 204.12.1.0/24. Use a route-map to match the IP addresses in the prefix lists.

Hints: The above task dictates that R3 should originate a default route into the OSPF domain. However, a stipulation is placed on its generation of this default. This default should only be generated if its connections to either BBR2 or BBR3 are up. This type of stipulation is known as *conditional* advertisement. To enable the conditional advertisement of a default route in OSPF a route-map is required for the **default-information originate** statement. If the route-map is true, a default route is originated. If the route-map is false, a default route is not originated.

R1# show ip route

```
Gateway of last resort is 191.1.13.3 to network 0.0.0.0
```

```
R3#debug ip ospf lsa-generation
R3#conf t
R3(config)#int e0/1
R3(config-if)#shutdown
R3(config)#interface s2/1
R3(config-if)#shutdown
```

R1# show ip route

```
Gateway of last resort is not set
```

3.7. RIPv2

- Configure RIPv2 on R3 and R6's connections to the 204.12.1.0/24 network. Advertise R6's interface Loopback 0 into RIP.
- R3 should not accept any routes from BBR3 that have an odd number in the first octet. **Requirement:** Use a distance statement to accomplish this. **Hint:** Create a standard access list to permit networks that have an odd number in the first octet. Define a distance statement with the largest metric possible with the source address of the IP address along with a mask that will only select this host address of RBB3 then the access list. **Description:** By altering the administrative distance of the routes to infinite (255 for RIP), these routes will be removed from the IP routing table.

Verification

Verify basic RIP configuration (note the distance set for updates from BBR3)

R3# show ip protocols | begin rip

```
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: connected, ospf 1 (internal, external 1 & 2, nssa-external 1 & 2)

  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    Ethernet0/1           2     2
  Automatic network summarization is not in effect
```

```
  Maximum path: 4
  Routing for Networks:
    204.12.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    204.12.1.254         255      00:00:09
    204.12.1.6           120      00:00:03
  Distance: (default is 120)
    Address         Wild mask       Distance  List
    204.12.1.254              0.0.0.0      255  1
```

Verify that we receive all the prefixes from BB3

R3# debug ip rip

```
*Sep 13 04:51:03.171: RIP: received v2 update from 204.12.1.254 on Ethernet0/1
*Sep 13 04:51:03.171:      30.0.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.171:      30.1.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      30.2.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      30.3.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      31.0.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      31.1.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      31.2.0.0/16 via 0.0.0.0 in 1 hops
*Sep 13 04:51:03.172:      31.3.0.0/16 via 0.0.0.0 in 1 hops
```

Verify that only prefixes with an even first octet are installed into the routing table.

R3# show ip route rip

```
Gateway of last resort is not set
      30.0.0.0/16 is subnetted, 4 subnets
R        30.0.0.0 [120/1] via 204.12.1.254, 00:00:16, Ethernet0/1
R        30.1.0.0 [120/1] via 204.12.1.254, 00:00:16, Ethernet0/1
R        30.2.0.0 [120/1] via 204.12.1.254, 00:00:16, Ethernet0/1
R        30.3.0.0 [120/1] via 204.12.1.254, 00:00:16, Ethernet0/1
      150.1.0.0/16 is variably subnetted, 13 subnets, 2 masks
R        150.1.6.0/24 [120/1] via 204.12.1.6, 00:00:14, Ethernet0/1
```

3.8. IGP Redistribution

- On router R3, redistribute RIP into OSPF but ONLY the prefix of R6's Loopback 0 network is permitted. **Hint:** Accomplished this by matching R6's Loopback 0 address with a prefix-list, then matching the prefix-list in a route-map, and applying the route-map to filter the redistribution of RIP into OSPF.
- Redistribute OSPF into RIP but be careful. The statements to do the redistribution are:

```
router rip
redistribute connected metric 1 route-map CONNECTED->RIP
redistribute ospf 1 metric 1
!
route-map CONNECTED->RIP permit 10
match interface Ethernet0/0 Loopback0 Serial2/0 Serial2/1 Serial2/2
Serial2/3
```

NOTE: R3's Loopback 0 interface has been advertised into the OSPF domain through redistribution. Although OSPF is redistributed into RIP, this does not imply that R3's Loopback 0 interface is redistributed into RIP. Indirect redistribution between two protocols cannot be accomplished on the same local devices. For example, suppose that protocol A is redistributed into protocol B. Protocol B is then redistributed into protocol C. This does not imply that protocol A was redistributed into protocol C. Instead, protocol A must be manually redistributed into protocol C to achieve the desired effect. This can be seen in the above output since R3's Loopback 0 network is redistributed as connected into the RIP domain.

Verify that only R6's Loopback0 is redistributed into OSPF from RIP

R1# show ip route ospf | include 150.1.6.0

```
O E2     150.1.6.0/24 [110/99999] via 191.1.13.3, 00:00:08, Serial2/1
```

Note: the metric of 99999. This is the value that you will use in your ospf rip redistribution statement.

Next verify that you have full network connectivity with the following addresses. You will need to add the IP addresses for the Frame Relay network between R8, R11 and R12. **NOTE:** you will NOT be able to ping everything (i.e. router R13).

3.9. EIGRP AS10

- Configure EIGRP AS 128 on routers R11, R12 and R13. Advertise R13's loopback interface in EIGRP. Use the inverted mask 0.0.0.255 specify each interface.

R12# show ip eigrp nei

```
EIGRP-IPv4 Neighbors for AS(128)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   191.1.128.13            Et0/0                    13 00:06:57    7   100  0  5
0   191.1.128.11            Et0/0                    12 00:09:59   14   100  0  6
```

R12# show ip route eigrp

```
Gateway of last resort is 10.129.228.190 to network 0.0.0.0
      150.1.0.0/16 is variably subnetted, 14 subnets, 2 masks
D        150.1.13.0/24 [90/409600] via 191.1.128.13, 00:00:30, Ethernet0/0
      191.1.0.0/16 is variably subnetted, 21 subnets, 2 masks
D        191.1.129.0/24 [90/307200] via 191.1.128.13, 00:00:27, Ethernet0/0
```

- Configure EIGRP AS 10 on R6's Frame Relay link to BBR1.

R6#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   54.1.3.254              Se2/0                   175 00:17:50 1587  5000  0  2
```

R6#show ip route eigrp

```
Gateway of last resort is not set
D     200.0.0.0/24 [90/2297856] via 54.1.3.254, 00:18:00, Serial2/0
D     200.0.1.0/24 [90/2297856] via 54.1.3.254, 00:18:00, Serial2/0
D     200.0.2.0/24 [90/2297856] via 54.1.3.254, 00:18:00, Serial2/0
D     200.0.3.0/24 [90/2297856] via 54.1.3.254, 00:18:00, Serial2/0
```

- Configure EIGRP AS 10 on R4's Loopback 4 interface. Use the inverted mask to advertise a /24.

R4#show ip protocols | begin eigrp 10

```
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```
  NSF-aware route hold timer is 240
  Router-ID: 150.1.4.4
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  191.1.4.0/24
Routing Information Sources:
  Gateway         Distance      Last Update
Distance: internal 90 external 170
```

3.10. EIGRP Redistribution

- R11 and R12, redistribute EIGRP into OSPF and OSPF into EIGRP (i.e. mutual redistribution). Because there are two routers which will be redistributing routes you will need to use route tags to prevent routing loops.

R13# show ip route 150.1.1.1

```
Routing entry for 150.1.1.0/24
  Known via "eigrp 128", distance 170, metric 2560025856
  Tag 88, type external
  Redistributing via eigrp 128
  Last update from 191.1.128.11 on Ethernet0/0, 00:52:42 ago
  Routing Descriptor Blocks:
  * 191.1.128.11, from 191.1.128.11, 00:52:42 ago, via Ethernet0/0
      Route metric is 2560025856, traffic share count is 1
      Total delay is 1010 microseconds, minimum bandwidth is 1 Kbit
      Reliability 1/255, minimum MTU 1 bytes
      Loading 1/255, Hops 1
      Route tag 88
```

R8# show ip route 150.1.13.13

```
Routing entry for 150.1.13.0/24
  Known via "ospf 1", distance 110, metric 20
  Tag 111, type extern 2, forward metric 1953
  Last update from 10.129.228.129 on Serial2/0, 00:19:00 ago
  Routing Descriptor Blocks:
  * 10.129.228.129, from 150.1.11.11, 00:57:10 ago, via Serial2/0
      Route metric is 20, traffic share count is 1
      Route tag 111
```

Verification

Use the following TCL script to verify that you have full connectivity. If you there are any unsuccessful pings you will need to troubleshoot until you are able to ping all the IP address.

```
tclsh

foreach i {
150.1.1.1
150.1.2.2
150.1.3.3
150.1.4.4
150.1.5.5
150.1.6.6
150.1.7.7
150.1.8.8
150.1.9.9
150.1.10.10
150.1.11.11
150.1.12.12
150.1.13.13
191.1.13.1
191.1.125.1
191.1.23.2
191.1.27.2
192.10.1.3
204.12.1.3
191.1.23.3
191.1.34.3
191.1.48.4
191.1.45.4
191.1.40.4
191.1.49.4
191.1.34.4
191.1.5.5
191.1.125.5
191.1.45.5
191.1.59.5
191.1.50.5
204.12.1.6
191.1.27.7
191.1.7.7
191.1.77.7
191.1.177.7
191.1.48.8
191.1.49.9
191.1.59.9
191.1.40.10
191.1.50.10
191.1.10.10
191.1.129.13
10.225.0.1
10.226.0.1
10.227.0.1
10.228.0.1
10.229.0.1
10.230.0.1
10.231.0.1
10.232.0.1
10.233.0.1
10.234.0.1
10.235.0.1
10.236.0.1
10.237.0.1
10.238.0.1
10.239.0.1
10.240.0.1
10.241.0.1
10.242.0.1
10.242.0.1
10.244.0.1

} { puts [exec "ping $i" ] }
```

3.11. GRE Tunnel

Users on the 191.1.4.0/24 network needs access to file servers behind BBR1 however your corporate policy dictates that no other hosts on your network should have access to the resources on the 191.1.4.0/24 network or BBR1. In order to accomplish this you have decided to configure a GRE tunnel between R4 and R6. Use the IP addresses 191.1.46.x/24 (x = router number) for the tunnel interfaces. Ensure that 191.1.4.0/24 on R4 maintains connectivity if either the Serial link to R3 or the Ethernet link to R5 goes down. As an additional integrity check ensure that any corrupt packets received over the tunnel interface are discarded. **Hint:** you will need to use a checksum to accomplish this.

Verification

Verify that tunnel is up and working.

```
R6# ping 191.1.46.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.1.46.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/20/22 ms
```

```
R6# traceroute 191.1.46.6
Type escape sequence to abort.
Tracing the route to 191.1.46.6
VRF info: (vrf in name/id, vrf out name/id)
  1 191.1.46.6 6 msec 4 msec 5 msec
```

```
R6# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   191.1.46.4              Tu0                      11 00:01:28   23  1470  0  3
0   54.1.3.254              Se2/0                   137 03:14:59 1021  5000  0  2
```

```
R6# show ip route eigrp
Gateway of last resort is not set
      191.1.0.0/16 is variably subnetted, 25 subnets, 2 masks
D        191.1.4.0/24 [90/26905600] via 191.1.46.4, 00:01:54, Tunnel0
D     200.0.0.0/24 [90/2297856] via 54.1.3.254, 03:15:23, Serial2/0
D     200.0.1.0/24 [90/2297856] via 54.1.3.254, 03:15:23, Serial2/0
D     200.0.2.0/24 [90/2297856] via 54.1.3.254, 03:15:23, Serial2/0
D     200.0.3.0/24 [90/2297856] via 54.1.3.254, 03:15:23, Serial2/0
```

Verify that R4 can ping R6 EIGRP-enabled interfaces, as well as BBR1 EIGRP prefixes with the following Tcl script

```
tclsh
foreach i {
200.0.0.1
54.1.3.6
54.1.3.254
200.0.1.1
200.0.2.1
200.0.3.1
} { puts [exec "ping $i" ] }
```

4.0. Exterior Gateway Routing

Non BGP speaking devices do not need IP reachability to BGP learned prefixes.

4.1. BGP Peering

- Configure BGP on the following devices with the following AS numbers:

Device	BGP AS
R3	200
R4	100
R6	100
BBR1	54
BBR2	254
BBR3	54

- Configure the BGP peering sessions as follows:

Device 1	Device 2
R6	BBR1
R6	BBR3
R6	R3
R6	R4
R3	BBR2

c

- All BGP traffic between R4 and R6 should traverse the GRE tunnel.
- Configure R3 to authenticate its BGP peering session with BBR2 using the password CISCO.

Verification

Verify BGP neighbors. Ensure that R6 and R4 peer over the GRE tunnel.

```
R6#show ip bgp summary | begin Neighbor
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
54.1.3.254      4           54      65      66       46    0    0 00:46:54        10
191.1.46.4      4          100      54      64       46    0    0 00:46:55         0
204.12.1.3      4          200      10      14       46    0    0 00:04:23         5
204.12.1.254    4           54      65      63       46    0    0 00:46:57        10
```

4.2. BGP Best path Selection

- Administrators of your network have reported congestion on the Ethernet segment between R6 and BBR3. In order to alleviate this congestion administrators of AS 100 have decided to send traffic for all prefixes learned from AS 54 to BBR1.
- Configure your network to reflect this policy.
- Do not use local preference to accomplish this.

Verification

Verify that best paths to AS54 prefixes are through BBR1

```
R6# show ip bgp regexp _54$
BGP table version is 46, local router ID is 150.1.6.6
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
 *>  28.119.16.0/24   54.1.3.254                             100 54 i
 *                    204.12.1.254             0             0 54 i
 *>  28.119.17.0/24   54.1.3.254                             100 54 i
 *                    204.12.1.254             0             0 54 I

*** Output Omitted ***
```

```
R6#show ip route 28.119.16.0
Routing entry for 28.119.16.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 54, type external
  Last update from 54.1.3.254 00:50:39 ago
  Routing Descriptor Blocks:
  * 54.1.3.254, from 54.1.3.254, 00:50:39 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 54
      MPLS label: none
```

4.3. BGP Filtering

- Memory usage on your BGP speaking devices is getting dangerously high. After investigating the problem, you have determined that the BGP table is consuming too much memory. In order to help cut down on the memory requirements throughout the BGP domain, your design team has implemented a new filtering policy. This policy states that AS 100 will not accept any prefixes from AS 54 with a mask longer than a /20.
- Configure R6 to reflect this policy.
- The prefix-list used to accomplish this should only have one line.

Verification

Verify that the routers only receives /20 prefixes or shorter. First verify the BGP configuration

R6#show ip protocols | begin bgp

```
Routing Protocol is "bgp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Route flap dampening configured and enabled
  Dampening routemap is DAMPEN
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    54.1.3.254                                            BBR3
    191.1.46.4
    204.12.1.3
    204.12.1.254                                          FROM_BBR3
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    204.12.1.254          20      00:53:21
    204.12.1.3            20      00:10:33
    54.1.3.254            20      00:53:21
  Distance: external 20 internal 200 local 200
```

R6#debug ip bgp updates
R6#clear ip bgp 204.12.1.254 soft in

```
*Sep 13 11:00:18.241: BGP(0): 204.12.1.254 rcvd UPDATE w/ attr: nexthop
204.12.1.254, origin i, metric 0, merged path 54, AS_PATH
*Sep 13 11:00:18.241: BGP(0): 204.12.1.254 rcvd 28.119.16.0/24 -- DENIED due to:
route-map;
*Sep 13 11:00:18.241: BGP(0): 204.12.1.254 rcvd 28.119.17.0/24 -- DENIED due to:
route-map;
*Sep 13 11:00:18.241: BGP: nbr_topo global 204.12.1.254 IPv4 Unicast:base
(0xB391FB10:1) rcvd Refresh End-of-RIB
```

Verify that the prefix-list has only one line

R6# show running-config | include ip prefix-list

```
ip prefix-list SLASH_20_AND_UNDER seq 5 permit 0.0.0.0/0 le 20
```

4.4. BGP Summarization

- Configure R3 to advertise a summary of your major network, 191.x.0.0/16, and your Loopback 0 addresses, 150.x.0.0/20, into BGP. You are required to use two static routes on R3 to accomplish this.

Verification

Verify that R3 originates the summaries

R3# show ip bgp regexp ^$

```
R3#show ip bgp regexp ^$
BGP table version is 16, local router ID is 150.1.3.3
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
 *>  150.1.0.0/20     0.0.0.0                  0         32768 ?
 *>  191.1.0.0        0.0.0.0                  0         32768 ?
```

R6# show ip bgp

```
BGP table version is 46, local router ID is 150.1.6.6
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
 *>  28.119.16.0/24   54.1.3.254                             100 54 i
 *>  28.119.17.0/24   54.1.3.254                             100 54 i
 *>  112.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
 *>  113.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
 *>  114.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
 *>  115.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
 *>  116.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
 *>  117.0.0.0        54.1.3.254               0             100 54 i
 *                    204.12.1.254                             0 54 i
```

```
*>  118.0.0.0        54.1.3.254              0           100 54 i
*                    204.12.1.254                          0 54 i
*>  119.0.0.0        54.1.3.254              0           100 54 i
*                    204.12.1.254                          0 54 i
*>  150.1.0.0/20     204.12.1.3              0             0 200 ?
*>  191.1.0.0        204.12.1.3              0             0 200 ?
*>  205.90.31.0      204.12.1.3                            0 200 254 ?
*>  220.20.3.0       204.12.1.3                            0 200 254 ?
*>  222.22.2.0       204.12.1.3                            0 200 254 ?
```

4.5. BGP Table Stability

High CPU utilization has been reported on R6. After further investigation, you have discovered that the prefixes 112.0.0.0/8 and 113.0.0.0/8 from AS 54's customers have been constantly flapping and causing R6 to continuously recalculate the BGP topology. In order to minimize the impact of this flapping on the rest of the BGP domain, configure R6 so that these prefixes are not advertised if they are consistently unstable. No other prefixes should be affected by this configuration.

Hint: Define a prefix-list that will match the 112.0.0.0/8 and 113.0.0.0/8 networks. Define a route-map that will match these address and set the dampening parameters to: Half-Life =15, Value to start reusing a route = 750, Value to start suppressing a route = 2000, and Maximum duration to suppress a stable route = 60. Then apply the route-map to bgp using the bgp dampening route-map (your defined route).