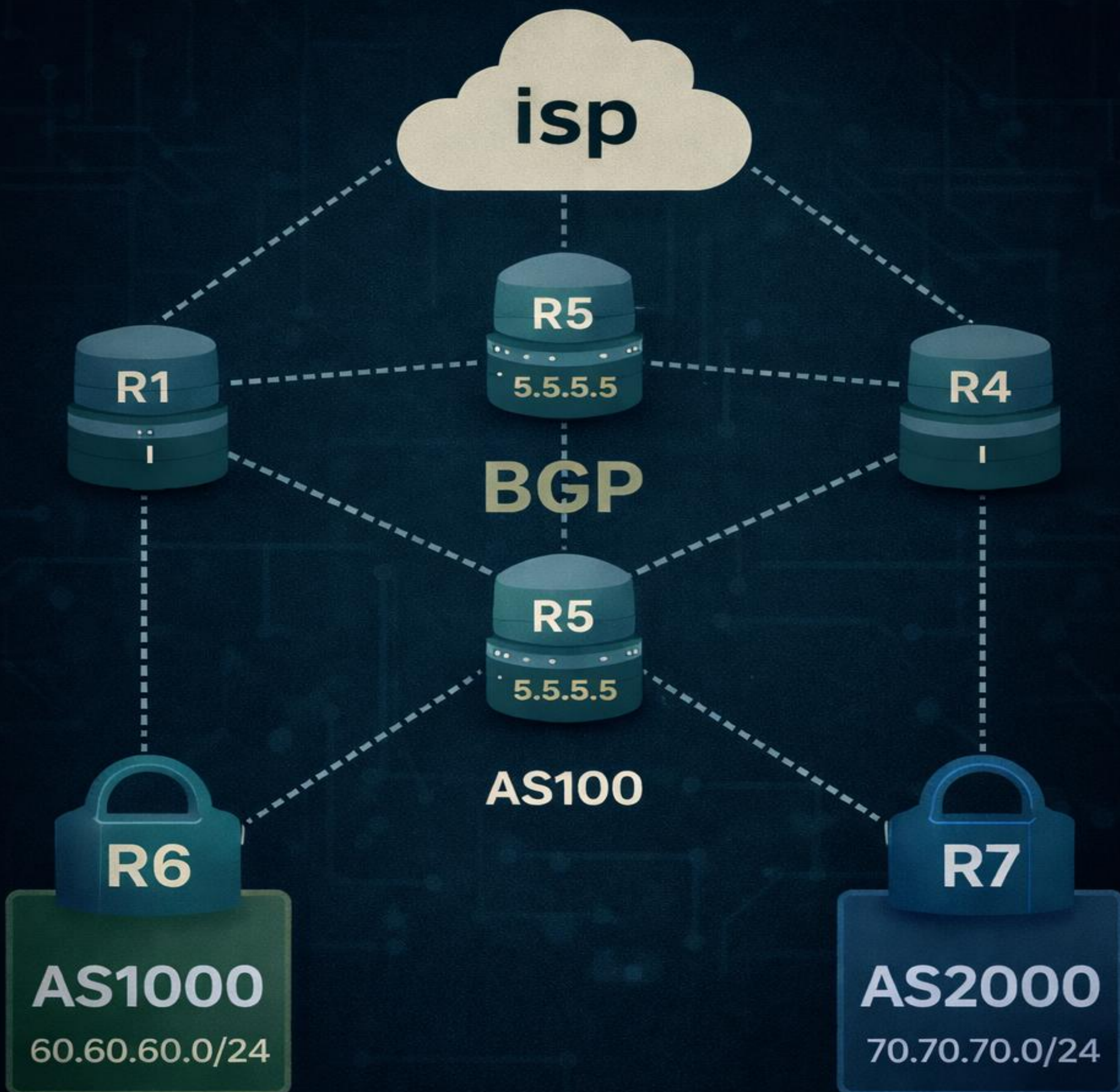
Hussain
NETWORKING



ISP BGP CORE WITH ROUTE REFLECTORS LAB

ISP BGP Core with Route Reflectors Lab

Table of Contents

ISP BGP Core with Route Reflectors Lab

Scenario

This lab simulates a small Internet Service Provider (ISP) backbone using Border Gateway Protocol (BGP) with a Route Reflector (RR) design.

The ISP core network operates under Autonomous System 100 (AS100) and consists of five routers (R1–R5). Router R5 acts as the Route Reflector, while R1–R4 operate as edge routers connecting the ISP core to external networks.

Two external autonomous systems are connected to the ISP:

AS1000 (R6) – Customer Network 1

AS2000 (R7) – Customer Network 2

Each external AS advertises its own network prefix to AS100 using eBGP. These prefixes are then distributed internally within AS100 using iBGP and Route Reflection.

OSPF is used as the Interior Gateway Protocol (IGP) inside AS100 to provide internal reachability between routers and to carry loopback addresses.

The lab demonstrates how an ISP uses route reflectors to scale iBGP, provide transit connectivity, and exchange routing information between multiple autonomous systems.

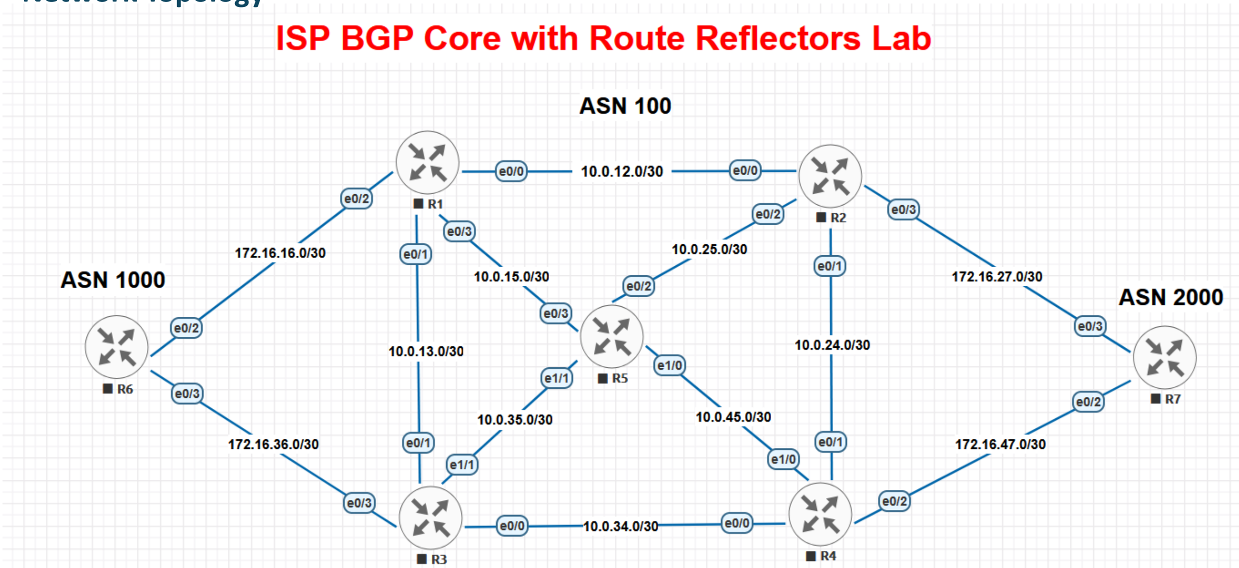
Objectives

After completing this lab, the student will be able to:

1. **Configure OSPF as an internal routing protocol for an ISP core network.**
2. **Establish iBGP sessions using loopback interfaces.**
3. **Implement a Route Reflector to eliminate full-mesh iBGP requirements.**
4. **Configure eBGP peering with external autonomous systems.**
5. **Advertise customer networks using BGP.**
6. **Understand and apply the next-hop-self feature.**
7. **Verify BGP routing using show commands.**
8. **Demonstrate end-to-end connectivity between external autonomous systems.**
9. **Analyze control-plane and data-plane behavior in a multi-AS environment.**
10. **Troubleshoot BGP next-hop and reachability issues.**

ISP BGP Core with Route Reflectors Lab

Network Topology



Address Table			
Device	**Interface**	**IP address**	**Subnet mask**
R1	E0/0	10.0.12.1	255.255.255.252
	E0/1	10.0.13.1	255.255.255.252
	E0/2	172.16.16.1	255.255.255.252
	E0/3	10.0.15.1	255.255.255.252
	Loopback 0	1.1.1.1	255.255.255.255
R2	E0/0	10.0.12.2	255.255.255.252
	E0/1	10.0.24.1	255.255.255.252
	E0/2	10.0.25.1	255.255.255.252
	E0/3	172.16.27.1	255.255.255.252
	Loopback 0	2.2.2.2	255.255.255.255
R3	E0/0	10.0.34.1	255.255.255.252
	E0/1	10.0.13.2	255.255.255.252
	E0/3	172.16.36.1	255.255.255.252
	E1/1	10.0.35.1	255.255.255.252
	Loopback 0	3.3.3.3	255.255.255.255
R4	E0/0	10.0.34.2	255.255.255.252
	E0/1	10.0.24.2	255.255.255.252
	E0/2	172.16.47.1	255.255.255.252

ISP BGP Core with Route Reflectors Lab

	E1/0	10.0.45.1	255.255.255.252
	Loopback 0	4.4.4.4	255.255.255.255
R5	E0/2	10.0.25.2	255.255.255.252
	E0/3	10.0.15.2	255.255.255.252
	E1/0	10.0.45.2	255.255.255.252
	E1/1	10.0.35.2	255.255.255.252
	Loopback 0	5.5.5.5	255.255.255.255
R6	E0/2	172.16.16.2	255.255.255.252
	E0/3	172.16.36.2	255.255.255.252
	Loopback 0	60.60.60.1	255.255.255.0
R7	E0/2	172.16.47.2	255.255.255.252
	E0/3	172.16.27.2	255.255.255.252
	Loopback 0	70.70.70.1	255.255.255.0

ISP BGP Core with Route Reflectors Lab

Step 1: Prepare the routers for the lab.

Import the topology diagram “**ISP BGP Core with Route Reflectors Lab.zip**” from the **GitHub repository** in EVE-NG. The routers should have configurations preloaded.

Step 2: Configure basic settings for each router.

You can copy and paste the following configurations into your routers to begin.

Router R1

```
enable
conf t
hostname R1
no ip domain lookup
banner motd #
****************************************************
*             UNAUTHORIZED ACCESS WARNING          *
*                                                  *
* This system is restricted to authorized users.   *
* All activity may be monitored and recorded.      *
* Unauthorized access is prohibited by law.        *
*                                                  *
* Lab: ISP BGP Core with Route Reflectors          *
* Owner: Hussain Ali                               *
****************************************************
#
interface Loopback0
ip address 1.1.1.1 255.255.255.255
```

```
no shut
exit
interface Ethernet0/0
ip address 10.0.12.1 255.255.255.252
no shut
exit
interface Ethernet0/1
ip address 10.0.13.1 255.255.255.252
no shut
exit
interface Ethernet0/2
ip address 172.16.16.1 255.255.255.252
no shut
exit
interface Ethernet0/3
ip address 10.0.15.1 255.255.255.252
no shut
exit
```

Router R2

```
enable
conf t
hostname R2
no ip domain lookup
banner motd #
****************************************************
*             UNAUTHORIZED ACCESS WARNING          *
*                                                  *
* This system is restricted to authorized users.   *
* All activity may be monitored and recorded.      *
* Unauthorized access is prohibited by law.        *
```

```
*                                                    *
* Lab: ISP BGP Core with Route Reflectors            *
* Owner: Hussain Ali                                 *
*****************************************************
#
interface Loopback0
ip address 2.2.2.2 255.255.255.255
 no shut
 exit
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.252
 no shut
 exit
interface Ethernet0/1
 ip address 10.0.24.1 255.255.255.252
 no shut
 exit
interface Ethernet0/2
 ip address 10.0.25.1 255.255.255.252
 no shut
 exit
interface Ethernet0/3
 ip address 172.16.27.1 255.255.255.252
 no shut
 exit
```

Router R3

```
enable
conf t
hostname R3
no ip domain lookup
```

```
banner motd #
***************************************************
*           UNAUTHORIZED ACCESS WARNING           *
*                                                 *
* This system is restricted to authorized users.  *
* All activity may be monitored and recorded.     *
* Unauthorized access is prohibited by law.       *
*                                                 *
* Lab: ISP BGP Core with Route Reflectors         *
* Owner: Hussain Ali                              *
***************************************************
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
 no shut
 exit
interface Ethernet0/0
 ip address 10.0.34.1 255.255.255.252
 no shut
 exit
interface Ethernet0/1
 ip address 10.0.13.2 255.255.255.252
 no shut
 exit
interface Ethernet0/3
 ip address 172.16.36.1 255.255.255.252
 no shut
 exit
interface Ethernet1/1
 ip address 10.0.35.1 255.255.255.252
```

```
 no shut
 exit
```

Router R4

```
enable
conf t
hostname R4
no ip domain lookup
banner motd #
****************************************************
*             UNAUTHORIZED ACCESS WARNING          *
*                                                  *
* This system is restricted to authorized users.   *
* All activity may be monitored and recorded.      *
* Unauthorized access is prohibited by law.        *
*                                                  *
* Lab: ISP BGP Core with Route Reflectors          *
* Owner: Hussain Ali                               *
****************************************************
#
interface Loopback0
ip address 4.4.4.4 255.255.255.255
 no shut
 exit
interface Ethernet0/0
 ip address 10.0.34.2 255.255.255.252
 no shut
 exit
interface Ethernet0/1
 ip address 10.0.24.2 255.255.255.252
 no shut
```

```
 exit
interface Ethernet0/2
 ip address 172.16.47.1 255.255.255.252
 no shut
 exit
interface Ethernet1/0
 ip address 10.0.45.1 255.255.255.252
 no shut
 exit
```

Router R5

```
enable
conf t
hostname R5
no ip domain lookup
banner motd #
****************************************************
*             UNAUTHORIZED ACCESS WARNING          *
*                                                  *
* This system is restricted to authorized users.   *
* All activity may be monitored and recorded.      *
* Unauthorized access is prohibited by law.        *
*                                                  *
* Lab: ISP BGP Core with Route Reflectors          *
* Owner: Hussain Ali                               *
****************************************************
#
interface Loopback0
ip address 5.5.5.5 255.255.255.255
 no shut
 exit
```

```
interface Ethernet0/2
 ip address 10.0.25.2 255.255.255.252
 no shut
 exit
interface Ethernet0/3
 ip address 10.0.15.2 255.255.255.252
 no shut
 exit
interface Ethernet1/0
 ip address 10.0.45.2 255.255.255.252
 no shut
 exit
interface Ethernet1/1
 ip address 10.0.35.2 255.255.255.252
 no shut
 exit
```

Router R6

```
enable
conf t
hostname R6
no ip domain lookup
banner motd #
****************************************************
*            UNAUTHORIZED ACCESS WARNING           *
*                                                  *
* This system is restricted to authorized users.   *
* All activity may be monitored and recorded.      *
* Unauthorized access is prohibited by law.        *
*                                                  *
* Lab: ISP BGP Core with Route Reflectors          *
```

```
* Owner: Hussain Ali                                 *
*****************************************************
#
interface Loopback0
ip address 60.60.60.1 255.255.255.0
 no shut
 exit
interface Ethernet0/2
 ip address 172.16.16.2 255.255.255.252
 no shut
 exit
interface Ethernet0/3
 ip address 172.16.36.2 255.255.255.252
 no shut
 exit
```

Router R7

```
enable
conf t
hostname R7
no ip domain lookup
banner motd #
*****************************************************
*             UNAUTHORIZED ACCESS WARNING           *
*                                                   *
* This system is restricted to authorized users.    *
* All activity may be monitored and recorded.       *
* Unauthorized access is prohibited by law.         *
*                                                   *
* Lab: ISP BGP Core with Route Reflectors           *
* Owner: Hussain Ali                                *
```

```
**************************************************
#
interface Loopback0
ip address 70.70.70.1 255.255.255.0
 no shut
 exit
interface Ethernet0/2
 ip address 172.16.47.2 255.255.255.252
 no shut
 exit
interface Ethernet0/3
 ip address 172.16.27.2 255.255.255.252
 no shut
 exit
```

Step 3: Configure OSPF

Configure OSPF between the R1, R2, R3, R4 and R5 routers and advertise directly connected networks and loopback 0

***Use route summarization to limit the network advertising**

```
R1(config)# router ospf 100
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
R1(config-router)# network 10.0.12.0 0.0.3.255 area 0
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
```

```
R2(config)# router ospf 100
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
R2(config-router)# network 10.0.0.0 0.0.31.255 area 0
R2(config-router)# network 2.2.2.2 0.0.0.0 area 0
```

```
R3(config)# router ospf 100
R3(config-router)# router-id 3.3.3.3
R3(config-router)# auto-cost reference-bandwidth 1000
R3(config-router)# network 10.0.0.0 0.0.63.255 area 0
R3(config-router)# network 3.3.3.3 0.0.0.0 area 0
```

```
R4(config)# router ospf 100
R4(config-router)# router-id 4.4.4.4
R4(config-router)# auto-cost reference-bandwidth 1000
R4(config-router)# network 10.0.0.0 0.0.63.255 area 0
R4(config-router)# network 4.4.4.4 0.0.0.0 area 0
```

```
R5(config)# router ospf 100
R5(config-router)# router-id 5.5.5.5
R5(config-router)# auto-cost reference-bandwidth 1000
R5(config-router)# network 10.0.0.0 0.0.63.255 area 0
R5(config-router)# network 5.5.5.5 0.0.0.0 area 0
```

In this step, OSPF is configured as the Interior Gateway Protocol inside AS100. OSPF is used to provide dynamic routing between all internal routers and to advertise loopback interfaces.

Each router is assigned a unique router ID to ensure stable identification in the OSPF domain. The reference bandwidth is adjusted to allow accurate cost calculation for high-speed links.

Network statements are configured using wildcard masks to enable OSPF on multiple interfaces and to summarize internal networks. Loopback interfaces are also advertised so that they can be reached by other routers.

In this lab, iBGP sessions use loopback interfaces instead of physical interfaces. Because loopbacks are not directly connected, routers cannot reach them without an IGP. OSPF provides this reachability.

By completing this step, all routers inside AS100 learn each other's internal and loopback networks. This creates the foundation required for stable iBGP operation.

Step 4: iBGP Configuration

Disable default bgp ipv4 unicast on R1, R2, R3, R4 and R5

no bgp default ipv4-unicast

Configure iBGP peering between R1, R2, R3, R4 and R5 inside AS 100 using loopback 0

```
R1(config)# router bgp 100
R1(config-router)# no bgp default ipv4-unicast
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# neighbor 5.5.5.5 remote-as 100
R1(config-router)# neighbor 5.5.5.5 update-source Loopback0
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 5.5.5.5 activate
```

```
R2(config)# router bgp 100
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# neighbor 5.5.5.5 remote-as 100
R2(config-router)# neighbor 5.5.5.5 update-source Loopback0
R2(config-router)# address-family ipv4 unicast
R2(config-router-af)# neighbor 5.5.5.5 activate
```

```
R3(config)# router bgp 100
R3(config-router)# no bgp default ipv4-unicast
R3(config-router)# bgp router-id 3.3.3.3
R3(config-router)# neighbor 5.5.5.5 remote-as 100
R3(config-router)# neighbor 5.5.5.5 update-source Loopback0
R3(config-router)# address-family ipv4 unicast
R3(config-router-af)# neighbor 5.5.5.5 activate
```

```
R4(config)# router bgp 100
R4(config-router)# no bgp default ipv4-unicast
R4(config-router)# bgp router-id 4.4.4.4
R4(config-router)# neighbor 5.5.5.5 remote-as 100
R4(config-router)# neighbor 5.5.5.5 update-source Loopback0
R4(config-router)# address-family ipv4 unicast
R4(config-router-af)# neighbor 5.5.5.5 activate
```

```
R5(config)# router bgp 100
R5(config-router)# no bgp default ipv4-unicast
R5(config-router)# bgp router-id 5.5.5.5
R5(config-router)# bgp cluster-id 5.5.5.5
R5(config-router)# neighbor 1.1.1.1 remote-as 100
R5(config-router)# neighbor 1.1.1.1 update-source Loopback0
R5(config-router)# neighbor 2.2.2.2 remote-as 100
R5(config-router)# neighbor 2.2.2.2 update-source Loopback0
R5(config-router)# neighbor 3.3.3.3 remote-as 100
R5(config-router)# neighbor 3.3.3.3 update-source Loopback0
R5(config-router)# neighbor 4.4.4.4 remote-as 100
R5(config-router)# neighbor 4.4.4.4 update-source Loopback0
R5(config-router)# address-family ipv4 unicast
R5(config-router-af)# neighbor 1.1.1.1 activate
R5(config-router-af)# neighbor 1.1.1.1 route-reflector-client
R5(config-router-af)# neighbor 2.2.2.2 activate
R5(config-router-af)# neighbor 2.2.2.2 route-reflector-client
R5(config-router-af)# neighbor 3.3.3.3 activate
R5(config-router-af)# neighbor 3.3.3.3 route-reflector-client
R5(config-router-af)# neighbor 4.4.4.4 activate
R5(config-router-af)# neighbor 4.4.4.4 route-reflector-client
```

In this step, iBGP is configured between all routers inside AS100 to exchange routing information within the ISP backbone.

Each router uses its loopback interface as the BGP source address. This improves session stability because loopback interfaces remain active even if physical links fail. The update-source Loopback0 command ensures that BGP sessions are established using these addresses.

The no bgp default ipv4-unicast command disables automatic IPv4 routing and requires manual activation under the address-family. This provides better control over which neighbors exchange routing information.

iBGP sessions are formed between routers R1–R4 and the route reflector R5. Instead of creating a full-mesh topology, all routers peer only with R5.

Router R5 is configured as a Route Reflector using the route-reflector-client command. This allows R5 to receive routes from one client and reflect them to other clients, reducing the number of required BGP sessions.

The bgp cluster-id command assigns R5 to a route reflector cluster. This prevents routing loops if multiple route reflectors exist in the network.

In this configuration, internal routers do not advertise their loopback addresses using the network command. Instead, routing information is learned dynamically through iBGP and route reflection.

The next-hop-self command is not configured at this stage because next-hop handling is managed later at the network edge during eBGP configuration.

After completing this step, iBGP connectivity is established inside AS100, and routing information can be distributed efficiently through the route reflector.

Step 5: EBGP Configuration

eBGP Configuration with AS1000 (R6)

```
R6(config)# router bgp 1000
R6(config-router)# no bgp default ipv4-unicast
R6(config-router)# bgp router-id 6.6.6.6
R6(config-router)# neighbor 172.16.16.1 remote-as 100
R6(config-router)# neighbor 172.16.36.1 remote-as 100
R6(config-router)# address-family ipv4 unicast
R6(config-router-af)# network 60.60.60.0 mask 255.255.255.0
R6(config-router-af)# neighbor 172.16.16.1 activate
R6(config-router-af)# neighbor 172.16.36.1 activate
```

```
R1(config)# router bgp 100
R1(config-router)# neighbor 172.16.16.2 remote-as 1000
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 172.16.16.2 activate
R1(config-router-af)# network 172.16.16.0 mask 255.255.255.252
R1(config-router-af)# neighbor 172.16.16.2 next-hop-self
```

```
R3(config)# router bgp 100
R3(config-router)# neighbor 172.16.36.2 remote-as 1000
R3(config-router)# address-family ipv4 unicast
R3(config-router-af)# neighbor 172.16.36.2 activate
R3(config-router-af)# network 172.16.36.0 mask 255.255.255.252
R3(config-router-af)# neighbor 172.16.36.2 next-hop-self
```

In this part, eBGP is configured between AS100 and the first customer network AS1000 using router R6.

Router R6 is assigned to AS1000 and establishes eBGP sessions with routers R1 and R3 in AS100. Because the routers belong to different autonomous systems, these sessions are formed using eBGP.

The neighbor command is used to define the external peering relationships and specify the remote autonomous system numbers. This allows the routers to recognize each other as valid BGP neighbors.

The network 60.60.60.0 command on R6 advertises the customer's internal network to the ISP. This makes the AS1000 prefix visible inside AS100.

On routers R1 and R3, the network command is used to advertise the directly connected customer links. This ensures that these interfaces are included in the BGP routing table and can be used for forwarding traffic.

The next-hop-self command is applied on R1 and R3 to change the next-hop address of customer routes to the local router. This is required because routes learned from eBGP are passed into iBGP without changing the next hop. Without this command, internal routers may not be able to reach the external next-hop address.

The IPv4 address family is activated to enable route exchange between peers.

After completing this part, AS100 learns the AS1000 customer network and distributes it internally through iBGP and the route reflector. This allows all internal routers and other customers to reach AS1000.

eBGP Configuration with AS2000 (R7)

```
R7(config)# router bgp 1000
R7(config-router)# no bgp default ipv4-unicast
R7(config-router)# bgp router-id 7.7.7.7
R7(config-router)# neighbor 172.16.27.1 remote-as 100
R7(config-router)# neighbor 172.16.47.1 remote-as 100
R7(config-router)# address-family ipv4 unicast
R7(config-router-af)# network 70.70.70.0 mask 255.255.255.0
R7(config-router-af)# neighbor 172.16.27.1 activate
R7(config-router-af)# neighbor 172.16.47.1 activate
```

```
R2(config)# router bgp 100
R2(config-router)# neighbor 172.16.27.2 remote-as 2000
R2(config-router)# address-family ipv4 unicast
R2(config-router-af)# neighbor 172.16.27.2 activate
R2(config-router-af)# network 172.16.27.0 mask 255.255.255.252
R2(config-router-af)# neighbor 172.16.27.2 next-hop-self
```

ISP BGP Core with Route Reflectors Lab

```
R4(config)# router bgp 100
R4(config-router)# neighbor 172.16.47.2 remote-as 2000
R4(config-router)# address-family ipv4 unicast
R4(config-router-af)# neighbor 172.16.47.2 activate
R4(config-router-af)# network 172.16.47.0 mask 255.255.255.252
R4(config-router-af)# neighbor 172.16.47.2 next-hop-self
```

In this part, eBGP is configured between AS100 and the second customer network AS2000 using router R7.

Router R7 is assigned to AS2000 and establishes eBGP sessions with routers R2 and R4 in AS100. These sessions enable routing information exchange between the customer and the ISP.

The neighbor command defines the external peering relationships and identifies the remote autonomous system numbers.

The network 70.70.70.0 command on R7 advertises the customer's internal network to AS100. This makes the AS2000 prefix available inside the ISP backbone.

On routers R2 and R4, the network command advertises the customer-facing links into BGP. This ensures that these interfaces are included in the routing table.

The next-hop-self command is configured on R2 and R4 to modify the next-hop attribute of external routes. This guarantees that internal routers can reach customer networks through the correct edge router.

Without this command, internal routers may receive routes with unreachable next-hop addresses, resulting in traffic loss.

The IPv4 address family is activated to enable routing updates.

After completing this part, AS100 learns the AS2000 customer network and distributes it throughout the backbone using iBGP and route reflection. This enables communication between AS2000, AS1000, and the ISP core.

Conclusion

In this lab, OSPF was used to provide internal reachability, iBGP with route reflection was implemented to distribute routing information efficiently, and eBGP was configured to connect external customer networks. The combination of these protocols allowed AS100 to operate as a scalable ISP backbone and provide end-to-end connectivity between multiple autonomous systems.

Verification and Testing

R6

```
R6#ping 70.70.70.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 70.70.70.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R6#traceroute 70.70.70.1
Type escape sequence to abort.
Tracing the route to 70.70.70.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.36.1 [AS 100] 1 msec 0 msec 1 msec
  2 10.0.34.2 0 msec 1 msec 1 msec
  3 172.16.47.2 [AS 100] 1 msec *  1 msec
```

R7

```
R7#ping 60.60.60.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.60.60.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R7#traceroute 60.60.60.1
Type escape sequence to abort.
Tracing the route to 60.60.60.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.47.1 [AS 100] 0 msec 1 msec 0 msec
  2 10.0.34.1 1 msec 0 msec 1 msec
  3 172.16.36.2 [AS 100] 1 msec *  1 msec
```