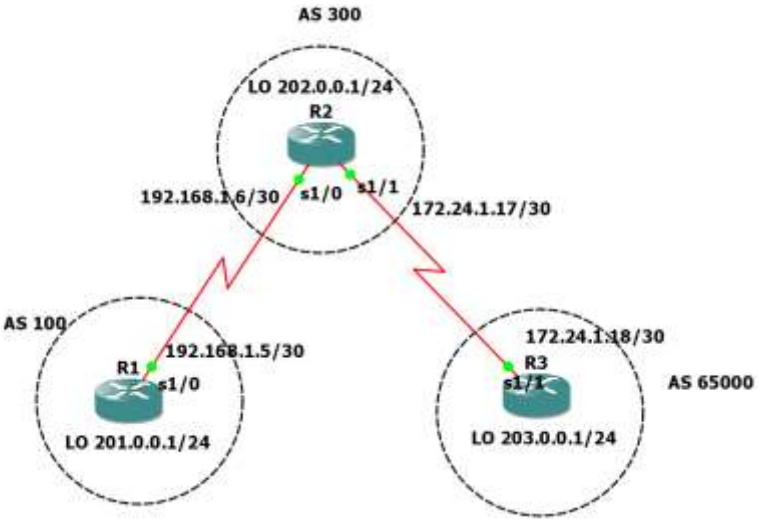
Practical No.2

Using the AS_PATH Attribute –



In this lab, the student will use BGP commands to prevent private AS numbers from being advertised to the outside world. The student will also use the AS_PATH attribute to filter BGP routes based on their source AS numbers.

Scenario

The International Travel Agency's Internet service provider ISP2 has been assigned an AS number of 300. This provider uses BGP to exchange routing information with several customer networks. Each customer network is assigned an AS number from the private range, such as AS 65000. Configure ISP2 to remove the private AS numbers within the AS_Path information from the CusRtr. In addition, Provider ISP2 would like to prevent its customer networks from receiving route information from International Travel Agency's AS 100. Use the AS_PATH attribute to implement this policy.

IP ADDRESS CONFIGURATION –

R1 Commands –

```
R1#Conf Term
R1(config)#INT S1/0
R1(config-if)#NO IP ADDRESS
R1(config-if)#IP ADDRESS 192.168.1.5 255.255.255.252
R1(config-if)#NO SHUT
R1(config-if)#EXIT
R1(config)#INT LO0
R1(config-if)#IP ADDRESS 201.0.0.1 255.255.255.0
R1(config-if)#NO SHUT
R1(config-if)#EXIT
```

R2 COMMANDS –

```
R2#CONF TERM
R2(config)#INT S1/0
R2(config-if)#IP ADDRESS 192.168.1.6 255.255.255.252
R2(config-if)#NO SHUT
R2(config-if)#EXIT
R2(config)#INT S1/1
R2(config-if)#IP ADDRESS 172.24.1.17 255.255.255.252
R2(config-if)#NO SHUT
```

R2(config-if)#EXIT
R2(config)#INT LO0
R2(config-if)#IP ADDRESS 202.0.0.1 255.255.255.0
R2(config-if)#NO SHUT
R2(config-if)#EXIT

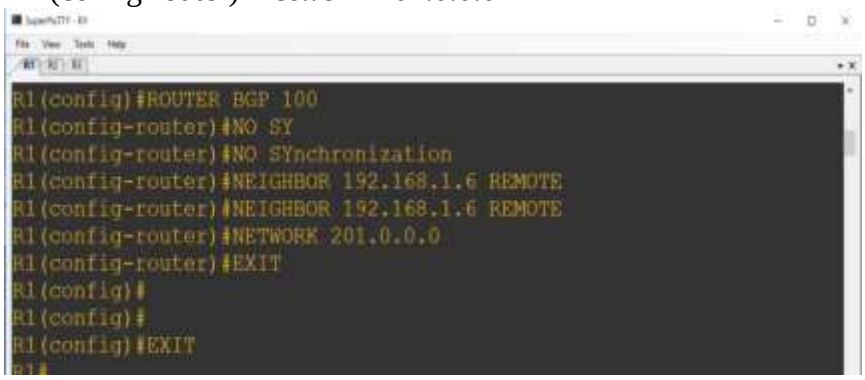
R3 COMMANDS –

R3#CONF TERM
R3(config)#INT S1/1
R3(config-if)#IP ADDRESS 172.24.1.18 255.255.255.252
R3(config-if)#NO SHUT
R3(config-if)#EXIT
R3(config)#
R3(config)#INT LO0
R3(config-if)#IP ADDRESS 203.0.0.1 255.255.255.0
R3(config-if)#NO SHUT
R3(config-if)#EXIT

Build and configure the network according to the diagram, but do not configure a routing protocol. Use **ping** to test connectivity between the directly connected routers.

Configure BGP for normal operation. Enter the appropriate BGP commands on each router so that they will identify their BGP neighbors and advertise their Ethernet networks –

R1 (config)#**router bgp 100**
R1 (config-router)#**no synchronization**
R1 (config-router)#**neighbor 192.168.1.6 remote-as 300**
R1 (config-router)#**network 201.0.0.0**

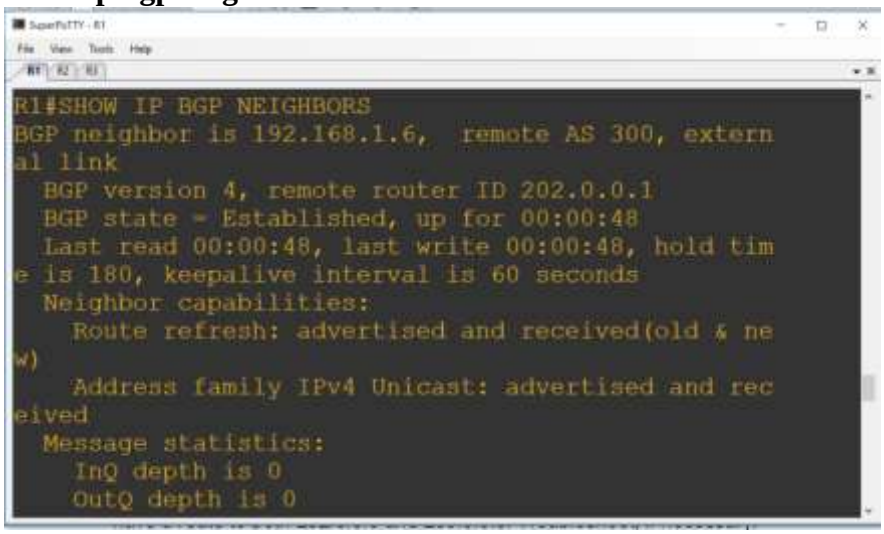


R2 (config)#**router bgp 300**
R2(config-router)#**no synchronization**
R2 (config-router)#**neighbor 192.168.1.5 remote-as 100**
R2 (config-router)#**neighbor 172.24.1.18 remote-as 65000**
R2 (config-router)#**network 202.0.0.0**

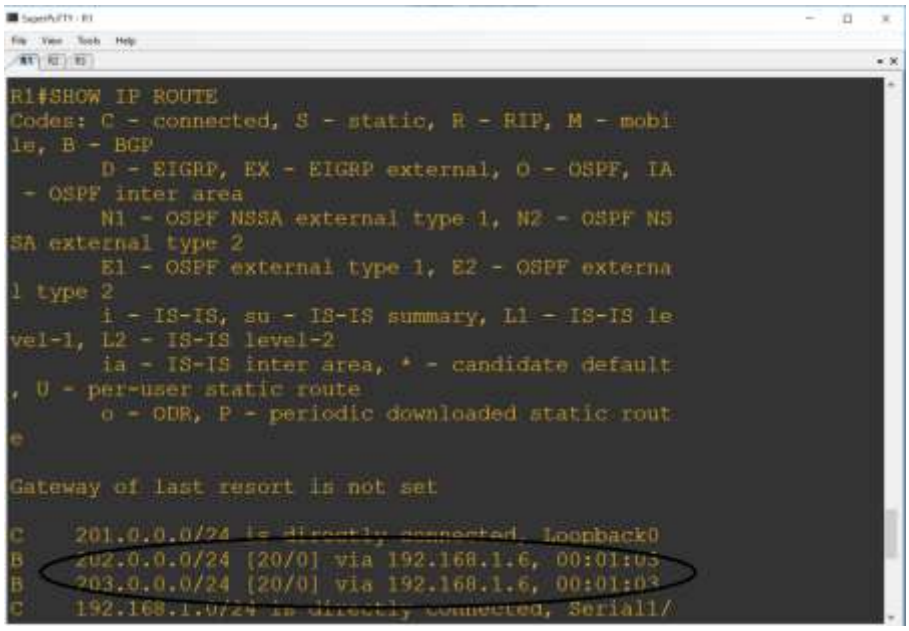
R3 (config)#**router bgp 65000**
R3 (config-router)#**no synchronization**
R3 (config-router)#**neighbor 172.24.1.17 remote-as 300**
R3 (config-router)#**network 203.0.0.0**

Verify that these routers have established the appropriate neighbor relationships by issuing the

Show ip bgp neighbors command at each router.



Check the routing table from R1 by using the **show ip route** command. R1 should have a route to both 202.0.0.0 and 203.0.0.0.



Check the BGP table from R1 by using the **show ip bgp** command. Note the AS path for the 203.0.0.0 network. The AS 65000 should be listed in the path to 203.0.0.0.

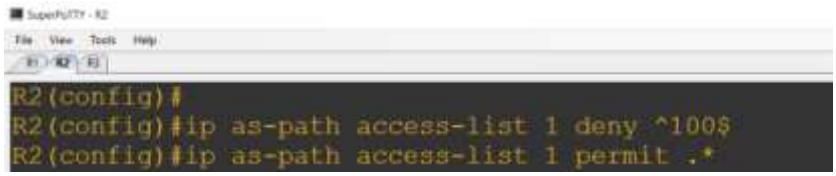
Configure R2 to strip the private AS numbers from BGP routes exchanged with R1. Use the following commands:
R2(config)#**router bgp 300**
R2(config-router)#**neighbor 192.168.1.5 remove-private-as**

After issuing these commands, use the **clear ip bgp *** command on R1 to re-establish the BGP relationships between the three routers.

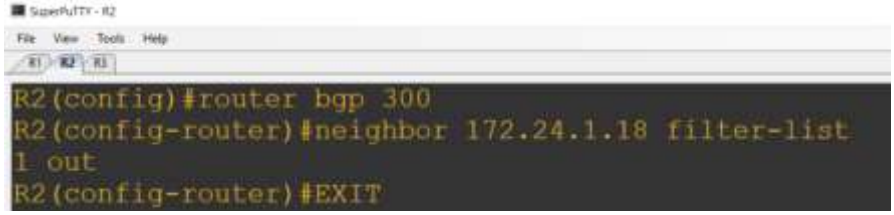
Wait several seconds, and then return to R1 to check its routing table.
R1 should be able to ping 203.0.0.0.
Now check the BGP table on R1. The AS_PATH to the 203.0.0.0 network should be AS 300.

As a final configuration, use the AS_PATH attribute to filter routes based on their origin. In a complex environment, this attribute can be used to enforce routing policy. In this case, the provider router R2, must be configured so that it does not propagate routes that originate from AS 100 to the customer router, R3.
First, configure a special kind of access list to match BGP routes with an AS_PATH attribute that both begins and ends with the number 100. Enter the following commands on R2:

R2(config)#**ip as-path access-list 1 deny ^100$**
R2(config)#**ip as-path access-list 1 permit .***



Now that the access list has been configured, apply it as follows:
R2(config)#**router bgp 300**
R2(config-router)#**neighbor 172.24.1.18 filter-list 1 out**



The **out** keyword specifies that the list should be applied to routing information sent to this neighbor.
Use the **clear ip bgp *** command to reset the routing information. Wait several seconds, and then check the routing table for R2. The route to 201.0.0.0 should be in the routing table.
Check the routing table for R3. It should not have a route to 201.0.0.0 in its routing table.

Return to R2 and verify that the filter is working as intended. Issue the command **show ip bgp regexp ^100$**.
The output of this command shows all matches for the regular expressions that were used in the access list. The path to 201.0.0.0 matches the access list and is filtered out of updates to R3.