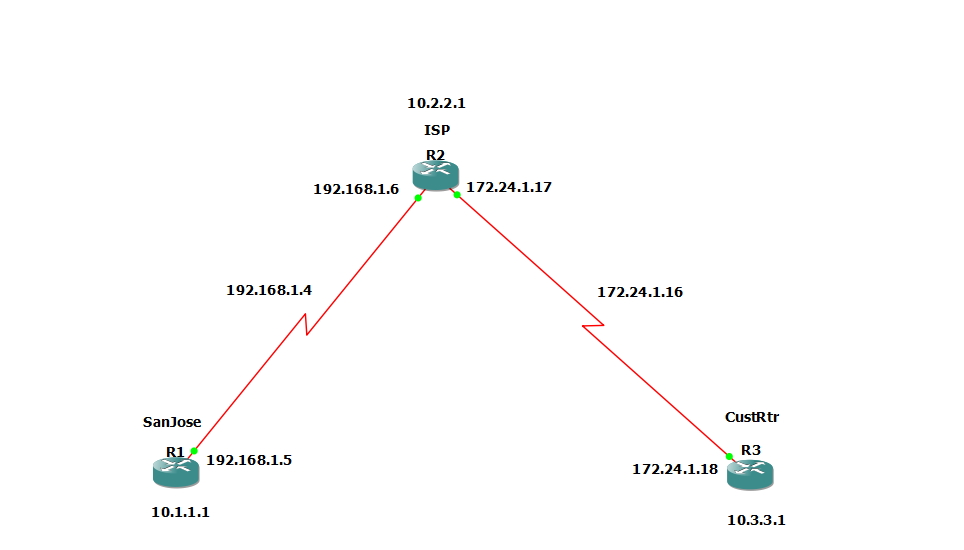
**Practical 2**

**Aim:- Using the AS\_PATH Attribute**

**Topology:-**



**Step 1:- Prepare the routers for the lab.**

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations.

**Step 2:- Configure the hostname and interface addresses.**

1. Enter the following configurations into your routers to begin.

**Router R1 (hostname SanJose)**

Conf t

hostname SanJose

interface Loopback0

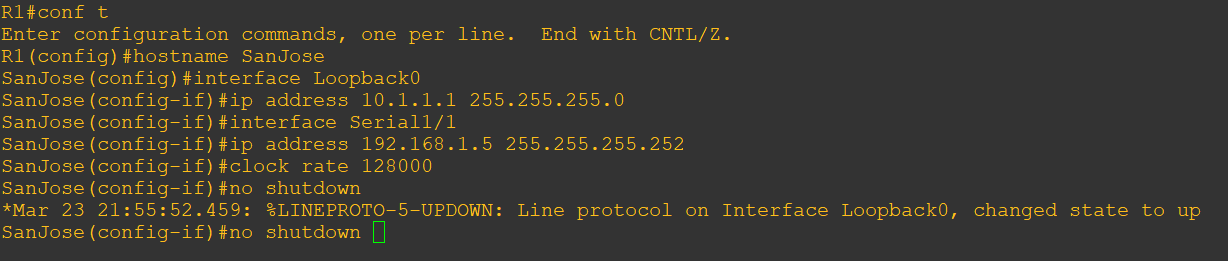
ip address 10.1.1.1 255.255.255.0

interface Serial1/1

ip address 192.168.1.5 255.255.255.252

clock rate 128000

no shutdown



**Router R2 (hostname ISP)**

Conf t

hostname ISP

interface Loopback0

ip address 10.2.2.1 255.255.255.0

interface Serial1/1

ip address 192.168.1.6 255.255.255.252

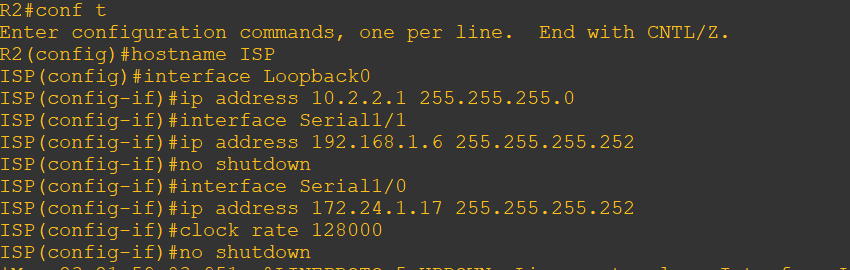
no shutdown

interface Serial1/0

ip address 172.24.1.17 255.255.255.252

clock rate 128000

no shutdown



**Router R3 (hostname CustRtr)**

Conf t

hostname CustRtr

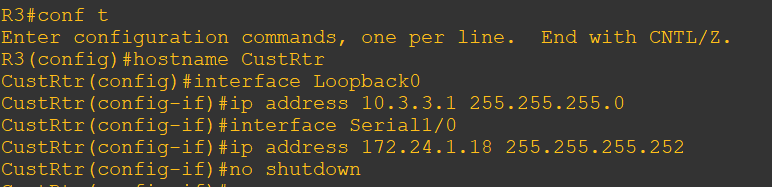
interface Loopback0

ip address 10.3.3.1 255.255.255.0

interface Serial1/0

ip address 172.24.1.18 255.255.255.252

no shutdown



b)Use ping to test the connectivity between the directly connected routers.

Note:- SanJose will not be able to reach either ISP’s loopback (10.2.2.1) or CustRtr’s loopback (10.3.3.1), nor will it be able to reach either end of the link joining ISP or CustRtr (172.24.1.17 or 172.24.1.18).

Step 3:- Configure BGP

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

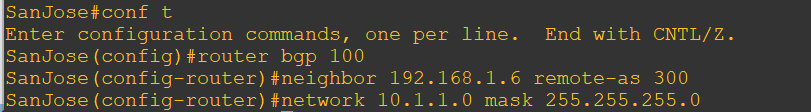
**Router R1 (hostname SanJose)**

Conf t

router bgp 100

neighbor 192.168.1.6 remote-as 300

network 10.1.1.0 mask 255.255.255.0



**Router R2 (hostname ISP)**

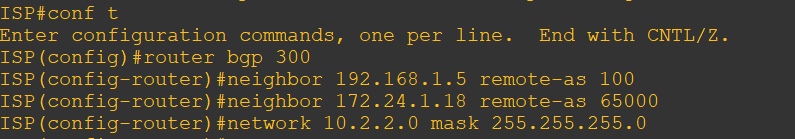
Conf t

router bgp 300

neighbor 192.168.1.5 remote-as 100

neighbor 172.24.1.18 remote-as 65000

network 10.2.2.0 mask 255.255.255.0



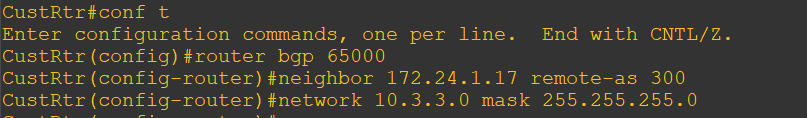
**Router R3 (hostname CustRtr)**

Conf t

router bgp 65000

neighbor 172.24.1.17 remote-as 300

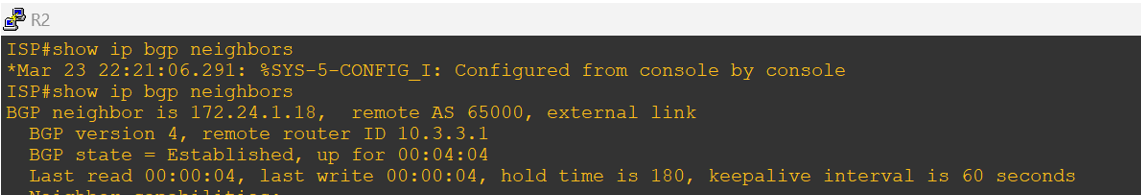
network 10.3.3.0 mask 255.255.255.0



b)Verify that these routers have established the appropriate neighbor relationships by issuing the show ip bgp neighbors command on each router.

Router R2 (hostname ISP)

show ip bgp neighbors



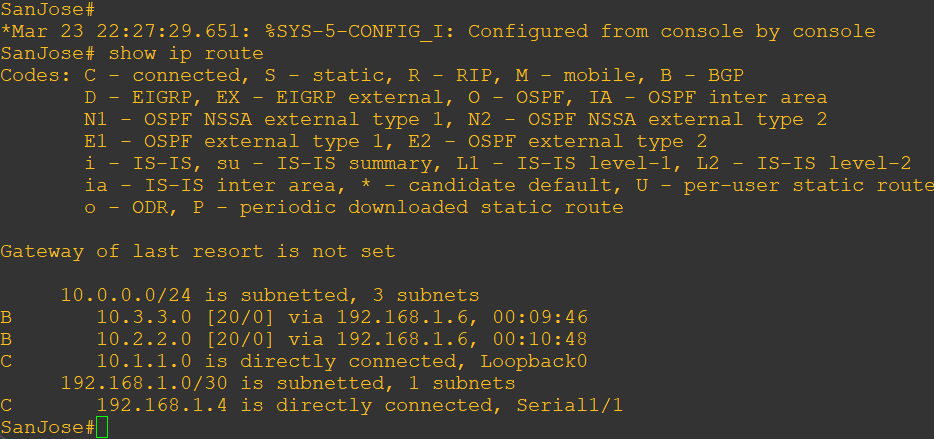
One more neighbour will get is 192.168.1.5

Step 4:- Remove the private AS.

1. Display the SanJose routing table using the show ip route command. SanJose should have a route to both 10.2.2.0 and 10.3.3.0. Troubleshoot if necessary.

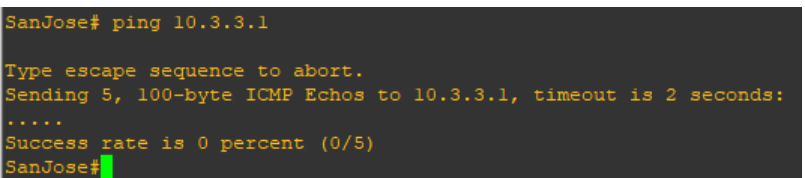
Router R1 (hostname SanJose)

show ip route



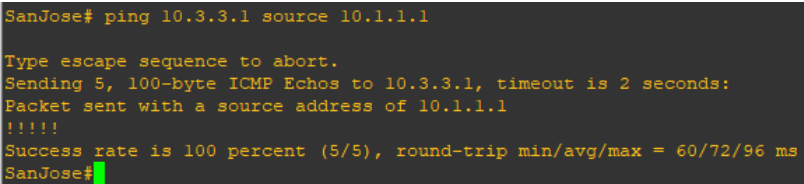
b)Ping the 10.3.3.1 address from the SanJose.

ping 10.3.3.1



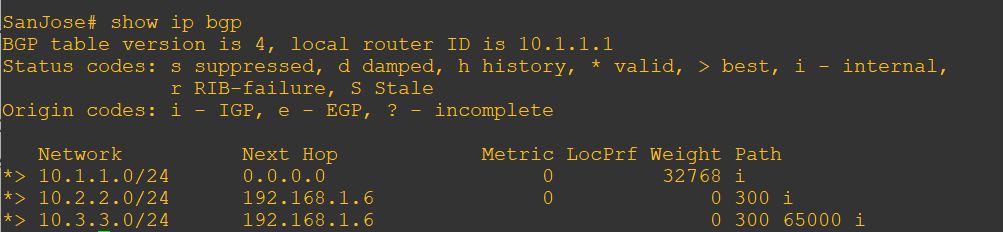
c)Ping again, this time as an extended ping, sourcing from the Loopback0 interface address.

ping 10.3.3.1 source 10.1.1.1

****

d) Check the BGP table from SanJose by using the show ip bgp command. Note the AS path for the 10.3.3.0 network. The AS 65000 should be listed in the path to 10.3.3.0.

show ip bgp



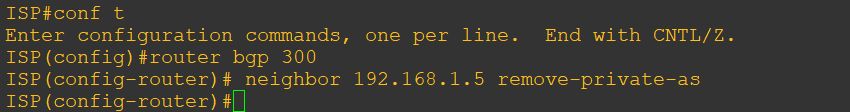
e) Configure ISP to strip the private AS numbers from BGP routes exchanged with SanJose using the following commands.

Router R2 (hostname ISP)

Conf t

router bgp 300

neighbor 192.168.1.5 remove-private-as

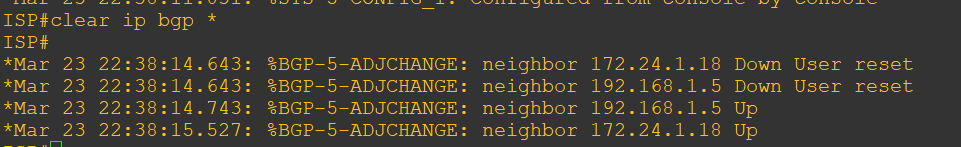


f) After issuing these commands, use the clear ip bgp \* command on ISP to re-establish the BGP relationship between the three routers. Wait several seconds and then return to SanJose to check its routing table.

Note:- The **clear ip bgp \*** soft command can also be used to force each router to resend its BGP table.

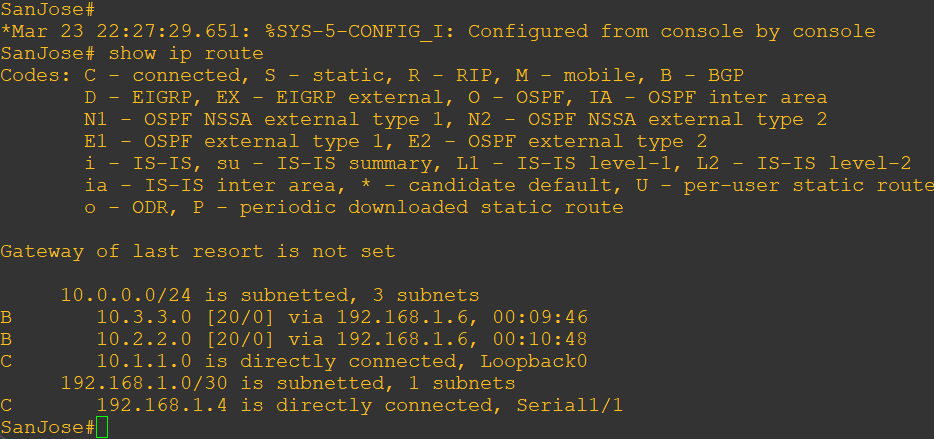
**Router R2 (hostname ISP)**

clear ip bgp \*



**Router R1 (hostname SanJose)**

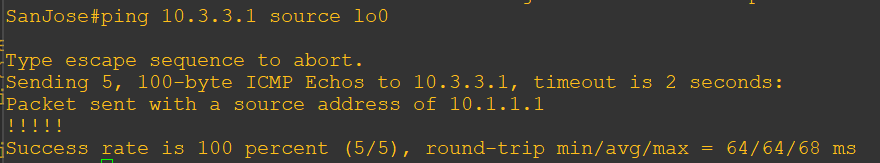
show ip route



SanJose should be able to ping 10.3.3.1 using its loopback0 interface as the source of the ping.

**Router R1 (hostname SanJose)**

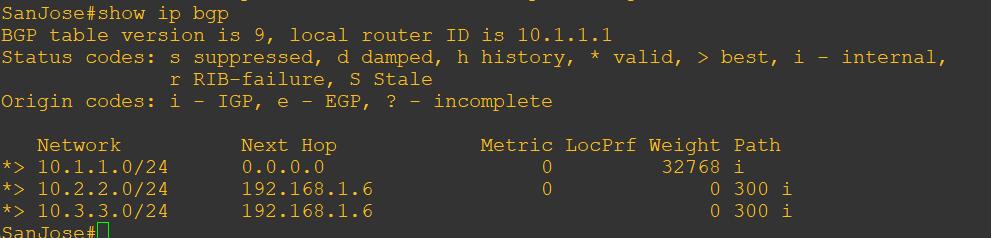
ping 10.3.3.1 source 10.1.1.1 / ping 10.3.3.1 source lo0



g) Now check the BGP table on SanJose. The AS\_PATH to the 10.3.3.0 network should be AS 300. It no longer has the private AS in the path.

**Router R1 (hostname SanJose)**

show ip bgp



**Step 5:- Use the AS\_PATH attribute to filter routes.**

As a final configuration, use the AS\_PATH attribute to filter routes based on their origin. In a complex environment, you can use this attribute to enforce routing policy. In this case, the provider router, ISP, must be configured so that it does not propagate routes that originate from AS 100 to the customer router CustRtr.

AS-path access lists are read like regular access lists. The statements are read sequentially, and there is an implicit deny at the end. Rather than matching an address in each statement like a conventional access list, AS path access lists match on something called a regular expression. Regular expressions are a way of matching text patterns and have many uses. In this case, you will be using them in the AS path access list to match text patterns in AS paths.

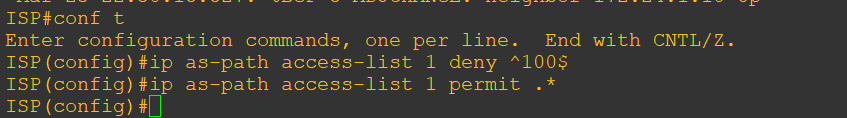
a) Configure a special kind of access list to match BGP routes with an AS\_PATH attribute that both begins and ends with the number 100. Enter the following commands on ISP.

**Router R2 (hostname ISP)**

conf t

ip as-path access-list 1 deny ^100$

ip as-path access-list 1 permit .\*



The first command uses the ^ character to indicate that the AS path must begin with the given number 100. The $ character indicates that the AS\_PATH attribute must also end with 100. Essentially, this statement matches only paths that are sourced from AS 100. Other paths, which might include AS 100 along the way, will not match this list.

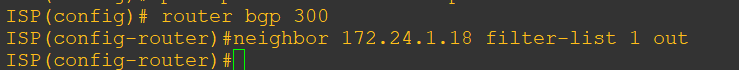
In the second statement, the . (period) is a wildcard, and the \* (asterisk) stands for a repetition of the wildcard. Together, .\* matches any value of the AS\_PATH attribute, which in effect permits any update that has not been denied by the previous access-list statement.

1. Apply the configured access list using the neighbor command with filter-list option.

**Router R2 (hostname ISP)**

router bgp 300

neighbor 172.24.1.18 filter-list 1 out



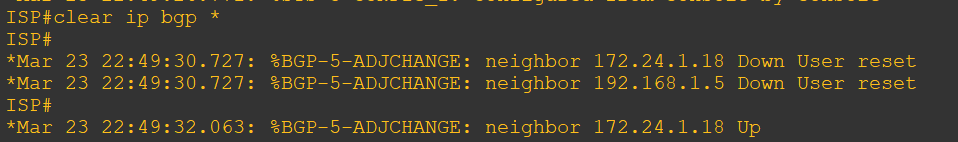
The out keyword specifies that the list is applied to routing information sent to this neighbor.

c) Use the **clear ip bgp \*** command to reset the routing information. Wait several seconds and then check the routing table for ISP. The route to 10.1.1.0 should be in the routing table.

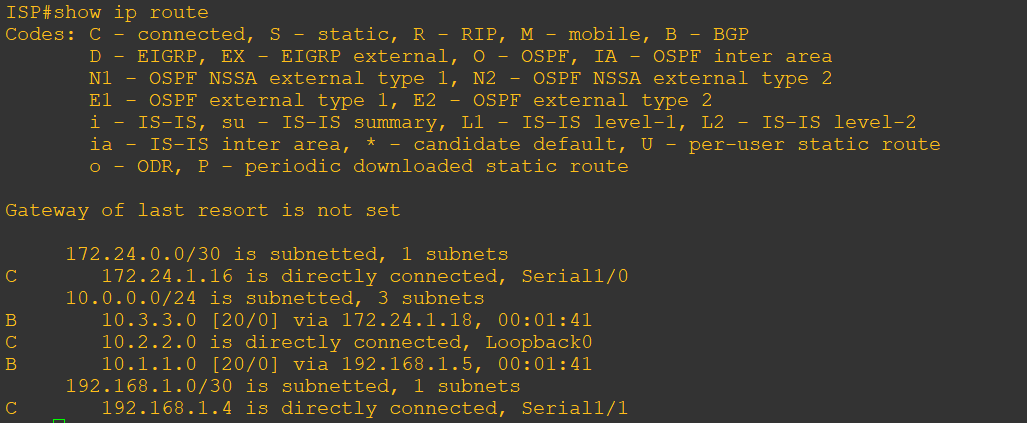
Note:- To force the local router to resend its BGP table, a less disruptive option is to use the clear ip bgp \* out or clear ip bgp \* soft command (the second command performs both outgoing and incoming route resync).

**Router R2 (hostname ISP)**

clear ip bgp \*



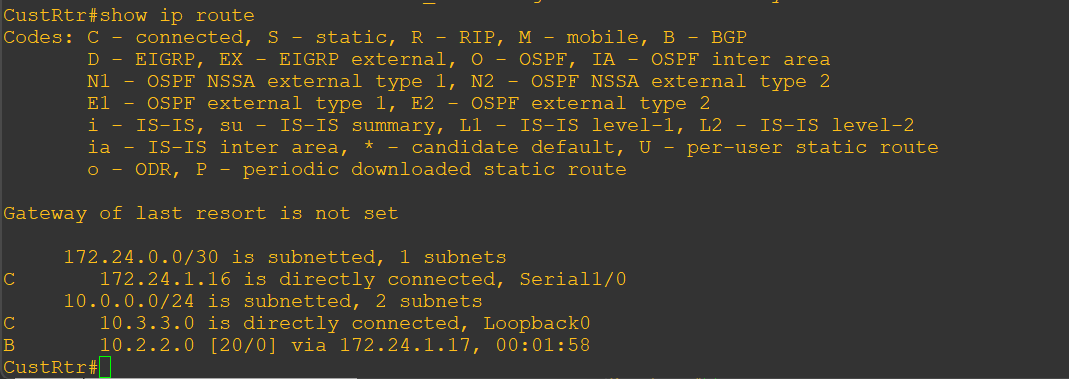
show ip route



d) Check the routing table for CustRtr. It should not have a route to 10.1.1.0 in its routing table.

Router R3 (hostname CustRtr)

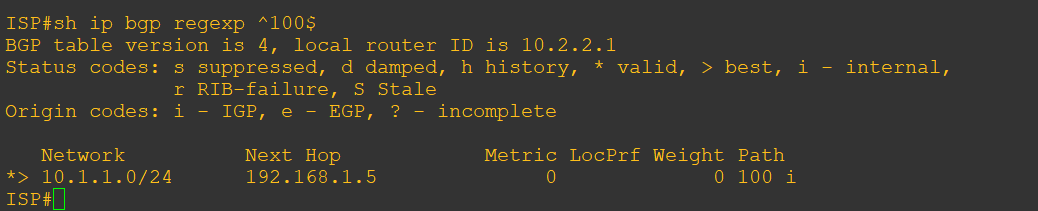
show ip route



e) Return to ISP and verify that the filter is working as intended. Issue the show ip bgp regexp ^100$ command.

**Router R2 (hostname ISP)**

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 10.1.1.0 matches the access list and is filtered from updates to CustRtr.

f) Run the following Tcl script on all routers to verify whether there is connectivity. All pings from ISP should be successful. SanJose should not be able to ping the CustRtr loopback 10.3.3.1 or the WAN link 172.24.1.16/30. CustRtr should not be able to ping the SanJose loopback 10.1.1.1 or the WAN link 192.168.1.4/30.

**Router R2 (hostname ISP)**

tclsh

foreach address {

10.1.1.1

10.2.2.1

10.3.3.1

192.168.1.5

192.168.1.6

172.24.1.17

172.24.1.18

} { Ping $address }

