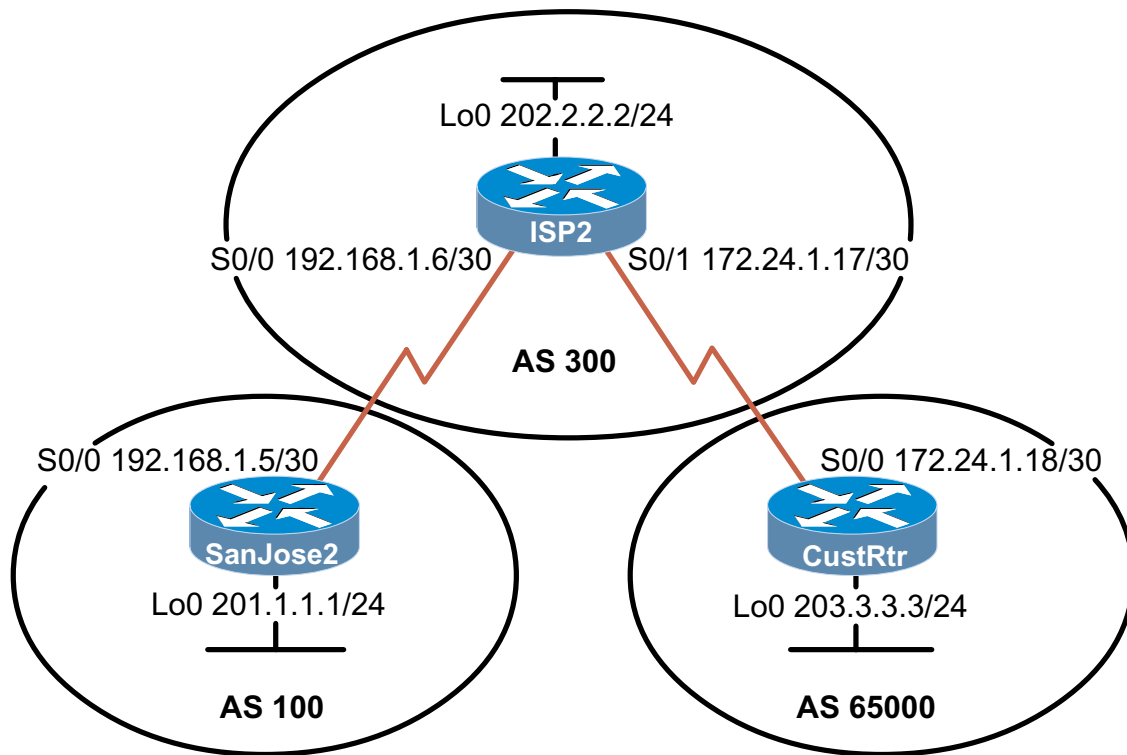


8.8.3 Using the AS_PATH Attribute



Objective

In this lab, you use BGP commands to prevent private AS numbers from being advertised to the outside world. You 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. Before leaving the provider's network, these private AS numbers must be stripped from the AS_PATH information. You are asked to configure this. In addition, Provider ISP2 would like to prevent its customer networks from receiving route information from International Travel Agency's AS 100. You need to use the AS_PATH attribute to implement this policy.

Step 1

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.

Note: SanJose2 will not be able to reach ISP2's customer network, CustRtr.

Step 2

Configure BGP for normal operation. Enter the appropriate BGP commands on each router so that they advertise their Ethernet networks:

```
SanJose2(config)#router bgp 100
SanJose2(config-router)#no synchronization
SanJose2(config-router)#neighbor 192.168.1.6 remote-as 300
SanJose2(config-router)#network 201.1.1.0

ISP2(config)#router bgp 300
ISP2(config-router)#no synchronization
ISP2(config-router)#neighbor 192.168.1.5 remote-as 100
ISP2(config-router)#neighbor 172.24.1.18 remote-as 65000
ISP2(config-router)#network 202.2.2.0

CustRtr(config)#router bgp 65000
CustRtr(config-router)#no synchronization
CustRtr(config-router)#neighbor 172.24.1.17 remote-as 300
CustRtr(config-router)#network 203.3.3.0
```

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

Step 3

Check SanJose2's routing table by using the **show ip route** command. SanJose2 should have a route to both 202.2.2.0 and 203.3.3.0. Troubleshoot, if necessary.

Check SanJose2's BGP table by using the **show ip bgp** command. Note the AS path for the 203.3.3.0 network. The AS 65000 should be listed in the path to 203.3.3.0. Why is this a problem?

Configure ISP2 to strip the private AS numbers from BGP routes exchanged with SanJose2. Use the following commands:

```
ISP2(config)#router bgp 300
ISP2(config-router)#neighbor 192.168.1.5 remove-private-as
```

After you issue these commands, use the **clear ip bgp *** command on SanJose2 to reestablish the BGP relationships between the three routers.

Wait several seconds, and then return to SanJose2 to check its routing table.

1. Does SanJose2 still have a route to 203.3.3.0?

SanJose2 should be able to ping 203.3.3.3.

Now check SanJose2's BGP table. The AS_PATH to the 203.3.3.0 network should be AS 300.

Step 4

As a final configuration, you 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, you must configure Provider ISP2 so that its router (ISP2) does not propagate routes that originate from AS 100 to the customer router (CustRtr).

First, you must 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 ISP2:

```
ISP2(config)#ip as-path access-list 1 deny ^100$
ISP2(config)#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 . character is a wildcard, and the * symbol 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.

Now that you configured the access list, apply it to the appropriate neighbor (CustRtr):

```
ISP2(config)#router bgp 300
ISP2(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 ISP2's routing table. The route to 201.1.1.0 should be in the routing table.

Check CustRtr's routing table. It should not have a route to 201.1.1.0 in its routing table.

Return to ISP2 and verify that your filter is working as intended. Issue the command **show ip bgp regexp ^100\$**.

The output of this command shows all matches for the regular expression that you used in your access list. The path to 201.1.1.0 matches the access list and is filtered out of updates to CustRtr.