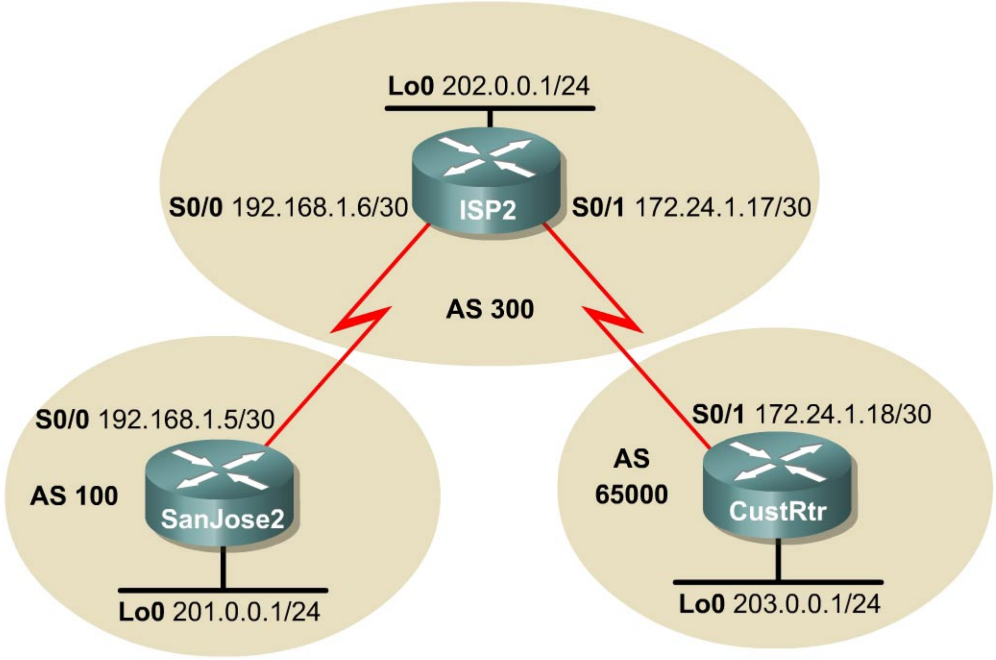
Lab 9.11.3 Using the AS_PATH Attribute



Objective

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.

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 the customer network for ISP2, CustRtr. It will not be able to reach it by the IP address in the link leading to the CustRtr, nor the loopback interface, 202.0.0.1/24.

Step 2

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:

```
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 201.0.0.0

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 202.0.0.0

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 203.0.0.0
```

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

Step 3

Check the routing table from SanJose2 by using the **`show ip route`** command. SanJose2 should have a route to both 202.0.0.0 and 203.0.0.0. Troubleshoot, if necessary.

1. Can the SanJose2 router be pinged to the 203.0.0.0 /24 network off of CustRtr?

   ____

2. A ping should not be successful when issuing just a standard **`ping`**. Why is this the case?

   ____

Try the **`ping`** again, this time as an extended **`ping`**, sourcing from the Loopback 0 interface as follows:

```
SanJose2#ping
Protocol [ip]:
Target IP address: 203.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 201.0.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

Check the BGP table from SanJose2 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. Why is this a problem?

```
BGP table version is 4, local router ID is 201.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal   Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 201.0.0.0        0.0.0.0                  0         32768 i
*> 202.0.0.0        192.168.1.6              0             0 300 i
*> 203.0.0.0        192.168.1.6                            0 300 65000 i
```

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 issuing these commands, use the **`clear ip bgp *`** command on SanJose2 to re-establish the BGP relationships between the three routers.

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

3. Does SanJose2 still have a route to 203.0.0.0?

____

SanJose2 should be able to ping 203.0.0.0.

Now check the BGP table on SanJose2. The AS_PATH to the 203.0.0.0 network should be AS 300.

```
BGP table version is 8, local router ID is 201.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal   Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 201.0.0.0        0.0.0.0                  0         32768 i
*> 202.0.0.0        192.168.1.6              0             0 300 i
*> 203.0.0.0        192.168.1.6                            0 300 i
```

Step 4

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, ISP2, must be configured so that it does not propagate routes that originate from AS 100 to the customer router, CustRtr.

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 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 the access list has been configured, apply it as follows:

```
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 the routing table for ISP2. The route to 201.0.0.0 should be in the routing table.

Check the routing table for CustRtr. It should not have a route to 201.0.0.0 in its routing table.

Return to ISP2 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 CustRtr.

```
ISP2#show ip bgp regexp ^100$
BGP table version is 4, local router ID is 202.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 201.0.0.0        192.168.1.5              0             0 100 i
```