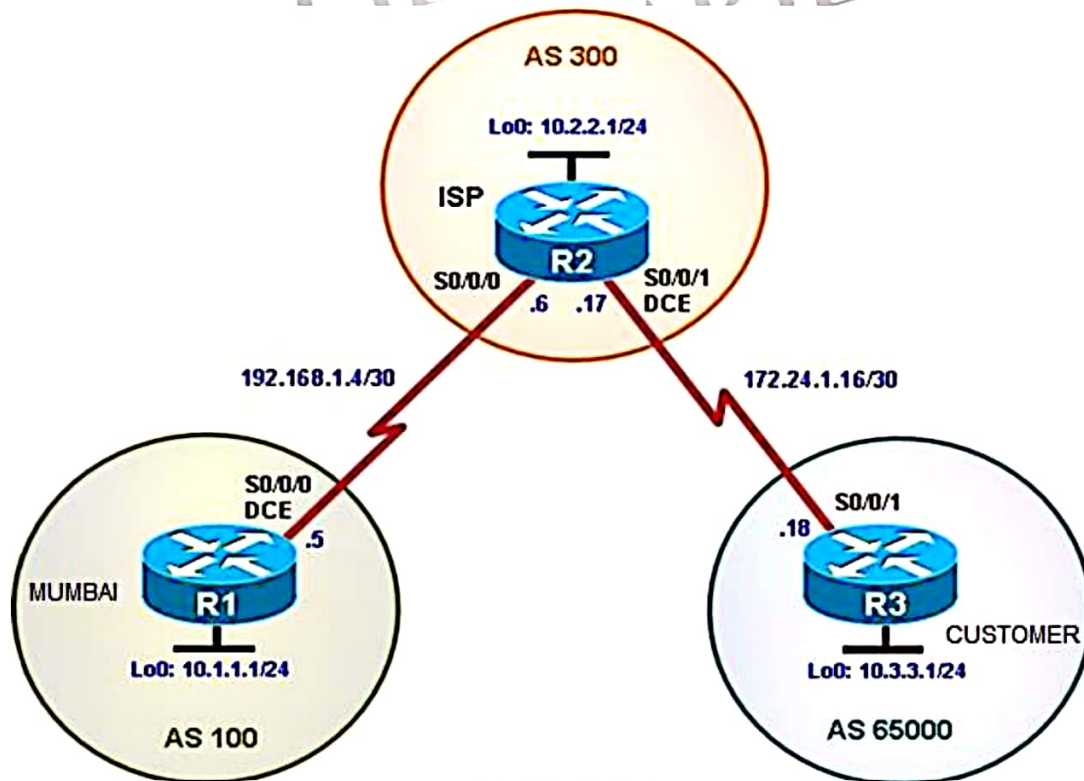


PRACTICAL NO. 2

Aim: Using the AS_PATH Attribute



Objectives

- Use BGP commands to prevent private AS numbers from being advertised to the outside world.
- Use the AS_PATH attribute to filter BGP routes based on their source AS numbers.

Background

The International Travel Agency's ISP 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 the ISP router to remove the private AS numbers from the AS Path information of Customer. In addition, the ISP 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.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. You can use other routers (such as 2801 or 2811) and Cisco IOS Software versions, if they have comparable capabilities and features. Depending

Mr. Chayan Bhattacharjee

on the router model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

Step 1: Prepare the routers for the lab. Cable the network as shown in the topology diagram.

Step 2: Configure the hostname and interface addresses and use **ping** command to test connectivity.

Router R1 (hostname Mumbai)

```
hostname Mumbai
```

```
interface Loopback0
ip address 10.1.1.1 255.255.255.0
interface Serial0/0/0
ip address 192.168.1.5 255.255.255.252
clock rate 128000
no shutdown
```

Router R2 (hostname ISP)

```
hostname ISP
```

```
interface Loopback0
ip address 10.2.2.1 255.255.255.0
interface Serial0/0/0
ip address 192.168.1.6 255.255.255.252
no shutdown
interface Serial0/0/1
ip address 172.24.1.17 255.255.255.252
clock rate 128000
no shutdown
```

Router R3 (hostname Customer)

```
hostname Customer

interface Loopback0
ip address 10.3.3.1 255.255.255.0
interface Serial0/0/1
ip address 172.24.1.18 255.255.255.252
no shutdown
```

Note: Mumbai will not be able to reach either ISP's loopback (10.2.2.1) or Customer's loopback (10.3.3.1), nor will it be able to reach either end of the link joining ISP to Customer (172.24.1.17 and 172.24.1.18).

Step 3: Configure BGP.

- a. 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.

```
Mumbai(config)# router bgp 100
Mumbai(config-router)# neighbor 192.168.1.6 remote-as 300
Mumbai(config-router)# network 10.1.1.0 mask 255.255.255.0
```

```
ISP(config)# router bgp 300
ISP(config-router)# neighbor 192.168.1.5 remote-as 100
ISP(config-router)# neighbor 172.24.1.18 remote-as 65000
ISP(config-router)# network 10.2.2.0 mask 255.255.255.0
```

```
Customer(config)# router bgp 65000
Customer(config-router)# neighbor 172.24.1.17 remote-as 300
Customer(config-router)# 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.

```
ISP# show ip bgp neighbors
```

```
BGP neighbor is 172.24.1.18, remote AS 65000, external link BGP  
version 4, remote router ID 10.3.3.1
```

```
BGP state = Established, up for 00:02:05
```

```
<output omitted>
```

```
BGP neighbor is 192.168.1.5, remote AS 100, external link BGP  
version 4, remote router ID 10.1.1.1
```

```
BGP state = Established, up for 00:04:19
```

```
<output omitted>
```

Step 4: Remove the private AS.

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

```
Mumbai# show ip route
```

```
*Mar 25 22:00:37.367: %SYS-5-CONFIG-I: Configured from console by  
console
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B -BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS  
level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user  
static route
```

```
o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/24 is subnetted, 3 subnets
```

B 10.3.3.0 [20/0] via 192.168.1.6,00:01:11
B 10.2.2.0 [20/0] via 192.168.1.6,00:02:16
C 10.1.1.0 is directly connected,Loopback0 192.168.1.0/30 is
subnetted, 1subnets
C 192.168.1.4 is directly connected,Serial0/0/0

- b. Ping the 10.3.3.1 address from Mumbai. Why does this fail?
- c. Ping again, this time as an extended ping, sourcing from the Loopback0 interface address.

```
Mumbai# ping
Protocol [ip]:
Target IP address: 10.3.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
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 10.3.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68
ms
```

Note: You can bypass extended ping mode and specify a source address using one of these commands:

```
Mumbai# ping 10.3.3.1 source 10.1.1.1
```

or

```
Mumbai# ping 10.3.3.1 source Lo0
```

- d. Check the BGP table from Mumbai 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.

Mumbai# show ip bgp

BGP table version is 5, local router ID is 10.1.1.1

Status codes: s suppressed, d damped, h history, * valid, > best, i-internal
Origin codes: i - IGP, e - EGP, ? -incomplete

Network	NextHop	Metric	LocPrf	WeightPath
*>10.1.1.0	0.0.0.0	0	32768 i	
*>10.2.2.0	192.168.1.6	0	0 300 i	
*>10.3.3.0	192.168.1.6	0	300 65000 i	

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

ISP(config)# router bgp 300

ISP(config-router)# 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 Mumbai 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.

Does Mumbai still have a route to 10.3.3.0?

Mumbai should be able to ping 10.3.3.1 using its loopback 0 interface as the source of the ping.

Mumbai# ping 10.3.3.1 source lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.1

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

g. Now check the BGP table on Mumbai. The AS_PATH to the 10.3.3.0 network should be AS 300.

It no longer has the private AS in the path.

Mumbai# show ip bgp

BGP table version is 8, local router ID is 10.1.1.1

Status codes: s suppressed, d damped, h history, * valid, > best, i-internal
Origin codes: i - IGP, e - EGP, ? -incomplete

Network	NextHop	Metric	LocPrf	Weight	Path
*>10.1.1.0	0.0.0.0	0	32768	i	
*>10.2.2.0	192.168.1.6	0	0	300i	
*>10.3.3.0	192.168.1.6	0	300i		

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 Customer.

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.

- 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.

```
ISP(config)# ip as-path access-list 1 deny ^100$
```

```
ISP(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 . (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^[2].

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

```
ISP(config)# router bgp 300
```

```
ISP(config-router)# 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).

```
ISP# show ip route
```

```
<output omitted>
```

```
172.24.0.0/30 is subnetted, 1 subnets
```

```
C      172.24.1.16 is directly connected, Serial0/0/1 10.0.0.0/24
      is subnetted, 3 subnets
```

```
B      10.3.3.0 [20/0] via 172.24.1.18, 00:07:34
```

```
C      10.2.2.0 is directly connected, Loopback0
```

```
B      10.1.1.0 [20/0] via 192.168.1.5, 00:10:53
```

```
      192.168.1.0/30 is subnetted, 1 subnets
```

```
C      192.168.1.4 is directly connected, Serial0/0/0
```

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

```
Customer# show ip route
```

```
<output omitted>
```

172.24.0.0/30 is subnetted, 1 subnets

C 172.24.1.16 is directly connected, Serial0/0/1 10.0.0.0/24 is subnetted, 2 subnets

C 10.3.3.0 is directly connected, Loopback0

B 10.2.2.0 [20/0] via 172.24.1.17, 00:11:57

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

ISP# show ip bgp regexp ^100\$

BGP table version is 4, local router ID is 10.2.2.1

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
*>10.1.1.0	192.168.1.5	0	0	100	i

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 Customer.

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

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 }
```

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than list all combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. For example, for an ISDN BRI interface, the string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Reference:

- ➔ http://www.configrouter.com/ccnp-route-lab-using-as_path-attribute-10644/
- ➔ More details on configuring regular expressions on Cisco routers:
http://www.cisco.com/en/US/docs/ios/12_2/termserv/configuration/guide/tcfaapre_ps1835_TSD_Products_Configuration_Guide_Chapter.html