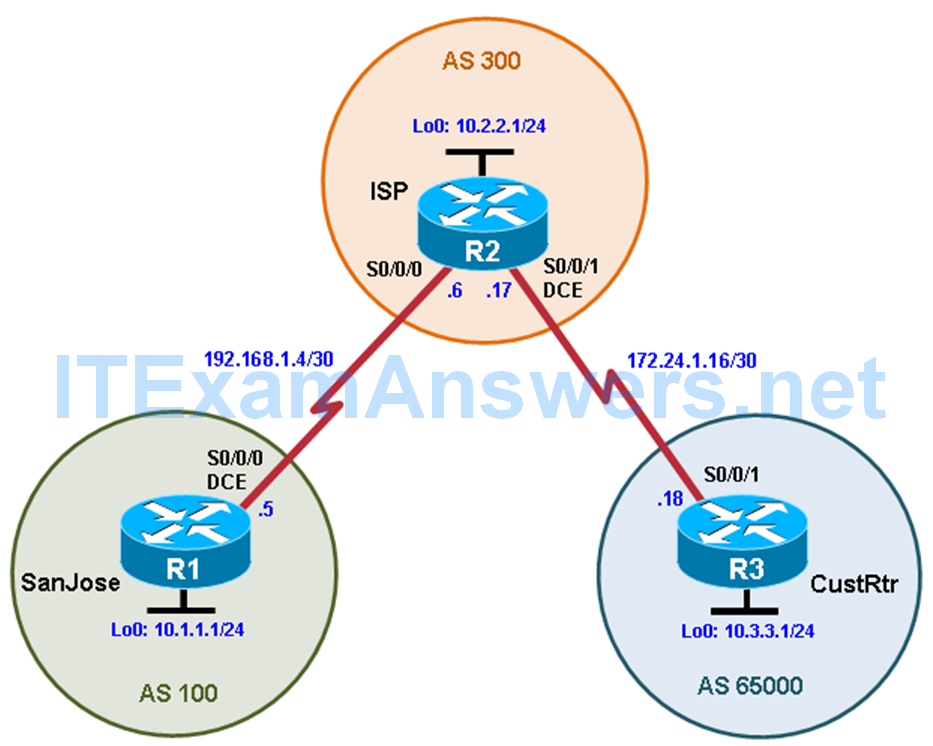
CCNP ROUTE Chapter 7 Lab 7-2, Using the AS\_PATH Attribute (Version 7)

### Topology



### 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 CustRtr. 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.

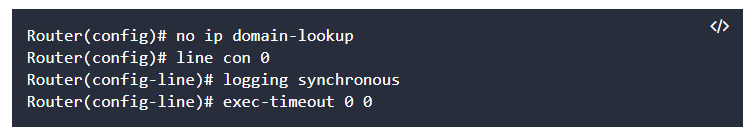
**Note:** This lab uses Cisco 1941 routers with Cisco IOS Release 15.4 with IP Base. The switches are Cisco WS-C2960-24TT-L with Fast Ethernet interfaces, therefore the router will use routing metrics associated with a 100 Mb/s interface. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

### Required Resources

* 3 routers (Cisco IOS Release 15.2 or comparable)
* Serial and Ethernet cables

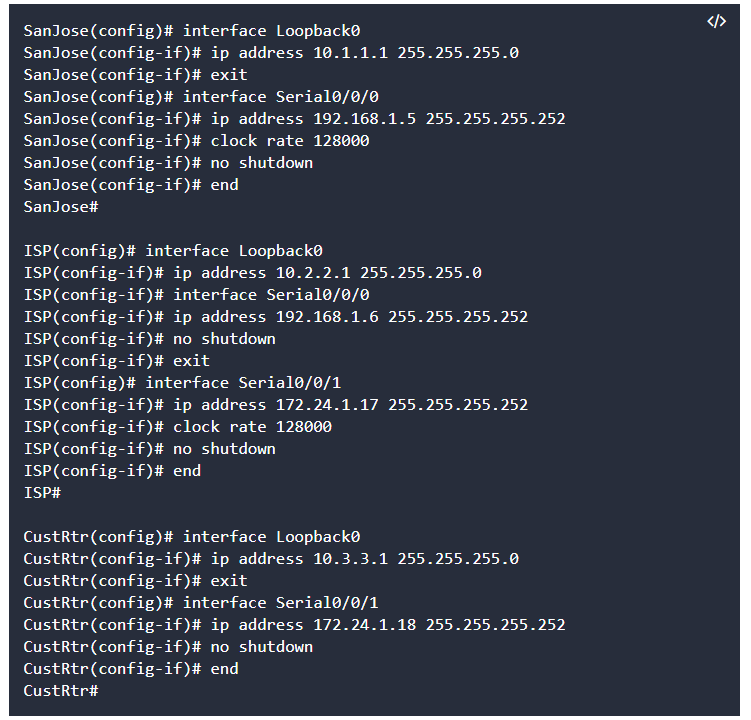
### Step 0: Suggested starting configurations.

a. Apply the following configuration to each router along with the appropriate **hostname.** The **exec-timeout 0 0** command should only be used in a lab environment.



### Step 1: Configure inteexitrface addresses.

b. Using the addressing scheme in the diagram, create the loopback interfaces and apply IPv4 addresses to these and the serial interfaces on SanJose (R1), ISP (R2), and CustRtr (R3). The ISP loopbacks simulate real networks. Set a clock rate on the DCE serial interfaces.

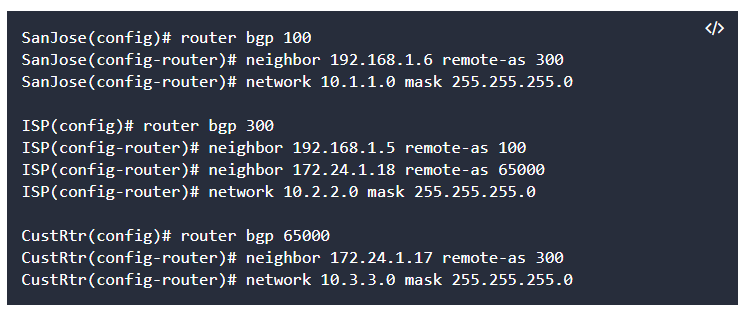


c. Use **ping** to test the connectivity between the directly connected routers.

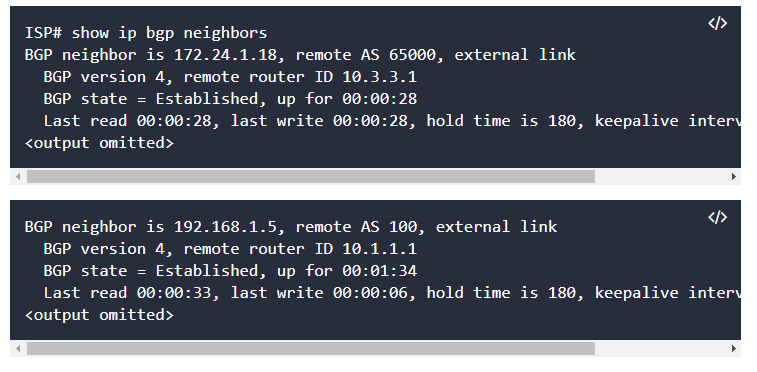
**Note:** SanJose will not be able to reach either ISP’s loopback (10.2.2.1) or CustRtr’s loopback (10.3.3.1), nor will it be able to reach either end of the link joining ISP to CustRtr (172.24.1.17 and 172.24.1.18).

### Step 2: 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.

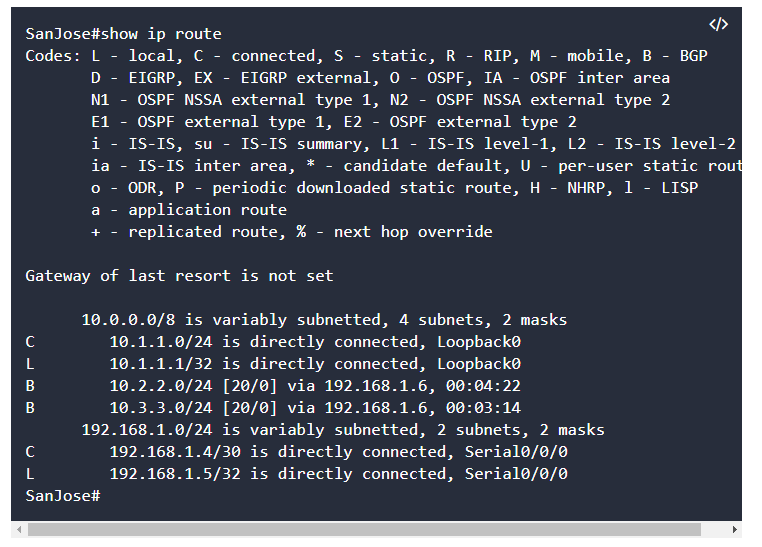


b. Verify that these routers have established the appropriate neighbor relationships by issuing the **show ip bgp neighbors** command on each router.



### Step 3: Remove the private AS.

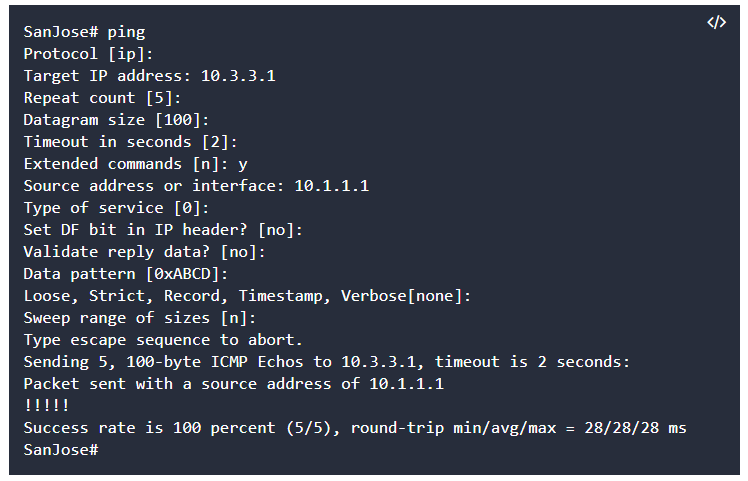
a. Display the SanJose routing table using the **show ip route** command. SanJose should have a route to both 10.2.2.0 and 10.3.3.0. Troubleshoot if necessary.

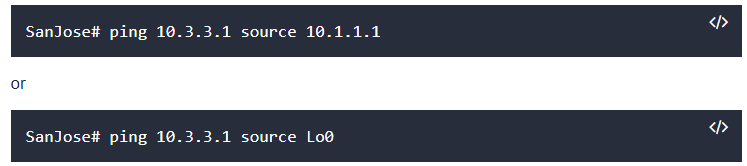


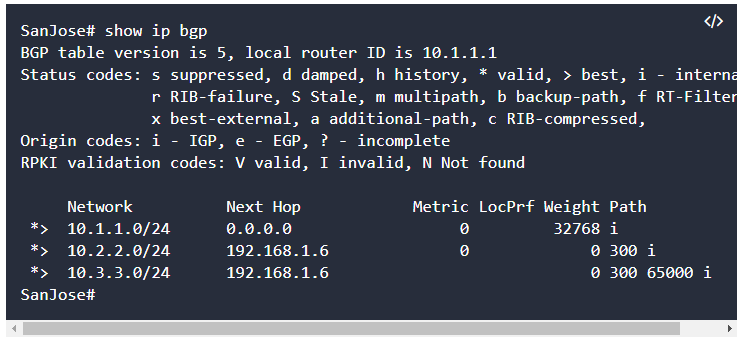
b. Ping the 10.3.3.1 address from SanJose.

Why does this fail?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

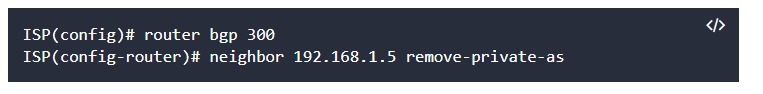


**Note:** You can bypass extended ping mode and specify a source address using one of these commands: 

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. 

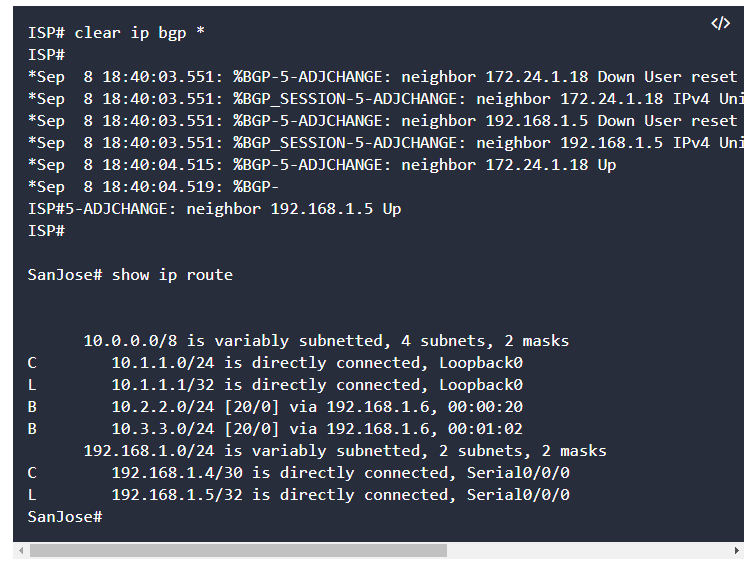
Why is this a problem?

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

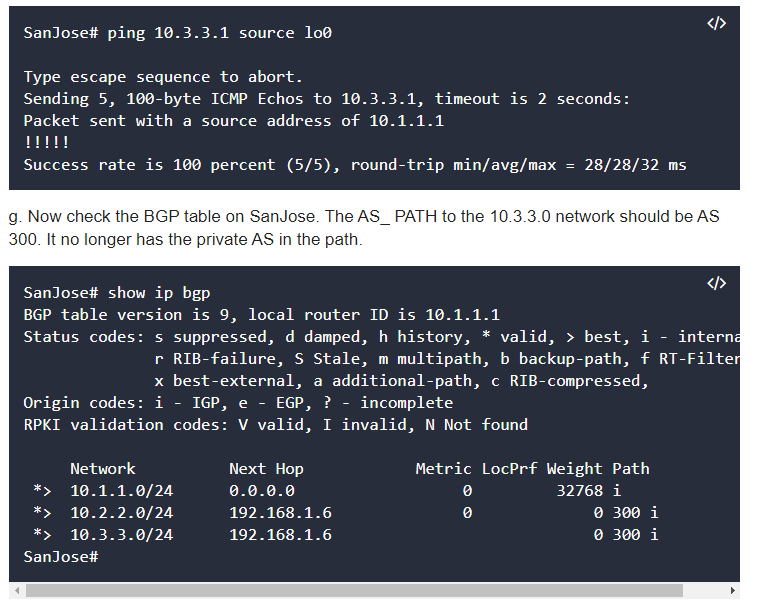


f. After issuing these commands, use the **clear ip bgp \*** command on ISP to reestablish the BGP relationship between the three routers. Wait several seconds and then return to SanJose to check its routing table.

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

Does SanJose still have a route to 10.3.3.0?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

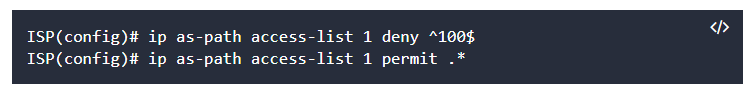


### Step 4: Use the AS\_PATH attribute to filter routes.

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.

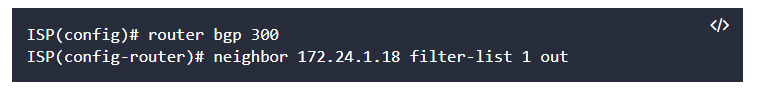
The first command uses the ^ character to indicate that the AS path must begin with the given number 100. The $ character indicates that the AS\_PATH attribute must also end with 100. Essentially, this statement matches only paths that are sourced from AS 100. Other paths, which might include AS 100 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.

For more details on configuring regular expressions on Cisco routers, see:

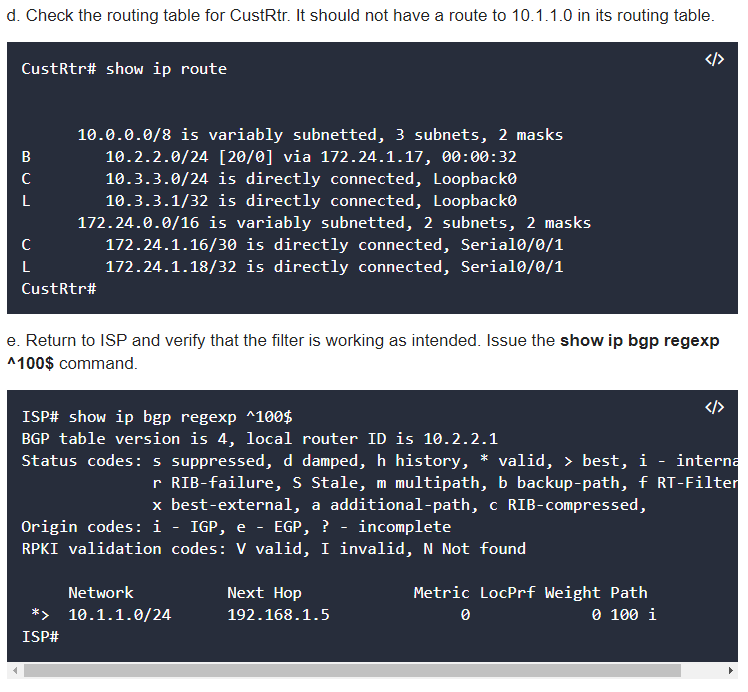
<http://www.cisco.com/c/en/us/td/docs/ios/12_2/termserv/configuration/guide/ftersv_c/tcfaapre.html>  
<http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13754-26.html>

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

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).

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.

