# Module 4 – Multihoming Strategies Lab

**Objective: Introduction to routing policy, the manipulation of BGP attributes to control traffic flow in a multihomed network.**

**Prerequisite: Module 2 and 3**

Topology :

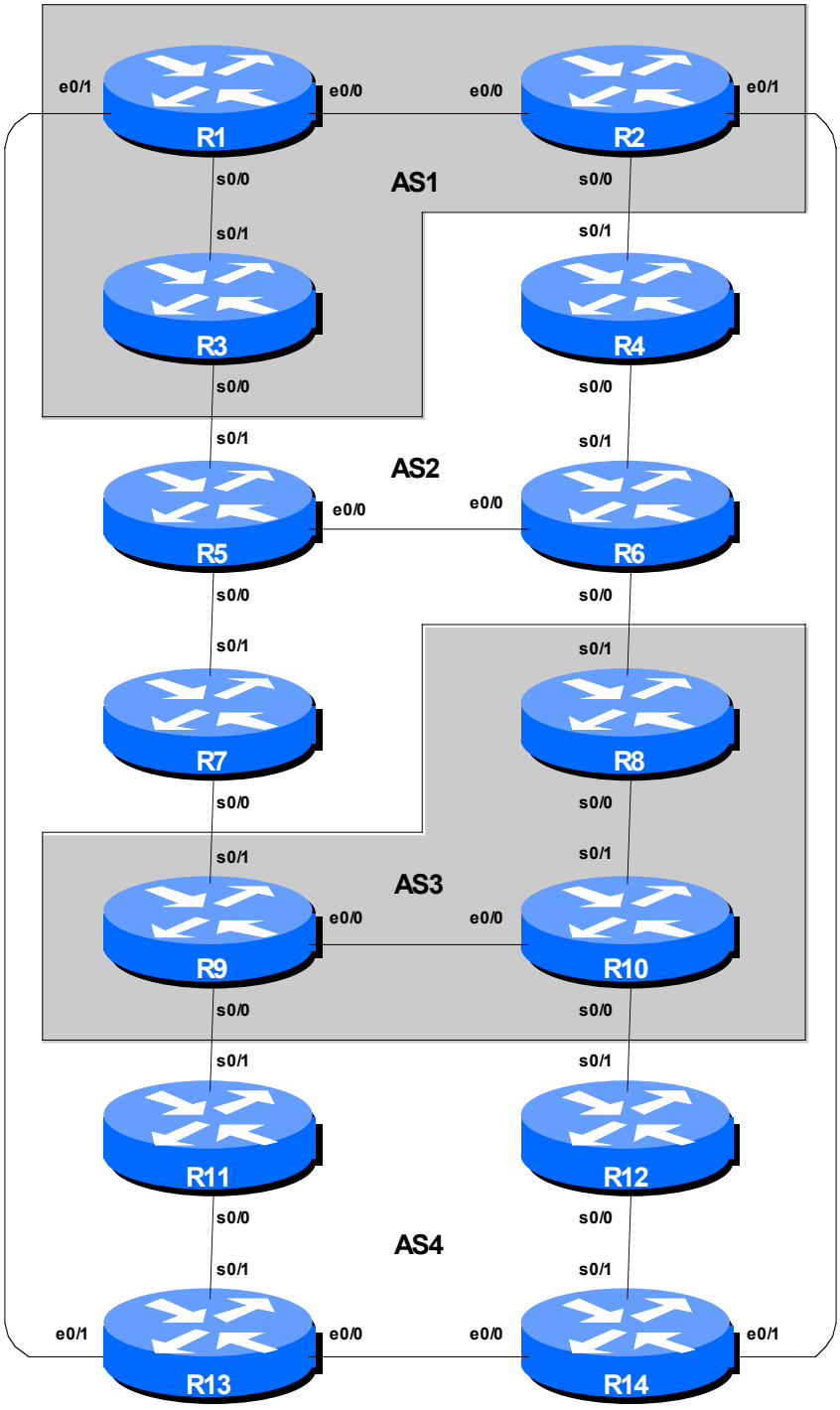


**Figure 1 – BGP AS Numbers**

## Lab Notes

This module demonstrates how an AS can use Local Preference to control outbound routing paths, and use AS path prepend and MEDs (multi-exit discriminators or metrics) to determine inbound routing paths. All three are very powerful tools for ISPs to control how their external peering links are used. Refer to the BGP documentation for more information about the BGP path selection process and the default values for, and priorities of, the "local_pref" and "metric" attributes.

Before starting this module, retain the topology and configurations as used in Module 2. This requires the removal of **all** the filtering and community configurations examined in Module 3.

**Recommendation:** Remember, if any configuration on a router is not in use, **it should be removed**. Surplus configuration usually gives rise to delayed error detection and debugging of configurations in cases of routing problems or other network failures.

## Lab Exercise

1. **Tidy up from Module 3.** If the previous module completed was Module 3, the router configuration needs to be tidied up substantially before this module is attempted. The following steps show exactly what is required.

   **Example: Router R1**

```
Router1#conf t
Router1(config)#router bgp 1
!
! First remove BGP damping
!
Router1(config-router)#no bgp dampening
!
! Now remove BGP neighbour route-map statement
!
Router1(config-router)#no neighbor 100.1.2.2 route-map infilter in
!
! Now remove community-tag from network statement
!
Router1(config-router)#no network 100.1.0.0 mask 255.255.240.0 route-map
community-tag
Router1(config-router)#network 100.1.0.0 mask 255.255.240.0
!
! Now remove route-maps
!
Router1(config)#no route-map community-tag
Router1(config)#no route-map infilter
!
! Now remove community list
!
Router1(config)#no ip community-list 1
!
! That's the configuration nice and tidy, the way it should be.
!
Router1(config)#end
!
! Now clear the bgp peering so that the old policy is removed
!
```

```
Router1#clear ip bgp 100.1.2.2 in
Router1#
```

2. **Advertising your AS's aggregate route**. Make sure that your AS is sending an aggregate prefix for all routes in the AS **along with** the more specific routes. Use the ***aggregate-address*** BGP configuration command to generate the aggregate.

   **Example:**

   AS 1 will advertise 100.1.0.0/18 and its subnets to AS 2 and AS 4.
   AS 4 will advertise 100.4.0.0/18 and its subnets to AS 1 and AS 3.
   Etc…

   Check routing tables and perform ***ping*** & ***traceroute*** tests to confirm connectivity. Test routing connectivity by disabling links to external peers and repeat the traceroute, this should show you the alternate path computed by BGP when the primary fails.

   **HINT:** The configuration on your router should now be the same as it was at the end of Module 3 but without the community settings, route-maps and community-lists. Soft-configuration shouldn't be necessary, but if any router team wishes to retain it for troubleshooting purposes, they should do so.

***Checkpoint #1****: Call your lab instructor and display the following:*

***i]*** *Output of a "**show ip route**" and "**show ip bgp**"*
***ii]*** *Outputs of the '**ping**' and '**trace**' to various destinations within the network*
***iii]*** *Outputs of the '**ping**' and '**trace**' after the primary link fails.*

3. **Aim of the Module:**

   The aim of the module is to demonstrate how to achieve a particular traffic flow using three different methods. These three methods involve modification of outbound policy, and two ways of modifying inbound policy. The reader should review the BGP presentation given prior to this module as a reminder on how to influence path choice using BGP policies.

   The diagram following (Figure 2) displays the traffic flows which are desired between particular routers and ASes. Six traffic flows are being implemented. The arrows in the figure show the flows which will be configured. Each arrow originates from a border router in an AS, and terminates on one of the routers in another AS. This signifies the traffic flows desired for the links between the two systems. Each of the following steps has a description on how to implement the traffic flow represented by each arrow. If at anytime there is any doubt as to the configuration required, consult the Cisco CD Documentation, or ask the lab instructors.

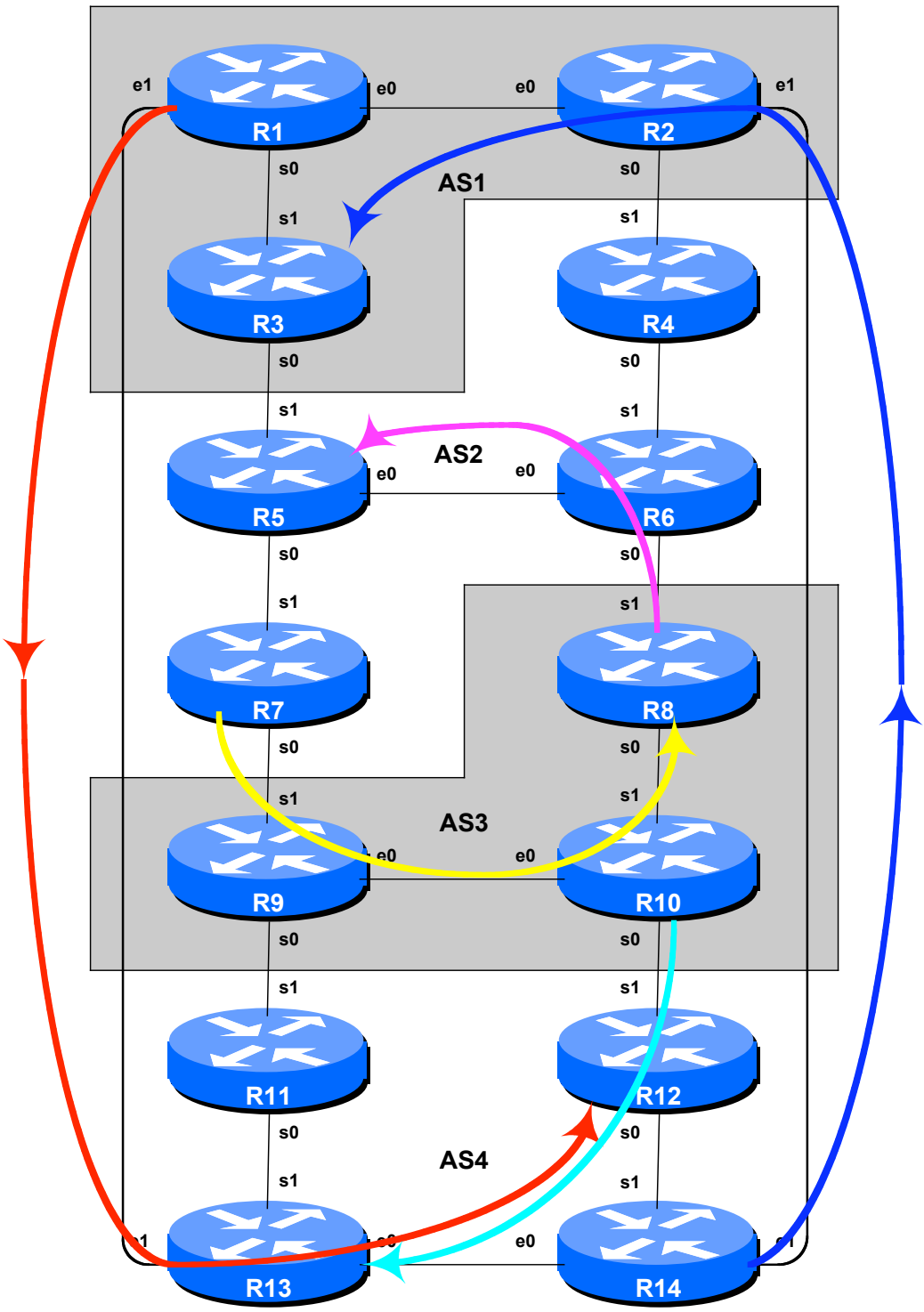


**Figure 2 – Preferred Paths**

## 4. Implement the following Outbound policies:

Discuss among teams in the same AS and negotiate with your neighbouring AS on how to implement each of the following policies on your routers. It is important that backup paths should still function. Based on the agreed method, configure the following primary paths:



**Cisco Systems Inc**
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

**AS 1**:
- All traffic **TO** 100.4.16.0/20 (R12) must exit AS 1 via Router R1 only.

**AS 2**:
- All traffic **TO** 100.3.0.0/20 (R8) must exit AS 2 via Router R7 only.

**AS 3**:
- All traffic **TO** 100.2.16.0/20 (R5) must exit AS 3 via Router R8 only.
- All traffic **TO** 100.4.32.0/20 (R13) must exit AS 3 via Router R10 only.

**AS 4**:
- All traffic **TO** 100.1.32.0/19 (R3) must exit AS 4 via Router R14 only.

Note that we are only trying to define outgoing traffic flow. The return path has no policies implemented, and the router's normal path decision process applies.

**Hints**:
- Remember in step 1 above that the router was configured to announce the aggregate as well as the specific networks in each AS? Therefore, mindful of this fact, use "**local preference**" internally to influence the exit path out of your AS. Set the preferred router to a higher than default local preference, and the less preferred routers to a lower than default local preference.
- Using a route filter is not a good way of achieving the above policies. You still need to allow alternate path rerouting if failure happens. Using **local preference** permits this.
- Draw your AS topology and address block assignment on a blank piece of paper. Discuss within your router team, and within your AS, which team should be applying which configuration at the AS boundaries. It is important to decide upon strategy before typing configuration into the router.

The example configurations below should be used as guidance for the router configuration for each router team. Note that one router in each AS will have to set high local preference, the remaining routers in the AS will set low local preference. The motivation for doing this is redundancy of configuration. If, for example, Router 7 lost its local-preference configuration due to some operator error, the low local preference set on the other three routers will ensure that the traffic policies required will still be implemented. It's quite common for many ISPs to have more than one configuration to implement a particular policy – a primary configuration, and an "inverse" secondary configuration on other routers which could be impacted.

**Example configurations for the AS 2 scenario above (using LOCAL_PREF).**
**Router 7:**

```
ip prefix-list R8-prefix permit 100.3.0.0/20
!
route-map set-local-pref-high permit 10
 match ip address prefix-list R8-prefix
 set local-preference 200
!
route-map set-local-pref-high permit 20
!
router bgp 2
 neighbor 100.3.17.1 remote-as 3
 neighbor 100.3.17.1 route-map set-local-pref-high in
```

```
!
```

**Router 4,5,6:**

```
ip prefix-list R8-prefix permit 100.3.0.0/20
!
route-map set-local-pref-low permit 10
 match ip address prefix-list R8-prefix
 set local-preference 50
!
route-map set-local-pref-low permit 20
!
router bgp 2
 neighbor x.x.x.x remote-as ASN
 neighbor x.x.x.x route-map set-local-pref-low in
!
```

***Checkpoint #2: Call your lab instructor and display the following:***

***i]*** *Each router in an AS will be asked to do a 'trace' to selected destinations, the trace must show packets exiting the AS as specified in the exercise given above.*

***ii]*** *Explain your configuration used to achieve the desired result to the instructor. Display the output of "show ip bgp", and "show ip bgp x.x.x.x" for the networks with local preference set to 200. Show the output of a trace according to instructions.*

***iii]*** *Wait until the lab instructor gives the goahead to move onto the next step.*

## STOP AND WAIT HERE

5. **Remove configuration from the previous step.** Before moving on to the next step it is important that the configuration from the previous step is removed. This involves removing the route-maps, prefix-lists and the per-neighbour configuration to set local preference. All router teams should do this, and then do a soft reset of their eBGP peerings.

6. **Implement the following Inbound policies using MEDs**. This step introduces one of two methods of influencing inbound policies. Here MEDs are used, while the next step will introduce the concept of AS path prepends. As for the previous step, read the instructions careful, and discuss in your team, and in your AS, how you are going to implement the following.

   The example in this step achieves exactly the same traffic flow between neighbouring ASes as in the previous step for the networks in question – remember that local preference is used by an AS to influence outbound traffic paths, whereas MEDs are used to influence inbound traffic paths. Refer to Figure 2 for a picture of traffic flow…

   **AS 1**:
   - All traffic **TO** 100.1.32.0/19 (R3) from anywhere in AS 4 must enter AS 1 via the R14 – R2 link. (**Hint:** this means that R1 must announce 100.1.32.0/19 to AS 4 with a higher metric than the equivalent announcement from R2.)

   **AS 2**:

- All traffic **TO** 100.2.16.0/20 (R5) from anywhere in AS 3 must enter AS 2 via the R8 – R6 link. (**Hint:** this means that R7 must announce 100.2.16.0/20 to AS 3 with a higher metric than the equivalent announcement from R6.)

**AS 3**:
- All traffic **TO** 100.3.0.0/20 (R8) from anywhere in AS 2 must enter AS 3 via the R7 – R9 link. (**Hint:** this means that R8 must announce 100.3.0.0/20 to AS 2 with a higher metric than the equivalent announcement from R9.)

**AS 4**:
- All traffic **TO** 100.4.16.0/20 (R12) from anywhere in AS 1 must enter AS 4 via the R1 – R13 link. (**Hint:** this means that R14 must announce 100.4.16.0/20 to AS 1 with a higher metric than the equivalent announcement from R13.)
- All traffic **TO** 100.4.32.0/20 (R13) from anywhere in AS 3 must enter AS 4 via the R10 – R12 link. (**Hint:** this means that R11 must announce 100.4.32.0/20 to AS 3 with a higher metric than the equivalent announcement from R12.)

**Example configurations for the AS 2 scenario above (using MED).**
**Router 6:**

```
ip prefix-list R5-prefix permit 100.2.16.0/20
!
route-map set-med-low permit 10
 match ip address prefix-list R5-prefix
 set metric 10
!
route-map set-med-low permit 20
!
router bgp 2
 neighbor 100.2.33.2 remote-as 3
 neighbor 100.2.33.2 route-map set-med-low out
!
```

**Router 7:**

```
ip prefix-list R5-prefix permit 100.2.16.0/20
!
route-map set-med-high permit 10
 match ip address prefix-list R5-prefix
 set metric 50
!
route-map set-med-high permit 20
!
router bgp 2
 neighbor 100.3.17.1 remote-as 3
 neighbor 100.3.17.1 route-map set-med-high out
!
```

**Note:** the teams operating Routers 3, 4, 5 and 10 have only to remove the configuration which was added in the previous step. They don't require to configure MEDs as above because they do not have peerings which require alterations to the inbound policy for their AS.

***Checkpoint #3*: Call your lab instructor and display the following:**

***i]*** *Each router in an AS will be asked to do a 'traceroute' to selected destinations, the trace must show packets exiting the AS as specified in the exercise given above.*

***ii]*** *Explain your configuration used to achieve the desired result to the instructor. Display the output of "show ip bgp", and "show ip bgp x.x.x.x" for the networks with MED set to 50. Show the output of a trace according to instructions.*

## STOP AND WAIT HERE

7. **Remove the configuration used for the previous step.** Before moving on to the next step it is important that the configuration from the previous step is removed. This involves removing the route-maps, prefix-lists and the per-neighbour configuration to set MEDs. All router teams should do this, and then do a soft reset of their eBGP peerings.

8. **Implement the following inbound policies using the AS path prepend method.** This step introduces the second of two methods of influencing inbound policies. As for the previous step, read the instructions carefully, and discuss within your team, and within your AS, how you are going to implement the following.

   The example in this step achieves exactly the same traffic flow between neighbouring ASes as in the previous step for the networks in question. Refer to Figure 2 for a picture of traffic flow…

   **AS 1**:
   - All traffic **TO** 100.1.32.0/19 (R3) from anywhere in the lab topology must enter AS 1 via the R14 – R2 link. (**Hint:** this means that R1 and R3 must announce 100.1.32.0/19 with a longer AS path than the other networks in AS 1. R2 needs to announce 100.1.32.0/19 with a longer AS path in its peering with R4.)

   **AS 2**:
   - All traffic **TO** 100.2.16.0/20 (R5) from anywhere in the lab topology must enter AS 2 via the R8 – R6 link. (**Hint:** this means that R4, R5 and R7 must announce 100.2.16.0/20 with a longer AS path than the other networks in AS 2.)

   **AS 3**:
   - All traffic **TO** 100.3.0.0/20 (R8) from anywhere in the lab topology must enter AS 3 via the R7 – R9 link. (**Hint:** this means that R8 and R10 must announce 100.3.0.0/20 with a longer AS path than the other networks in AS 3. R9 needs to announce 100.3.0.0/20 with a longer AS path in its peering with R11.)

   **AS 4**:
   - All traffic **TO** 100.4.16.0/20 (R12) from anywhere in the lab topology must enter AS 4 via the R1 – R13 link. (**Hint:** this means that R11, R12 and R14 must announce 100.4.16.0/20 with a longer AS path than the other networks in AS 4.)
   - All traffic **TO** 100.4.32.0/20 (R13) from anywhere in the lab topology must enter AS 4 via the R10 – R12 link. (**Hint:** this means that R11, R13 and R14 must announce 100.4.32.0/20 with a longer AS path than the other networks in AS 4.)

AS_PREPEND is commonly used by smaller ISPs who are multihoming to their upstream providers. It is convention on the Internet to add at least two ASes when using AS_PREPEND. More usually, three ASes are added, especially if the upstream ISPs have links to each other going through a third party.

**Example configuration for the AS 3 scenario above (using AS PATH prepend):**

```
ip prefix-list R8-prefix permit 100.3.0.0/20
!
route-map set-as-path permit 10
 match ip address prefix-list R8-prefix
 set as-path prepend 3 3 3
!
route-map set-as-path permit 20
!

router bgp 3
 neighbor 100.2.33.1 remote-as 2
 neighbor 100.2.33.1 route-map set-as-path out
!
```

**Note:** the team with Router 6 has only to remove the configuration which was added in the previous step. They don't require to configure AS path prepends as above because they do not have peerings which require alterations to the inbound policy for their AS.

***Checkpoint #4*: Call the lab instructor and display the following:**

***i]*** *Each router in an AS will be asked to do a 'traceroute' to selected destinations, the trace must show packets exiting the AS as specified in the exercise given above.*

***ii]*** *Explain your configuration used to achieve the desired result to the instructor. Display the output of "show ip bgp", and "show ip bgp x.x.x.x" for the networks with increased AS path length. Show the output of a trace according to instructions.*

***iii]*** *How has AS Path prepend changed the BGP table and the Routing decision. Can the decision be overridden using any other BGP configuration within an AS?* ***Answer:*** *review the BGP route selection rules from the slide in the presentation section.*

## 9. Summary:

This module has demonstrated several ways of influencing inbound and outbound routing policy.

**Q:** What is the difference in the resulting effects using the methods in steps 4) and 5)?

**A:** AS PATH prepend affects routing announcements between two ASes, and is visible everywhere, even outside the two ASes which are making use of the prepend information. MEDs only apply between multiple peerings between the same AS. If the peer AS is announcing the local AS onwards, the metric set is that of the peer AS, not the local AS.

Consult the BGP documentation for more information. There are many possible variations on the examples given in this module. Remember the following points:

- local preference is used for influencing policy within an AS
- MEDs are used to influence policy over multiple links between the local and an immediately neighbouring AS
- The AS path prepend is used to influence external policy on a global scale (which includes the immediately neighbouring AS). Current Internet practice is to add three of the local AS in any AS prepend – obviously the application determines what is actually deployed.

## *Review Questions*

1. Which is the most effective way of influencing how traffic leaves your network?

2. How useful do you think MEDs are in the real live Internet? Consider the answer to question one before replying!



**Cisco Systems Inc**
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

## *CONFIGURATION NOTES*

Documentation is critical! You should record the configuration at each ***Checkpoint***, as well as the configuration at the end of the module.