Module 2 – IPv6 iBGP and Basic eBGP

Objective: Using IPv6, simulate four different interconnected ISP backbones using a combination of OSPF, internal BGP, and external BGP.

Prerequisites: Module 1

Topology :

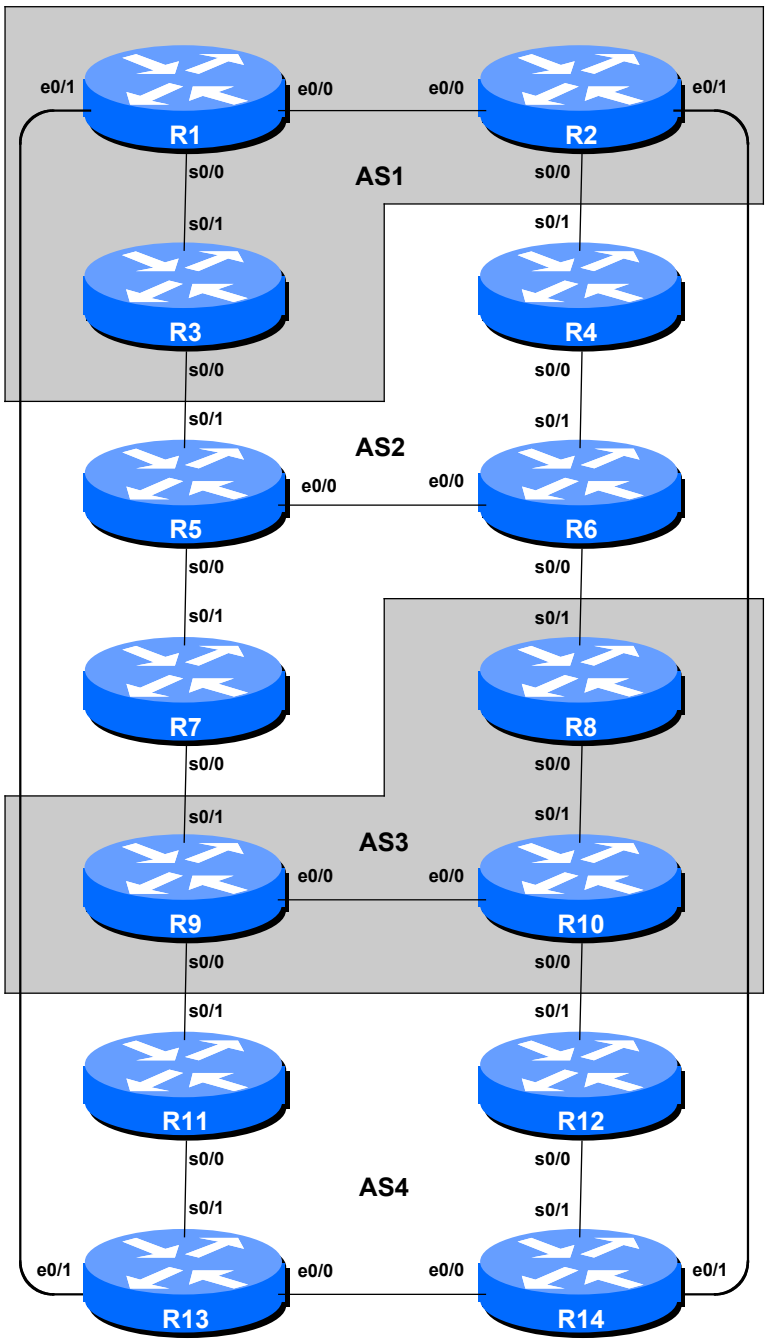

Figure 1 – BGP AS Numbers

Lab Notes

The purpose of this module is to introduce the student to external BGP (eBGP). This is the relationship between different autonomous systems in an "Internet". The classroom is split into four distinct networks, and the teams belonging to each network work together as a typical ISP. Each AS has two links to its neighbouring ASes, and this feature will used throughout a significant portion of this workshop.

The connectivity shown in the diagrams represents links between AS's. It is assumed that all the routers within an AS are physically connected to each other as per Figure 1.

Note: this IPv6 module can be completed independently of the IPv4 version of this module. It only requires the basic topology and connectivity provided by Module 2. If IPv4 is not configured at all, remember to manually set the OSPF and BGP router-ids.

Lab Exercises

1. Connect routers as shown in Figure 1. All routers within an AS must be physically connected and reachable. The relationship between the ASes is as drawn in Figure 2 and gives a view which can be related to the "real world".

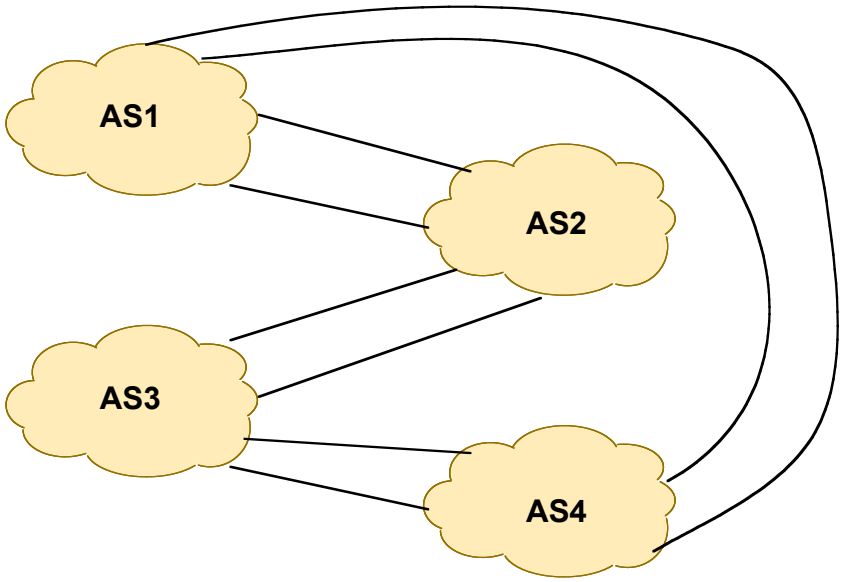

Figure 2 – AS relationship

2. The address assignments and addresses used for links between routers should be left the same as those chosen for Module 1.

3. **Re-configure BGP and OSPF (if coming from Module 1).** On each router, remove the BGP and OSPF processes from Module 1 by using the following two commands:

```
Router1(config)# no router bgp 10
Router1(config)# no ipv6 router ospf 41
```

This will clear the BGP and OSPF configuration for the current module.

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

(The alternative is to simply erase the entire router configuration using *write erase*, and then reload the router and start again, completing all steps of Module 1 up to Step 11. Or copying the configuration you saved at the end of Step 11, just prior to starting the OSPF configuration. Which you probably forgot to do, even with both the lab instructor and these written notes telling you to do so.)

4. **Configure IPv6 OSPF on the routers within each AS.** In each AS configure IPv6 OSPF routing. This means that networks for the links to each member in the AS must be entered in OSPF via the *network* statement. All the routers in an AS will be in the same OSPF *area 0* and use the same OSPF process ID. For example, Router 1, with two interfaces connecting to other routers in their AS, would have the following:

```
ipv6 router ospf 1
 passive-interface default
 no passive-interface ethernet 0/0  ! adjacencies only on eth0/0...
 no passive-interface serial 0/0    ! ...and ser0/0
 log-adjacency-changes
!
interface ethernet 0/0
 ipv6 ospf 1 area 0
interface ethernet 0/1
 ipv6 ospf 1 area 0
interface serial 0/0
 ipv6 ospf 1 area 0
interface loopback0
 ipv6 ospf 1 area 0
!
```

Notes:

- *Passive-interface default* makes sure that OSPF does not attempt to set up adjacencies on any interfaces apart from those specified by the *no passive-interface* commands.
- The number following "*ipv6 router ospf*" is a process ID and is used inside the router only (so it can be any number). But for this lab we recommend the OSPF process ID be the same as the AS number (which is the convention used by a number of ISPs).

5. **Ping Test.** Check the IPv6 routes known via OSPF. Make sure you can see all the networks within your AS. Ping all loopback interfaces within your AS. Use the "*show ipv6 ospf neighbor"* and *"show ipv6 route"* commands. If you cannot see the other routers in your AS, you will not be able to bring up BGP in the next steps.

6. **Save the configuration.** Don't forget to save the configuration to NVRAM!

Checkpoint #1 : *call the lab assistant to verify the connectivity.*

7. **Configure iBGP peering between routers within an AS.** Use the loopback address for the iBGP peerings. Also, configure the *network* command to add the address block assigned to each Router Team for advertisement in BGP.

```
router bgp 1
 no bgp default ipv4-unicast
```

```
 bgp log-neighbor-changes
 address-family ipv6
  no synchronization
  network 1001:10::/32
  neighbor 1001:11::1 remote-as 1
  neighbor 1001:11::1 update-source loopback 0
  neighbor 1001:11::1 description iBGP Link to R2
  neighbor 1001:13::1 remote-as 1
  neighbor 1001:13::1 update-source loopback 0
  neighbor 1001:13::1 description iBGP Link to R3
!
ipv6 route 1001:10::/32 Null0
```

Q: Do you need the BGP command ***no synchronization***? Why?

A: An ISP network is a **transit** network, meaning it accepts packets from one peering AS, carries it across the backbone, then hands it over to the next AS toward the destination. To ensure that routers internal to the AS are able to forward transit packets (from the ingress border router to the egress border router), all BGP border routers will wait for a network prefix to arrive in the IGP (as they all participate in the same IGP) before advertising them to external BGP peers. This is referred to as ***synchronization***. In other words, internal routers must be aware of those prefixes learned via IGP that border routers learn via iBGP.

As you can see, this applies to an environment where BGP routes are redistributed into the IGP. A typical ISP usually doesn't do that as the Internet routing table is somewhat large. Instead, it runs a fully meshed iBGP (or uses route-reflectors) among all routers in the backbone. Therefore synchronisation should be turned off in this kind of environment.

8. **Test internal BGP connectivity.** Use the BGP Show commands to ensure you are receiving everyone's routes from within your AS.

9. **Configure passwords on the iBGP sessions.** Passwords should now be configured on the iBGP sessions. Review the presentation why this is necessary. Agree amongst all your team members in your AS what the password should be on the iBGP session, and then apply it to all the iBGP peerings on your router. For example, on Router2's peering with Router3, with "cisco" used as the password:

```
router bgp 1
 address-family ipv6
  neighbor 1001:13::1 password cisco
```

IOS currently resets the iBGP session between you and your neighbouring router whenever an MD5 password is added. So when passwords are added to BGP sessions on live operational networks, this work should be done during a maintenance period when customers know to expect disruptions to service. In the workshop lab, it doesn't matter so much. (Future IOS releases will avoid having this rather serious service disruption.)

Watch the router logs – with the BGP session neighbour changes being logged, any mismatch in the password should be easy to spot.

Checkpoint #2: *Call the lab assistant and demonstrate the password as set on the iBGP session. Once confirmed by the lab assistant, move on to the next steps.*

10. **Configure eBGP peering.** Use Figure 1 to determine the links between the AS's. Addressing for eBGP links between 2 AS's will use the point-to-point interface addresses, ***NOT*** the loopback addresses (review the BGP presentation if you don't understand why). So, for Router1's peering with Router13, the configuration might look like:

```
router bgp 1
 address-family ipv6
  neighbor 1001:10:0:2::2 remote-as 4
  neighbor 1001:10:0:2::2 description eBGP to Router13
```

Use the BGP Show commands to ensure you are sending and receiving the BGP advertisements from your eBGP neighbours.

Q. Why can't the loopback interfaces be used for the eBGP peerings?

A. The IP address of a router's loopback interface is not known to external BGP peers, so the external peers will have no way of knowing how to contact each other to establish the peering.

Q. Which BGP show command allows you to see the state of the BGP connection to your peer?

A. Try *show bgp ipv6 unicast neighbor x.x.x.x* – this will give detailed information about the state of the peer. There are subcommands of this one, giving more information about the peering.

Q. Which BGP Show command will allow you to see exactly which networks you are advertising and receiving from your eBGP peers?

A. Try *show bgp ipv6 unicast neighbor x.x.x.x route* – this will show which routes you are receiving from your peer. Likewise, replacing *route* with *advertised-routes* will list the networks which are being announced to your peer. (Note that in general ISP operational practice, there are caveats here – if you apply route-maps and some BGP policies, these will not be processed by the *advertised-routes* command. Use the *advertised-routes* subcommand with due caution.)

11. **Configure passwords on the eBGP session.** Passwords should now be configured on the eBGP sessions between your and your neighbouring ASes. Agree between you and your neighbouring AS what the password should be on the eBGP session, and then apply it to the eBGP peering. For example, on Router2's peering with Router4, with "cisco" used as the password:

```
router bgp 1
 address-family ipv6
  neighbor 1001:11:0:1::2 password cisco
```

As previously for the iBGP session, watch the logs for password mismatches, or missing passwords. As with the iBGP sessions previously, you will find that the router will reset the eBGP session as soon as the password is applied.

Note: Wherever a BGP (either iBGP or eBGP) session is configured from now on in the workshop, all Router Teams MUST use passwords on these BGP sessions.

Checkpoint #3: *Call the lab assistant and demonstrate the password as set on the eBGP session. Once confirmed by the lab assistant, move on to the next steps.*

12. Aggregate each AS's CIDR Blocks. Each router team was allocated either a /32 address block or a /31 address block in the first Module. However, each AS has three or four routers in it, so we need to take the address space from each router team in the AS and aggregate it before we make any announcement to any external AS. It is expected by all Internet operators that any address space an ISP is using is aggregated as much as possible before it is announced to the rest of the Internet. Subdividing the address space inside an AS is perfectly acceptable and obviously very common – but leaking this subdivided address space out to the Internet at large is considered antisocial and unfriendly by many ISPs. In this case the address blocks belonging to each AS can be aggregated into a larger /30 address block.

For example, AS1 has three routers in it. Router 1 was allocated 1001:10::/32, Router 2 was allocated 1001:11::/32 and Router 3 was allocated 1001:12::/31. These three address blocks can be aggregated into the 1001:10::/30 network. And this /30 is what should be announced to eBGP neighbours.

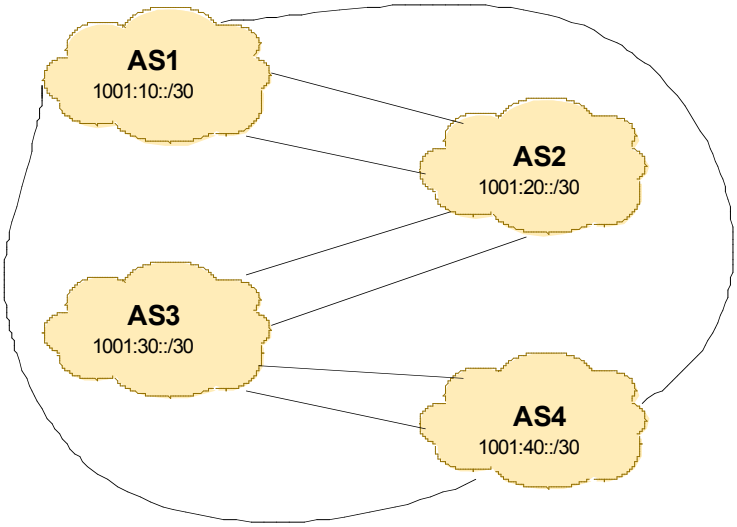

Figure 3 – Aggregates for each ASN

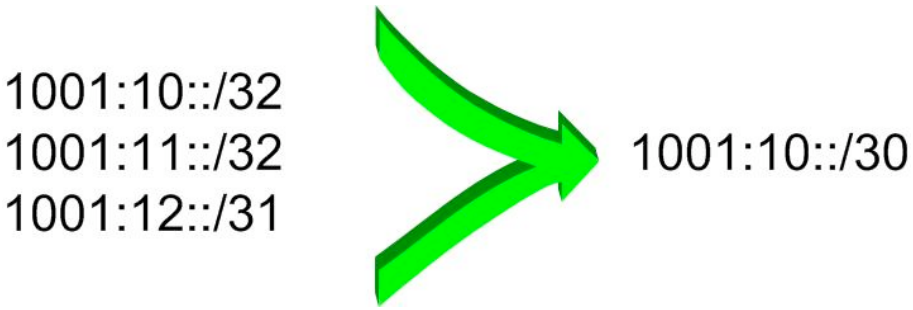

Figure 4 – Aggregating AS1 IPv6 address space into a /30

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

Q. How do you automatically aggregate via BGP smaller address blocks from within your network to a larger address block outside your network? ***Hint:*** *Review the BGP documentation.*

A. Configure:

```
router bgp 1
 address-family ipv6
  aggregate-address 1001:10::/30
```

Type ? after the command to see what options this command has.

13. **Examine the *origin* of the network prefixes.** What is the origin type for the aggregated prefixes? Write your answer here:

14. **Check the network paths.** Do traceroutes to hosts nominated on the network by the lab instructor.

Checkpoint #4: *Call the lab assistant to verify the connectivity. Use commands such as "show ip route sum", "show bgp ipv6 unicast sum", "show bgp ipv6 unicast", "show ipv6 route", and "show bgp ipv6 unicast neigh x.x.x.x route | advertise". There should be 13 specific prefixes and 4 aggregate prefixes (one for each ISP).*

Review Questions

1. How many *origin types* exist in BGP?
2. List the origin types. **Hint:** Review the BGP presentations.
3. How are they used?
4. Why are passwords necessary on both iBGP and eBGP sessions? What do they protect against?
5. Why is aggregation important for the Internet?

CONFIGURATION NOTES

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

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