IPv6 Module 6x – iBGP and Basic eBGP

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

Topology :

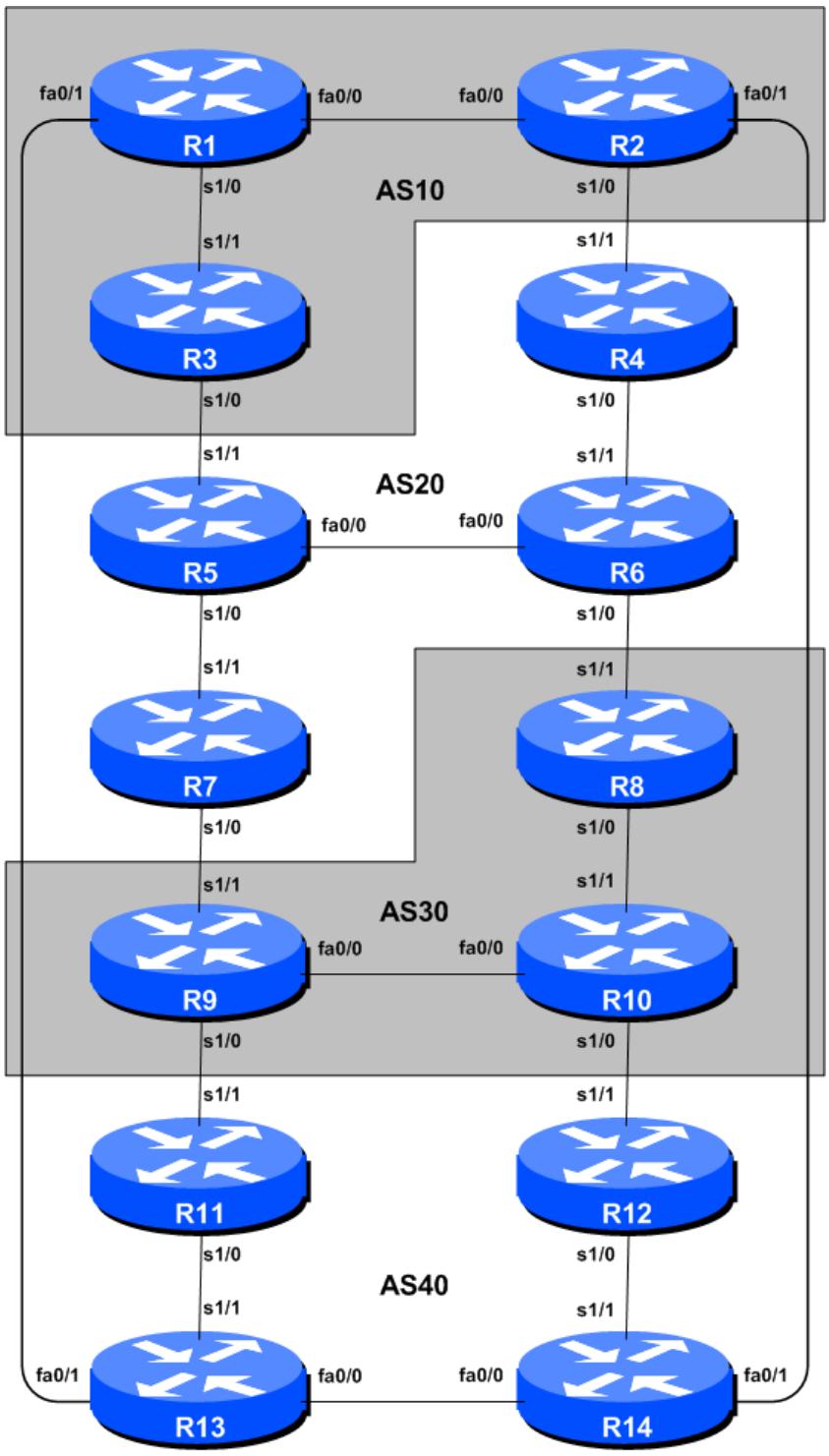

Figure 1 – BGP AS Numbers

Lab Notes

The purpose of this module is to build a basic 4 autonomous system network for the purpose of introducing IS-IS, iBGP and eBGP to the student. This infrastructure shows the relationship between different autonomous systems in an "Internet". 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 is intended to be completed after the IPv4 version of this module.

Lab Exercises

1. **Topology.** The instructor will have configured the network to the topology 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".

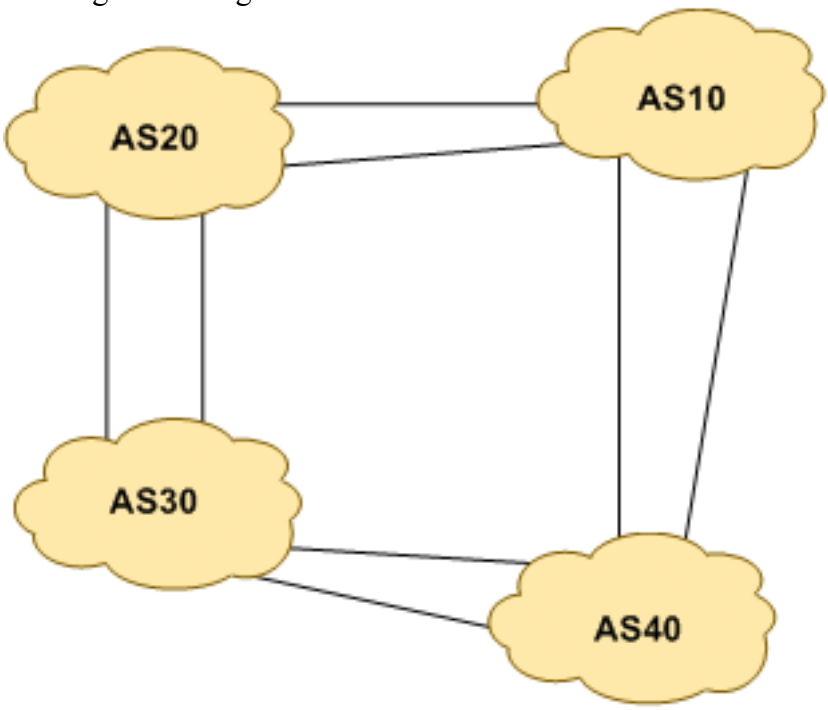

Figure 2 – AS relationship

2. **Enable IPv6.** Cisco routers with an IOS supporting IPv6 currently do not ship with IPv6 enabled by default. This needs to be done before any of the following exercises can be completed. To do this, use the following command:

```
Router(config)# ipv6 unicast-routing
```

   The router is now configured to support IPv6 Unicast (as well as IPv4 Unicast which is the default). Save the configuration.

3. **Enable IPv6 CEF.** Unlike IPv4, CEFv6 is not enabled by default. So we now need to enable IPv6 CEF also, using the following command:

```
Router(config)# ipv6 cef
```

   Nothing will break if IPv6 CEF is not enabled, but more advanced features such as NetFlow will not function without IPv6 CEF being enabled.

4. **Disable IPv6 Source Routing.** Unless you really believe there is a need for it, source routing should be disabled. This option, enabled by default, allows the router to process packets with source routing header options. This feature is a well-known security risk as it allows remote sites to send packets with different source address through the network (this was useful for troubleshooting networks from different locations on the Internet, but in recent years has been widely abused for miscreant activities on the Internet).

```
Router1 (config)# no ipv6 source-route
```

5. **IPv6 Addressing Plans.** Addressing plans in IPv6 are somewhat different from what has been considered the norm for IPv4. The IPv4 system is based around the RIRs allocating address space to an LIR (an ISP who is a member of the RIR) based on the needs of the ISP; that allocation is intended to be sufficient for a year of operation without returning to the RIR. The ISP is expected to implement a similar process towards their customers – so assigning address space according to the needs of the customer.

   The system changes a little for IPv6. While the RIRs still allocate address space to their membership according to their membership needs, the justification to receive an IPv6 allocation is somewhat lighter than it is for IPv4. A bigger advantage starts with the customer assignments made by the ISP – the ISP simply has to assign a /48 to each of their customers. This is the minimum assignment for any site/customer – within this /48 there are 64k possible subnets, deemed sufficient for all but the largest networks around these days. Within this /48, the smallest unit which can be assigned is a /64 – so every LAN and point-to-point link receives a /64. **Note: This workshop will adopt the recommendations of RFC6164 and use a /127 mask for each point-to-point link – even though the link still has a /64 reserved for it.**

   With this revised system, the address plan for IPv6 is greatly simplified. ISPs assign a single /48 for their network infrastructure, and the remainder of their /32 block is used for customer assignments. This workshop assumes this principle, as will be seen in the following steps.

6. **IPv6 Addressing.** As with the IPv4 portion of this Module, we need to come up with a sensible and scalable addressing plan for each AS in this network. The RIRs are typically handing out IPv6 address space in /32 chunks – we assume for the purposes of this lab that our ISP has received a /32. Each AS gets their own address block, a /32 (typical minimum allocation for a starter ISP). This address block should be assigned to links and loopbacks on the routers making up each ASN. The allocations are as follows:

AS10	**2001:db8::/32**	**AS30**	**2001:dba::/32**
AS20	**2001:db9::/32**	**AS40**	**2001:dbb::/32**

   The typical way that ISPs split up their allocated address space is to carve it into three pieces. One piece is used for assignments to customers, the second piece is used for infrastructure point-to-

point links, and the final piece is used for loopback interface addresses for all their backbone routers. Figure 3 below reminds how this could be done:

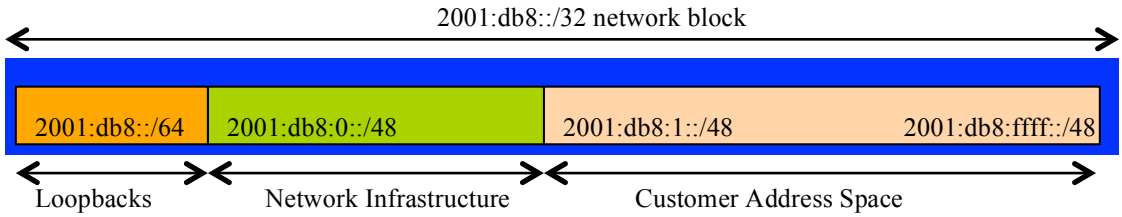

Figure 3 – Dividing allocated block of /20 into Customer, Infrastructure and Loopbacks

Please refer to the accompanying hand out for the address plan which should be used for this module onwards – it is entitled "Addressing Plan – Modules 6 to 9". Configure the addresses on each interface which will be used for this module, and check basic IP connectivity with your immediately adjacent neighbours.

7. **Configuring IPv6 Addresses on Interfaces.** Configure the addresses on each interface which will be used for this module, and check basic IP connectivity with your immediately adjacent neighbours. A sample configuration might look like:

```
Router2(config)# interface serial 1/0
Router2(config-if)# ipv6 address 2001:db8:0:6::/127
```

Q: What network mask should be used on all IPv6 enabled interfaces?

A: The network mask should be /127. This is the subnet size used for all point-to-point links as recommended in RFC6164. We still reserve the entire /64 for this point-to-point link though, allowing simpler operational scalability should future changes be required.

8. **Ethernet Connections.** As for the previous step, assign IPv6 addresses to the Ethernet point-to-point connections. As with a serial interface, a point-to-point Ethernet is addressed as a /127 out of a reserved /64.

9. **Ping Test.** Ping all physically connected subnets of the neighbouring routers. If the physically connected subnets are unreachable, consult with your neighbouring teams as to what might be wrong. Don't ignore the problem – it may not go away. Use the following commands to troubleshoot the connection:

```
show ipv6 neighbors                          : Shows the ipv6 neighbour cache
show ipv6 interface <interface> <number>     : Interface status and configuration
show ipv6 interface                          : Summary of IP interface status and configuration
```

10. **Router Loopback Interface Addressing.** As the minimum subnet size possible for IPv6 is a /64, we will assign the first /64 out of our /48 infrastructure block to be used for loopbacks even though each AS has either 3 or 4 routers in it. The loopback address assignments which will be used for this module are below:

Router1	**2001:db8::1**	**Router4**	**2001:db9::1**
Router2	**2001:db8::2**	**Router5**	**2001:db9::2**
Router3	**2001:db8::3**	**Router6**	**2001:db9::3**

Router7	**2001:db9::4**	**Router11**	**2001:dbb::1**
Router8	**2001:dba::1**	**Router12**	**2001:dbb::2**
Router9	**2001:dba::2**	**Router13**	**2001:dbb::3**
Router10	**2001:dba::3**	**Router14**	**2001:dbb::4**

For example, Router Team 1 would assign the following address and mask to the loopback on Router 1:

```
Router1(config)#interface loopback 0
Router1(config-if)#ipv6 address 2001:db8::1/128
```

Q: Why do we use /128 masks for the loopback interface address?

A: There is no physical network attached to the loopback so there can only be one device there. So we only need to assign a /128 mask – it is a waste of address space to use anything else.

11. **Configure ISIS for IPv6 on the routers within each AS.** Check that the ISIS configuration is in place and is functioning normally. Remember that ISIS should be configured on internal interfaces **only**. You do not want to set up adjacencies with devices outside your AS. Make sure that there are no *ipv6 router isis* commands on external interfaces. A side effect of this is that external link addresses will not appear in the IGP (see the next section discussion iBGP deployment).

    Don't forget to enable multi-topology ISIS when enabling ISIS to support IPv6. This will enable you to deploy ISIS for IPv6 across your ASN without breaking the IPv4 connectivity. (If your routers do not support multi-topology ISIS, you will need to coordinate activation of the IPv6 address family on a per-interface basis with adjacent routers.) Also remember to set the over-load bit as was done for the IPv4 topology.

    As an example, Router Team 1, with two interfaces in AS 10 would have the following:

```
Router1 (config)# router isis as10
Router1 (config-router)# net 49.0001.0100.0001.5224.00
Router1 (config-router)# is-type level-2-only
Router1 (config-router)# metric-style wide level-2
Router1 (config-router)# metric 100000
Router1 (config-router)# log-adjacency-changes
!
Router1 (config-router)# address-family ipv6
Router1 (config-router-af)# multi-topology
Router1 (config-router-af)# set-overload-bit on-startup wait-for-bgp
!
Router1 (config)# interface fastethernet 0/0
Router1 (config-if)# ipv6 router isis as10
Router1 (config-if)# isis ipv6 metric 2 level-2
!
Router1 (config)# interface serial 1/0
Router1 (config-if)# ipv6 router isis as10
Router1 (config-if)# isis ipv6 metric 20 level-2
!
```

    Remember that the interfaces on which you do not want to run ISIS need to be marked as *passive*. For ISIS, marking an interface as *passive* means that CLNS adjacencies are not solicited **and** the IP subnet used on the interface is inserted into ISIS. Note that you cannot mark interfaces as passive until you have ISIS assigned to at least one physical interface on the router.

```
Router1 (config)# router isis as10
Router1 (config-router)# passive-interface Loopback0
```

Notes:

- ISIS by default will only set up adjacencies and announce the prefixes of the interfaces which are activated by the "`ipv6 router isis`" command. This is different behaviour from OSPF which will attempt to set up adjacencies on interfaces covered by the `network` statement (and hence require the use of `passive` and `no passive` to control its behaviour).
- Different ISPs use different NET addressing schemes. But it is common to use the router loopback IP address as the system ID in either hex or decimal format. In this module all routers in an AS are level-2 in and one area (*49.0001*) only.

12. ISIS on Point-to-Point Ethernet Links. Confirm that ISIS is operating in point-to-point mode on point-to-point Ethernet links. It should be independent of the IPv6 protocol, so the adjacencies will still be active from the IPv4 lab.

13. Ping Test. Check the routes via ISIS. Make sure you can see all the networks within your AS, and see no networks from other ASs. Ping all loopback interfaces within your AS Set. Use the "*show clns neighbor"* and *"show ip route"* commands.

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

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

15. Turning on neighbour authentication for ISIS. Confirm that the neighbour authentication is still functional for ISIS. It should be independent of the IPv6 protocol, so the adjacencies will still be active.

16. 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 10
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 address-family ipv6
  distance bgp 200 200 200
  no synchronization
  network 2001:db8::/32
  neighbor 2001:db8::2 remote-as 10
  neighbor 2001:db8::2 update-source loopback 0
  neighbor 2001:db8::2 next-hop-self
  neighbor 2001:db8::2 description iBGP Link to R2
  neighbor 2001:db8::3 remote-as 10
  neighbor 2001:db8::3 update-source loopback 0
  neighbor 2001:db8::3 next-hop-self
  neighbor 2001:db8::3 description iBGP Link to R3
!
ipv6 route 2001:db8::/32 Null0
```

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

18. **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 10
 address-family ipv6
  neighbor 2001:db8::3 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.*

19. **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 10
 address-family ipv6
  neighbor 2001:db8:0:4::1 remote-as 40
  neighbor 2001:db8:0:4::1 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.)

20. **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 10
 address-family ipv6
  neighbor 2001:db8:0:3::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.*

21. **Adding a "customer" route into BGP.** As we did in Module 1, we are now going to add a "customer" route into BGP on each router. We don't have any "customers" as such connected to our routers in the lab, so we are going to simulate the connectivity by simply using a Null0 interface. The "customer" address space that each router team will introduce into the iBGP is listed below – again we will each use a /48, for simplicity's sake.

R1	**2001:db8:1::/48**	**R8**	**2001:dba:1::/48**
R2	**2001:db8:2::/48**	**R9**	**2001:dba:2::/48**
R3	**2001:db8:3::/48**	**R10**	**2001:dba:3::/48**
R4	**2001:db9:1::/48**	**R11**	**2001:dbb:1::/48**
R5	**2001:db9:2::/48**	**R12**	**2001:dbb:2::/48**
R6	**2001:db9:3::/48**	**R13**	**2001:dbb:3::/48**
R7	**2001:db9:4::/48**	**R14**	**2001:dbb:4::/48**

Each team should now set up a static route pointing to the **NULL0** interface for the /48 that they are to originate. Once the static is set up, the team should then add an entry into the BGP table. Here is an example for Router8:

```
ipv6 route 2001:dba:1::/48 Null0
!
router bgp 30
```

```
 address-family ipv6
  network 2001:dba:1::/48
!
```

22. Check the BGP table. Are there routes seen via ***show bgp ipv6***? If not, why not? Once every team in the class has done their configuration, each team should see the aggregate from each AS as well as the fourteen /48s introduced in the previous step. If this is not happening, work with your neighbours to fix the problem.

Checkpoint #4: *Call the lab assistant to verify the connectivity. Use commands such as "show ipv6 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 4 aggregate prefixes (one for each ISP) and the 14 customer /48's in the BGP table.*