Modulo 2 – IPv6 iBGP y eBGP Básico

Objetivo: Utilizando IPv6, similar cuatro dorsales de ISPs diferentes interconectados usando una combinación de OSPF, BGP interno y BGP externo.

Prerrequisitos: Modulo 1 (IPv6)

Topología:

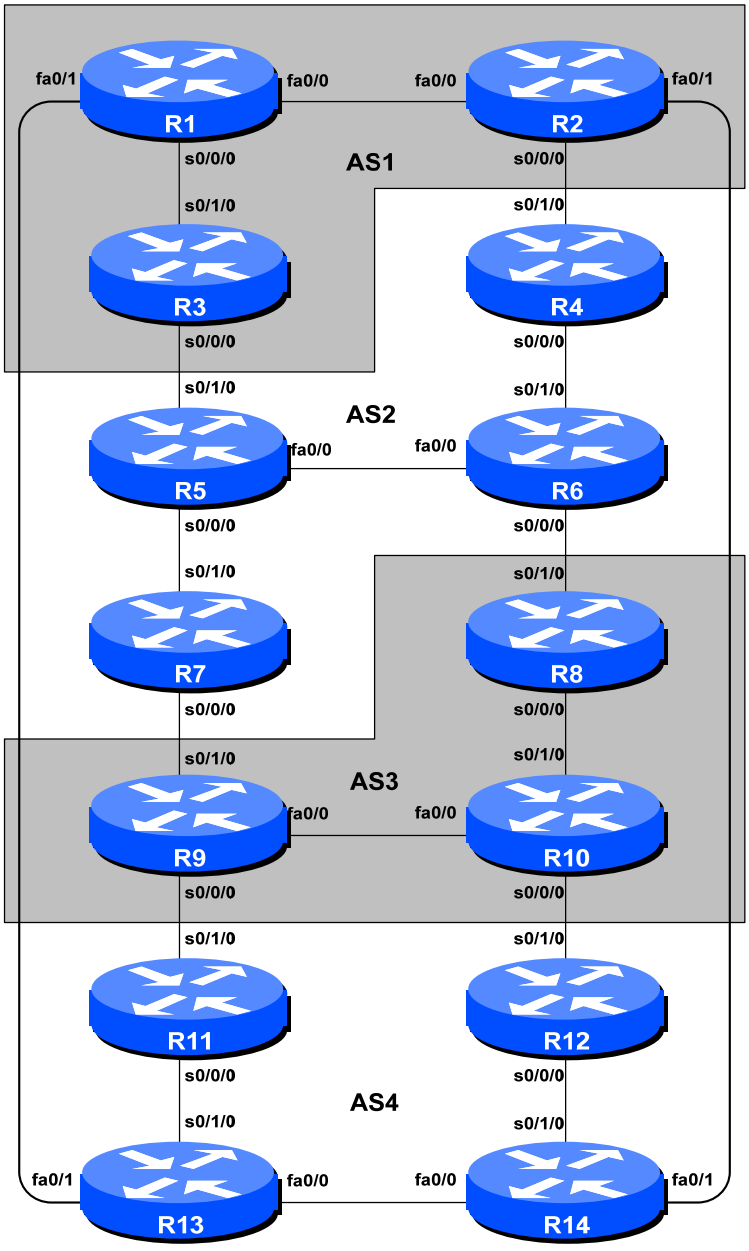

Figura 1 – Número de Sistemas Autónomas (AS) BGP

Notas para el Lab

El propósito de este modulo es introducir al estudiante a BGP externo. Esta es la relación entre diferentes sistemas autónomos en una “Internet”. La clase se divide en cuatro redes diferentes, y todos los equipos que pertenecen a cada red trabajan juntos como un ISP típico. Cada AS tiene dos enlaces a los AS vecinos.

La conectividad mostrada en los diagramas representan los enlaces entre los ASs. Se asume que todos los ruteadores dentro del AS están físicamente conectados entre si como muestra la Figura 1.

Ejercicios de Lab

1. Conecte los ruteadores como muestra la Figura 1. Todos los ruteadores dentro de un AS deben estar conectados físicamente y alcanzables. La relación entre sistema autónomos (AS) se muestra en la Figura 2 y nos da una visión que puede ser relacionado con el “mundo real”.

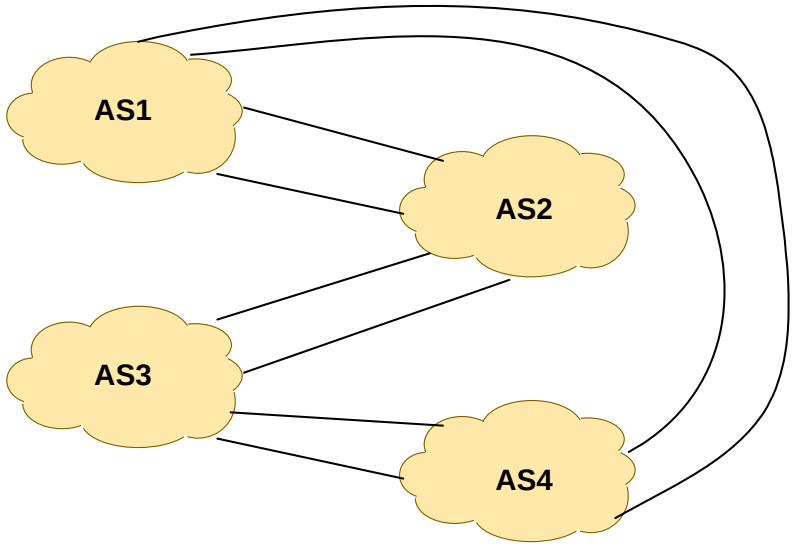

Figura 2 – Relación entre AS

2. La asignación de direcciones y las direcciones utilizadas en los enlaces deberá permanecer igual que los que se seleccionaron en el Modulo 1.

3. **Reconfigure OSPF para IPv6.** En cada ruteador, remueva los procesos de OSPF para IPv6 si todavía se encuentran presentes del Modulo 1 usando el siguiente comando:

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

   Esto eliminará OSPF para IPv6 de la configuración para el modulo actual.

   Cada equipo del ruteador también va a necesitar remover OSPF para IPv6 en cada interfase donde estaba corriendo OSPF en el Modulo 1.

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

4. **Configure OSPF para IPv6 OSPF en cada ruteador dentro del AS.** En cada AS configure ruteo OSPF para IPv6. Todos los ruteadores en el mismo AS va a ser la misma area 0 en OSPF y el mismo numero de proceso (ID) para OSPF. Por ejemplo, el ruteador 1, con dos interfaces conectados a otros dos ruteadores en el AS va a tener lo siguiente:

```
ipv6 router ospf 1
 passive-interface default
 no passive-interface FastEthernet 0/0 !adyacencias solo en FastEthernet0/0
 no passive-interface serial 0/0/0  ! ...y ser0/0/0
 log-adjacency-changes
!
interface FastEthernet 0/0
 ipv6 ospf 1 area 0
interface FastEthernet 0/1
 ipv6 ospf 1 area 0
interface serial 0/0/0
 ipv6 ospf 1 area 0
interface loopback0
 ipv6 ospf 1 area 0
!
```

   Notas:
   - *Passive-interface default* hace que OSPF no intenta crear una adyacencia una interfase a menos que se especifique con el comando *no passive-interface*.
   - El número después de "*ipv6 router ospf*" es el identificador del proceso y se usa solamente dentro del ruteador (y puede ser cualquier número). Pero para el lab se recomienda que sea el mismo ID del proceso que el numero del AS (lo cual es una practica común de algunos ISPs).

5. **Prueba de Ping.** Verifique que las rutas IPv6 son vistas mediante OSPF. Verifique que se pueden ver todas las redes dentro del AS. Haga ping a todas las interfases de loopback dentro del AS. Utilice los comandos "*show ipv6 ospf neighbor"* y *"show ipv6 route"*. Si no puede ver los otros ruteadores en el AS, no va a ser posible levantar a BGP en los pasos siguientes.

Punto de Verificación #1 : *llame al asistente del laboratorio para verificar la conectividad.*

6. **Configure iBGP entre los ruteadores dentro de cada AS.** Utilice la dirección de la interfase de loopback para hacer las asociaciones. También configure el comando *network* para agregar el bloque de direcciones asignado a cada equipo del ruteador para el anuncio mediante BGP.

```
router bgp 1
address-family ipv6
 no synchronization
 network 1001:10::/32
 neighbor 1001:11:ffff:ffff::1 remote-as 1
 neighbor 1001:11:ffff:ffff::1 update-source loopback 0
 neighbor 1001:11:ffff:ffff::1 description Enlace iBGP a R2
 neighbor 1001:11:ffff:ffff::1 activate
 neighbor 1001:13:ffff:ffff::1 remote-as 1
 neighbor 1001:13:ffff:ffff::1 update-source loopback 0
 neighbor 1001:13:ffff:ffff::1 description Enlace iBGP a R3
 neighbor 1001:13:ffff:ffff::1 activte
!
ipv6 route 1001:10::/32 Null0
```

P: ¿Necesita el comando en BGP ***no synchronization***? ¿Por que?

R: Una red de un ISP es una red de **transito**, lo que significa que acepta paquetes de un vecino AS, los lleva a través de su dorsal, y los entrega a otro AS en dirección del destino. Para asegurar que los ruteadores internos a un AS pueden enviar paquetes en transito (desde el ingreso por un ruteador de frontera hasta la salida por otro ruteador de frontera), todos los ruteadores con BGP van a esperar a que existe un prefijo en el proceso de enrutamiento IGP (interno) antes de anunciarlo al exterior con los vecinos en BGP. Esto se conoce como ***sincronización***. En otras palabras, los ruteadores internos debelan conocer los prefijos aprendidos por el proceso IGP que los ruteadores de frontera aprenden mediante iBGP.

Como puede ver, esto se aplica para un ambiente en donde las rutas BGP se redistribuyen al proceso IGP. Un ISP típicamente no hace esto dado que la tabla de ruteo del Internet es bastante grande. En cambio, crea un malla completa de iBGP (o usa route-reflectors) entre todos los ruteadores en la dorsal. Por lo tanto, la sincronización se deberá apagar en este tipo de ambiente.

7. **Prueba de conectividad de BGP interna.** Utilice los comandos de BGP Show para asegurar que se esta recibiendo rutas dentro del AS.

8. **Configure contraseñas en las sesiones de iBGP.** Las contraseñas se deberán configurar ahora en las sesiones de iBGP. Revise la presentación de porque es necesario. Pónganse de acuerdo entre todos los miembros del mismo AS cual contraseña usar en las sesiones iBGP, y luego aplícalo en cada sesión iBGP en su ruteador. Por ejemplo, en la asociación del Ruteador2 con el Ruteador3, con la contraseña de “cisco”:

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

Actualmente IOS reinicializa la sesión iBGP entre su ruteador y el ruteador del vecino cuando se agrega una contraseña MD5. Entonces cuando se agrega una contraseña en una red en producción, se deberá hacer en una ventana de mantenimiento cuando los clientes esperan tener una interrupción en el servicio. En el lab, realmente no importa tanto.

Ponga atención en la bitácora de los ruteadores – en el registro de cambio de sesiones del vecino BGP, cualquier contraseña que no coincide deberá ser fácil de verse.

Punto de Verificación #2: *Llame al asistente del laboratorio para demostrar el password que se configuro en la sesión de iBGP. Una vez confirmado, sigue con los siguientes pasos.*

9. **Configure la asociación eBGP.** Utilice la Figura 1 para determinar los enlaces entre los AS. Las direcciones que se usan para los enlaces de eBGP serán las direcciones punto-a-punto, ***NO*** las direcciones de loopback. Entonces para que el Ruteador1 se asocia con el Ruteador13, es posible que la configuración se vea como:

```
router bgp 1
 neighbor 1001:10:ffff:2::2 remote-as 4
 neighbor 1001:10:ffff:2::2 description eBGP al Ruteador13
 neighbor 1001:10:ffff:2::2 activate
```

Utilice los comandos de BGP Show para asegurar que esta enviando y recibiendo los anuncios de BGP con los vecinos.

P. ¿Por qué los interfaces de loopback no pueden ser utilizados para la asociación de eBGP?

R. La dirección IP de la interfase loopback no es conocido por los vecinos externos en BGP, entonces no hay forma de contactarse para establecer la asociación.

P. ¿Cuál comando de BGP muestra el estado de la conexión con su vecino?

R. Pruebe *show bgp ipv6 neighbor x.x.x.x* – con este comando se ve la información a detalle del estado de una asociación. Existen subcomandos de este que dan mas detalle de la asociación.

P. ¿Qué comando de BGP Show permite ver cuales son las redes anunciadas y recibidas de las asociaciones eBGP?

R. Pruebe *show bgp ipv6 neighbor x.x.x.x route* – este va a mostrar las ruta que esta recibiendo del asociado. De igual manera reemplaza *route* con *advertised-routes* y ve la lista de redes anunciadas al asociado. (Una nota general para la operación del ISP, existen excepciones – si aplica route-maps y algunas políticas de BGP, no van a ser procesados mediante el comando *advertised-routes*. Utilice el subcomando *advertised-routes* con precaución.)

10. **Configure la contraseña en la sesión eBGP.** Ahora se deberá configurar una contraseña en eBGP entre su sesión y su vecino en otro AS. Póngase de acuerdo en cual contraseña utilizar, luego aplícalo a la asociación. Por ejemplo para el Ruteador2 asociado con el Ruteador4, utilizando el password de “cisco”:

```
router bgp 1
 neighbor 1001:11:ffff:1::2 password cisco
```

Como se vio previamente en la sesión iBGP, revise la bitácora para contraseñas que no coinciden o faltan. Como iBGP, la sesión de eBGP se reinicializa al agregar una contraseña. SI NO sucede haga uso del comando “clear ip bgp 1001:10:FFFF:FFFF::1”.

Punto de Verificación #3: *Llame al asistente del laboratorio y muestre la contraseña con la sesión de eBGP. Una vez confirmado, continué al siguiente paso.*

11. **Agregue los bloques CIDR de cada AS.** Cada equipo del ruteador has sido asignado un bloque de direcciones /32 o /31 en el primer modulo. Pero cada AS tiene tres o cuatro, por lo que necesitamos tomar el espacio de direcciones de cada equipo y agregarlo antes de anunciarlo al exterior. Se espera de todos los operadores del Internet agreguen lo que mas pueda antes de anunciar al Internet. Es política aceptable y común subdividir el espacio de direccionamiento dentro de un AS – pero dejar salir estas subdivisiones al Internet se considera poco sociable por muchos ISPs. En este caso se debe de agregar los bloques de cada AS en un bloque mas grande /18.

Por ejemplo, AS1 tiene tres ruteadores. El Ruteador 1 tiene asignado 1001:10::/32, el Ruteador 2 fue asignado 1001:11::/32 y el Ruteador 3 fue asignado 1001:12::/31. Estos tres bloques de direcciones pueden ser agregados en una red 1001:10::/30. Y esta /30 es lo que se debe de anunciarse a los vecinos eBGP.

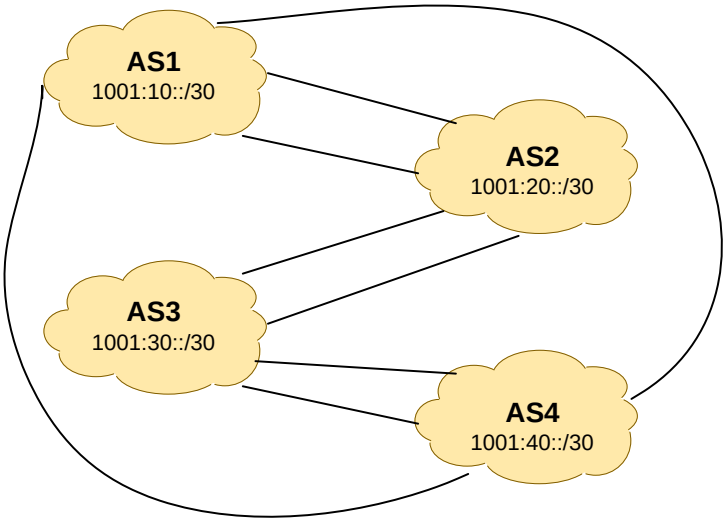

Figure 3 – Agregados para cada AS

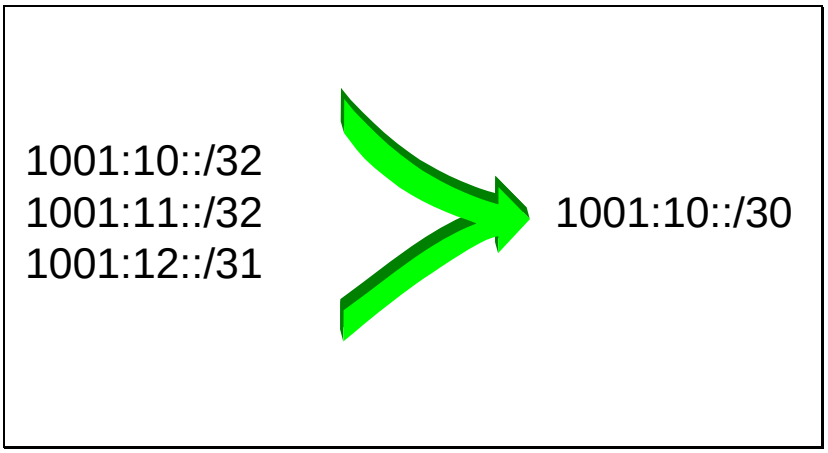

Figure 4 – Aggregando el espacio de direccionamiento IPv6 en AS1 IPv6 a un /30

P. ¿Cómo se puede agregar automáticamente a un bloque de direcciones más pequeño dentro de un bloque de direcciones más grande hacia afuera de su red? ***Sugerencia:*** *Revise la documentación de BGP.*

R. Configure:

```
router bgp 1
address-family ipv6
 aggregate-address 1001:10::/32
```

Pruebe ? después del comando para ver que opciones se tiene.

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

12. Examine el *origin* de los prefijos de red. ¿Cuál es el tipo de origen de los prefijos agregados? Escriba su respuesta aquí:

13. Verifique caminos de los prefijos. Haga traceroute a los nodos nominados por el instructor.

Punto de Verificación #4: *Llame al asistente del laboratorio para verificar la conectividad. Utilice los comandos como "show ip route sum", "show bgp ipv6 sum", "show bgp ipv6", "show ipv6 route", y "show bgp ipv6 neigh x.x.x.x route | advertise". Deberá existir 13 prefijos específicos y 4 prefijos agregados (uno por cada ISP).*

Preguntas para Revisión

1. ¿Cuántos tipos de *origin* existen en BGP?

2. Haga una lista de los tipos de origen.

3. ¿Cómo son utilizados?

4. ¿Por qué son necesarios los passwords para sesiones de iBGP y eBGP? ¿Contra que se protege?

5. ¿Por qué es importan agregar para el Internet?