Modulo 1 – IPv6 OSPF e iBGP

Objetivo: Crear un lab básico de interconexión usando IPv6 con un área OSPF y un AS BGP.

Prerrequisitos: Ninguno

Lo siguiente será la topología común usada en este ejercicio.

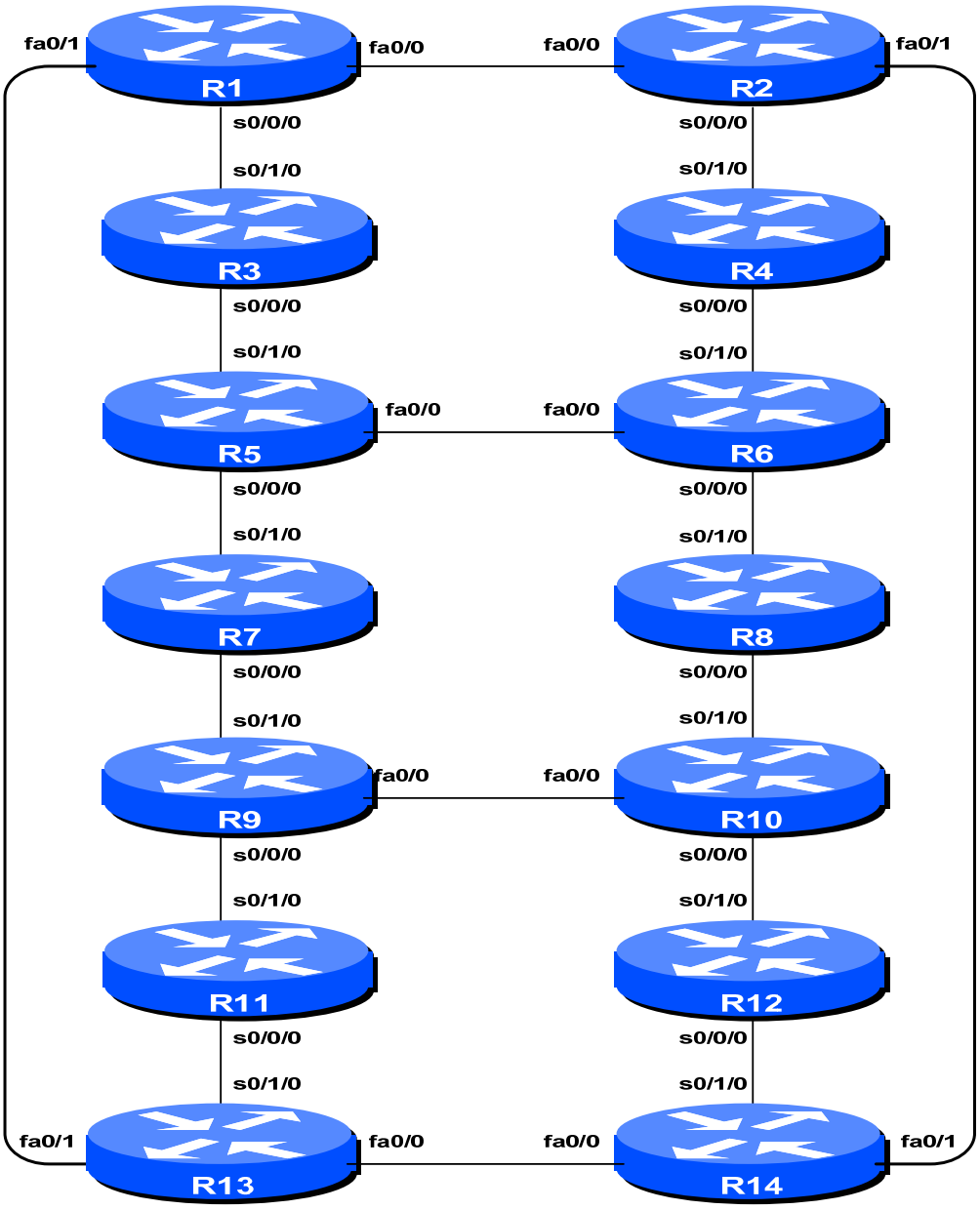

Figura 1 – Lab Básico de Configuración

Notas para el Lab

Los ruteadores que se usan en esta parte del taller deben soportar IPv6. Esto es básicamente cualquier imagen IP Plus del 12.2T en adelante. Es mejor verificar con el Cisco Feature Navigator en http://www.cisco.com/go/fn para asegurar que imagen y plataformas soportan IPv6. Desafortunadamente IPv6 no es parte del las imágenes IP only que usan muchos ISPs.

Ejercicios del Lab

1. **Ruteadores y participantes del Taller.** El taller esta organizado de tal forma que un grupo de dos personas pueden operar un ruteador. Existen 14 ruteadores lo cual implica que al menos 28 participantes. Cada taller con un número grande de participantes, es posible tener 3 participantes por ruteador.

2. **Nombre del Ruteador.** Cada ruteador va a tener un nombre de acuerdo su localización en la tabla, Ruteador1, Ruteador2, Ruteador3, etc. La documentación en el lab hará referencia a *Ruteador1* como R1. En el consola del ruteador, ingrese a modo "enable", luego ingrese "config terminal", o simplemente "config" solo:

```
Router> enable
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname Router1
Router1(config)#
```

3. **Apague la Resolución de Nombres de Dominio.** Los ruteadores Cisco siempre tratan de buscar en el DNS para un nombre o dirección especificado en la línea de comandos. Vamos a apagar esta resolución en el lab para acelerar el tiempo que procesa el comando traceroute.

```
Router1 (config)# no ip domain-lookup
```

4. **Deshabilita la Resolución de Nombres para Comandos.** El ruteador intenta usar varios transportes para resolver comandos introducidos en la línea de comandos. Si el comando no es parte de IOS, el ruteador va a intentar interpretar el significado del nombre. Por ejemplo si el comando es una dirección IP, el ruteador va a tratar de conectarse al destino remoto. Esto no es una funcionalidad deseable para un ISP ya que puede resultar en intentos de conexión a destinos remotos o largos tiempos de espera en lo que intenta de traducir el nombre en el DNS. Para esto eliminamos todos los transportes por omisión en la consola y las líneas virtuales.

```
Router1 (config)# line con 0
Router1 (config-line)# transport preferred none
Router1 (config-line)# line vty 0 4
Router1 (config-line)# transport preferred none
```

5. **Usuarios y Contraseñas.** Todos los usuarios y contraseñas de los ruteadores deberán ser ***cisco***. Por favor no cambie el usuario o contraseña a algo diferente o lo dejan sin configuración (el acceso a los puertos vty no son posibles si no tienen una contraseña). Es esencial para la operación del lab.

```
Router1 (config)# username cisco password cisco
Router1 (config)# enable secret cisco
Router1 (config)# service password-encryption
```


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

La directiva *service password-encryption* indica al ruteador que encrypta la contraseña antes de almacenar la configuración del ruteador.

6. **Habilitando el acceso a login para otros equipos.** Para permitir a los otros equipos hacer telnet a su ruteador en el futuro es necesario configurar una contraseña en las líneas virtuales.

```
Router1 (config)# aaa new-model
Router1 (config)# aaa authentication login default local
Router1 (config)# aaa authentication enable default enable
```

Con esta serie de comandos se le indica al ruteador que busque el usuario localmente (pareja de usuario y contraseña ya introducido anteriormente), y también para el "enable secret" para enable. Por omisión, el login se habilitará en todos los vtys para acceso de los otros equipos.

7. **Configuración de bitácoras del sistema.** Una parte vital para cualquier operación es la bitácora de eventos. Por omisión el ruteador despliega eventos en la consola del ruteador. Pero, esto no es lo deseable para ruteadores en operación, ya que la consola es una conexión a 9600 baudios, y causa una carga muy alta al procesador para procesar las interrupciones. Pero también queremos que se almacena la bitácora de eventos en un buffer – esto no causa interrupciones y permite al operador ver el historial de eventos que han sucedido en el ruteador.

```
Router1 (config)# no logging console
Router1 (config)# logging buffered 8192 debugging
```

Estos comandos deshabilitan la salida de eventos en la consola y los envía a un buffer de 8192 bytes dentro del ruteador.

8. **Crear las interfaces Loopback.** Para el ruteo dinámico de IPv6 con OSPF y BGP, el identificador del proceso generalmente es el primer Loopback que el ruteador encuentra cuando se inicializa la configuración. Lo mas común es que existe ruteo IPv4, y vamos a configurar una dirección IPv4 en el Loopback 0 para asegurar que este sea el valor que toma los procesos de OSPv4 y BGP.

Para reducir la complejidad del laboratorio, en la siguiente tabla se usarán las direcciones que corresponden al Loopback 0 de cada ruteador. Por ejemplo para configurar el ruteador 1, es como sigue:

```
Router1(config)#interface loopback 0
Router1(config-if)#ip address 100.1.15.1 255.255.255.255
```

R1	**100.1.15.1/32**	**R8**	**100.3.15.1/32**
R2	**100.1.31.1/32**	**R9**	**100.3.31.1/32**
R3	**100.1.63.1/32**	**R10**	**100.3.63.1/32**
R4	**100.2.15.1/32**	**R11**	**100.4.15.1/32**
R5	**100.2.31.1/32**	**R12**	**100.4.31.1/32**
R6	**100.2.47.1/32**	**R13**	**100.4.47.1/32**
R7	**100.2.63.1/32**	**R14**	**100.4.63.1/32**

9. **Habilitar IPv6.** Los ruteadores de Cisco con soporte a IPv6 no se embarcan con IPv6 habilitado por omisión. Se requiere iniciarlo antes de que los ejercicios pueden ser completados. Para esto se usa el siguiente comando:

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

   El ruteador ahora esta configurado para IPv6 Unicast (y también IPv4 Unicast que es por omisión).

10. **Esquema del Plan de Direccionamiento IPv6.** Los planes de direccionamiento en IPv6 son algo diferentes a lo que consideramos común para IPv4. El sistema de IPv4 esta basado en que el Registro Regional del Internet (RIR) asigna un espacio de direcciones al LIR (o un ISP que miembro del RIR) basado en las necesidades del ISP; la intención de la asignación es tener suficiente para un año de operación sin regresar al RIR. Se espera que el ISP implemente un proceso similar con sus clientes – asignando el espacio de direcciones según las necesidades del cliente.

    El sistema cambia un poco con IPv6. Mientras que el RIR todavía asigna el espacio de direcciones a su miembros de acuerdo a sus necesidades, la justificación para recibir una asignación es un poco mas ligero que en IPv4. Si un ISP puede demostrar un plan para conectar a 200 clientes al Internet usando IPv6, ellos recibirán una asignación. Pero, una mejor ventaja es la asignación de direcciones para clientes – el ISP simplemente tiene que asignar un /48 para cada cliente. Esta es la mínima asignación para un sitio/cliente – dentro del /48 hay la posibilidad de 64K subredes, considerado suficiente para todos menos las redes mas grandes hoy en día. Dentro del /48, la unidad mas pequeña que puede ser asignada es un /64 – entonces cada LAN y enlace punto a punto recibe un /64.

    Con este sistema modificado, el plan de direccionamiento de IPv6 se simplifica mucho. Cada ISP asigna un solo /48 para su red de infraestructura, y el resto del bloque de su /32 es usado para la asignación de clientes. En este taller se asume este principio.

11. **Direcciones IPv6.** Se va a asumir que cada ruteador es un ISP. Para el propósito de este suplemento vamos a asumir que la asignación mínima para el taller es /32 (la asignación realizada por un Registro Regional del Internet). Entonces cada equipo recibe un espacio de direcciones /32. Los equipos en los ruteador 3 y 10 reciben un espacio de direcciones /31 – no porque son especiales, sino que puede ser usado después de este modulo. La siguiente tabla indica la asignación de direcciones.

R1	**1001:10::/32**	**R8**	**1001:30::/32**
R2	**1001:11::/32**	**R9**	**1001:31::/32**
R3	**1001:12::/31**	**R10**	**1001:32::/31**
R4	**1001:20::/32**	**R11**	**1001:40::/32**
R5	**1001:21::/32**	**R12**	**1001:41::/32**
R6	**1001:22::/32**	**R13**	**1001:42::/32**
R7	**1001:23::/32**	**R14**	**1001:43::/32**

12. **Conexiones Punto a Punto Seriales**. Cada equipo ahora necesita asignar direcciones IPv6 a las conexiones seriales entre cada ruteador. Cada /32 permite al ISP asignar subredes /48 para clientes y su propia infraestructura. Se recomienda que cada equipo de ruteo toma un bloque de direcciones /48 y lo usa para sus necesidades de infraestructura del laboratorio. Dentro de cada asignación IPv6 /48 hay la posibilidad de 65536 subredes (la unidades de direccionamiento mas pequeño por LAN o enlace punto a punto es un /64). Cada equipo deberá usar la ultima /48 de los bloques de direccionamiento del /32 para su infraestructura. Por ejemplo, el Router 5 usará 1001:21:FFFF::/48 para enumerar su "infraestructura".

    Viendo el plan de direccionamiento en el Apéndice para algunas recomendaciones – usando el plan recomendado hará mas fácil el diagnostico.

    Nota que el lab no usa EUI-64 para el direccionamiento de interfaces, sino que asigna direcciones absolutas para cada interfase. Esto es mas fácil administrar, y mas fácil administrar relaciones con vecinos y enlaces punto a punto.

    Una configuración ejemplo puede ser como:

    ```
    Router2(config)# interface serial 0/0/0
    Router2(config-if)# ipv6 address 1001:11:ffff:1::1/64
    Router2(config-if)# clock rate 2000000
    Router2(config-if)# no shutdown
    ```

    P: ¿Que mascara de red se debe de usarse en todas las interfaces habilitadas para IPv6?
    R: La mascara de red deberá ser /64. Esta es el tamaño de subred para todas las LAN, enlaces punto a punto y demás. Mientras que algunos proveedores desean subdividir el /64 aun mas, esto va en contra del documento RFC3513 que especifica la arquitectura de direccionamiento IPv6. Entonces todos los enlaces punto a punto usan un /64, todos los LANs un /64, etc.

13. **Conexiones Ethernet.** Como en el paso anterior, hay que asignar direcciones IPv6 para cada enlace punto a punto Ethernet.

14. **Prueba de Ping #1.** Haga un Ping de todos las subredes físicamente conectadas a los ruteadores vecinos. Si las subredes físicamente conectadas no son alcanzables, consulte con el equipo del ruteador vecino para ver que puede ser el problema. No ignore el problema – no va a desaparecer. Utilice los siguiente comandos para hacer el diagnostico de la conexión:

    ```
    show ipv6 neighbors                          : Muestra el cache de vecinos IPv6
    show ipv6 interface <interfase> <numero>     : Estado del interfase y su configuración
    show ipv6 interface                          :Resumen del estado de interfaces y su configuración
    ```

15. **Asigna direcciones IPv6 a las interfaces Loopback.** Mientras que ninguna funcionalidad del ruteador usa la dirección de Loopback IPv6 todavía, todavía es útil configurar una dirección IPv6 aquí. Será usado para asociaciones iBGP en el lab. Nota que el ID del ruteador para los procesos de OSFP y BGP son enteros de 32 bits y IOS los deriva de la dirección IPv4 asignado a la interfase Loopback (esto puede ser un problema potencial para redes que no tienen IPv4 configurado).

    P. ¿Por qué cree que esto sea un problema? Pida al instructor que lo comente.

Como el tamaño mínimo de una subred para IPv6 es /64, vamos a asignar la ultima /64 de nuestro bloque de infraestructura /48 para los loopback. Aquí hay sugerencias del bloque de direcciones de cada equipo y su ruteador para las direcciones del Loopback (para las notas del lab se asume estas direcciones):

R1	**1001:10:ffff:ffff::1/64**	**R8**	**1001:30:ffff:ffff::1/64**
R2	**1001:11:ffff:ffff::1/64**	**R9**	**1001:31:ffff:ffff::1/64**
R3	**1001:13:ffff:ffff::1/64**	**R10**	**1001:33:ffff:ffff::1/64**
R4	**1001:20:ffff:ffff::1/64**	**R11**	**1001:40:ffff:ffff::1/64**
R5	**1001:21:ffff:ffff::1/64**	**R12**	**1001:41:ffff:ffff::1/64**
R6	**1001:22:ffff:ffff::1/64**	**R13**	**1001:42:ffff:ffff::1/64**
R7	**1001:23:ffff:ffff::1/64**	**R14**	**1001:43:ffff:ffff::1/64**

Para estos bloques, cada equipo deberá seleccionar UNA dirección para ser usado en el ruteador que están administrando. Para el propósito del taller, la primera dirección del bloque deberá ser usado (entonces xxxxxx:ffff::1/64 es la dirección de nodo). Por ejemplo, el equipo del Ruteador 1 asignará la siguiente dirección y mascara para el Ruteador 1:

```
Router1(config)#interface loopback 0
Router1(config-if)#ipv6 address 1001:10:ffff:ffff::1/64
```

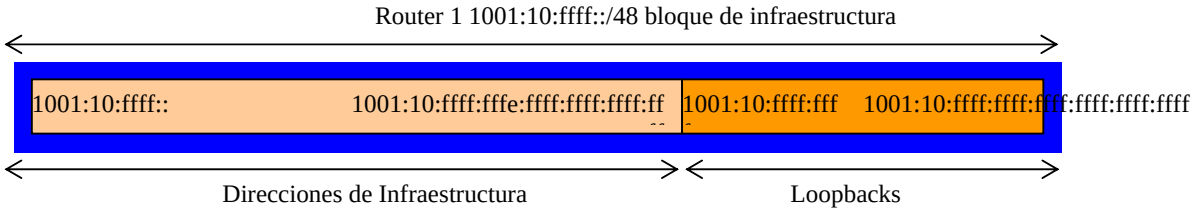

Figura 2 – Esquema de Direccionamiento de Loopback: Seleccionando el ultimo /64 del bloque asignado de /48

En el ejemplo en la figura 3 se muestra como el bloque de loopback/infraestructura queda dentro del esquema de direccionamiento de red del ISP.

16. **OSFP dentro del mismo sistema autónomo.** Cada equipo deberá habilitar OSPF para IPv6 en su ruteador. El número del proceso deberá ser 41 (ver ejemplo). (El identificador del proceso de OSPF es solo un número que identifica al proceso de OSPF en forma única dentro del ruteador. Esto no se pasa entre los ruteadores.) OSPF IPv6 se implementa un poco diferente del IPv4 en IOS – el ultimo usaba “network statements” para encontrar adyacencias e inyectar prefijos a la base de datos de enlaces (Link State Database). Para OSPF en IPv6, la configuración es independiente, como muestra el empleo a continuación. Nota que todas las interfaces deben de marcarse como pasivas por omisión:

```
Router1(config)#ipv6 router ospf 41
Router1(config-rtr)#passive-interface default
```

Una vez corriendo el proceso de OSPF, las interfaces de las cuales son en la base datos de enlaces (OSPF Link State Database) se deberán configurar. Esto se hace en la interfase específico, y se agrega el proceso OSFP, como muestra el ejemplo:

```
Router1(config)#interface loopback 0
```

```
Router1(config-if)#ipv6 ospf 41 area 0
!
Router1(config)#interface serial 0/0/0
Router1(config-if)#ipv6 ospf 41 area 0
!
...etc...
```

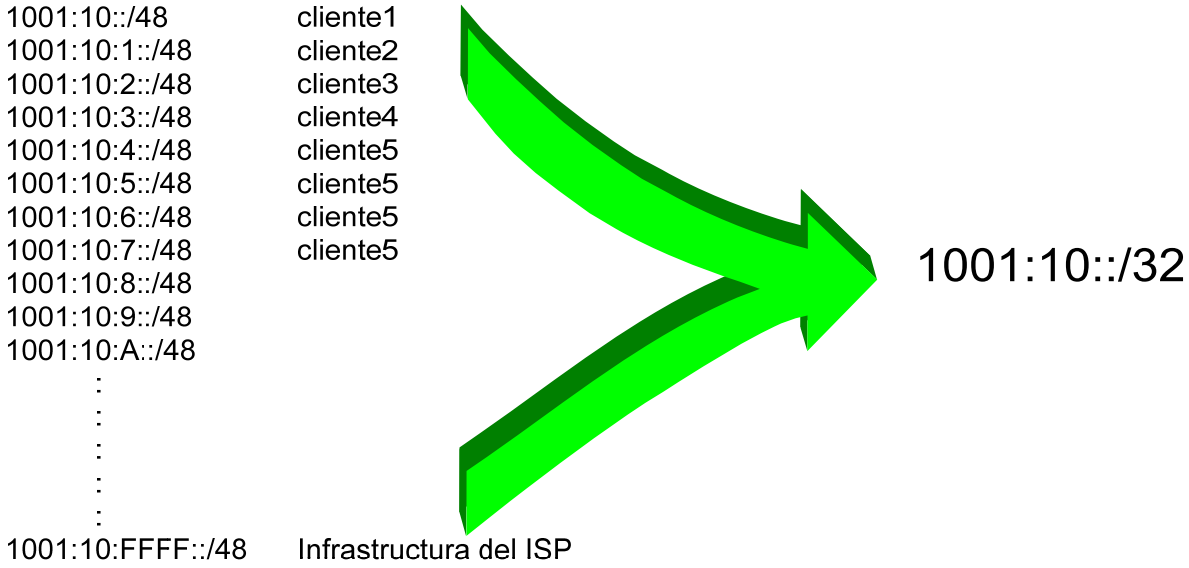

Figura 3 – Segmentos del plan de direccionamiento del ISP

Finalmente, las interfaces en que se espera formar adyacencias OSPF se deberán marcar como interfaces activas. Para esto, debemos de regresar al proceso principal de OSPF para marcar las interfaces con el subcomando *no passive-interface*:

```
Router1(config)#ipv6 router ospf 41
Router1(config-rtr)#no passive-interface serial 0/0/0
Router1(config-rtr)#no passive-interface FastEthernet 0/0
...etc...
```

Nota que la interfase loopback no tiene un no "network" asignado, no hay forma en que se puede conectarse a otro dispositivo de manera que pueda formar una adyacencia OSPF.

17. **Adyacencias en OSPF.** Habilite *logging* para los cambios de en las adyacencias de OSPF. Con esto cada vez que el estado de un vecino en OSPF cambia, se genera una notificación y es útil para propósitos de depuración:

```
Router2(config)#ipv6 router ospf 41
Router2(config-rtr)#log-adjacency-changes
```

18. **(Opcional). Habilite la traducción de nombres para OSPF en los ruteadores.** Siguiendo el paso anterior, ahora habilite la traducción de direcciones IP a nombres para OSPF en el ruteador.

```
Router2(config)#ipv6 ospf name-lookup
```

Con este comando habilitado se despliega los identificadores de los ruteadores en OSPF con sus nombres de dominio. Entonces en vez de desplegar los id-router con la traducción deshabilitado como sigue:

```
router2>sh ipv6 ospf neigh

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
100.1.15.224      1   FULL/BDR        00:00:36    1               Ethernet0/0
100.2.15.224      1   FULL/  -        00:00:32    2               Serial0/0
100.4.63.224      1   FULL/DR         00:00:38    3               Ethernet0/1
```

ahora el ruteador va a desplegar como sigue:

```
router2#sh ipv6 ospf neigh

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
router1.worksho   1   FULL/BDR        00:00:33    1               Ethernet0/0
router4.worksho   1   FULL/  -        00:00:39    2               Serial0/0
router14.worksh   1   FULL/DR         00:00:35    3               Ethernet0/1
```

lo cual tiene más información.

19. **Prueba de Ping #2.** Haga ping a todos las interfaces loopback en el taller. Esto asegura que el protocolo de ruteo interno OSPF esta conectado de extremo a extremo. Si hay problemas, utilice los siguientes comandos para determinar el problema:

```
show ipv6 route            : ver si hay una ruta para un destino
show ipv6 ospf             : ver información general de OSPF
show ipv6 ospf interface   : ver si OSPF esta habilitado en las interfaces deseadas
show ipv6 ospf neighbor    : ver la lista de vecinos de OSPF que el ruteador ve
```

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

20. **Configurando vecinos iBGP. (Primera Parte).** Todos los ruteadores usarán el Sistema Autónomo (AS) 10. La extensión para BGP para soportar múltiples protocolos se llama “address family” o familia de direcciones. *IPv4 unicast* es uno de los muchas familias que es soportado – es el que mas conocemos. IPv6 es otra familia de direcciones que es soportado por BGP multiprotocolo, y debemos de definir “peering” o asociaciones que corresponde a la familia de direcciones IPv6.

21. **Configurando vecinos iBGP. (Segunda Parte).** Ahora podemos configurar los vecinos iBGP para IPv6, como muestra el ejemplo del Ruteador 4 abajo. Utilice el comando *show bgp ipv6 summary* para verificar la asociación. La asociación de BGP se establecerá con la dirección IP del interfase loopback.

```
Router4(config)#router bgp 10
Router4 (config-router)#address-family ipv6
Router4 (config-router-af)#neighbor 1001:10:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:10:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:10:ffff:ffff::1 description iBGP con Router1
Router4 (config-router-af)#neighbor 1001:10:ffff:ffff::1 activate

Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:11:ffff:ffff::1 remote-as 10
```

```
Router4 (config-router-af)#neighbor 1001:11:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:11:ffff:ffff::1 description iBGP con Router2
Router4 (config-router-af)#neighbor 1001:11:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:13:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:13:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:13:ffff:ffff::1 description iBGP con Router3
Router4 (config-router-af)#neighbor 1001:13:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:21:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:21:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:21:ffff:ffff::1 description iBGP con Router5
Router4 (config-router-af)#neighbor 1001:21:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:22:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:22:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:22:ffff:ffff::1 description iBGP con Router6
Router4 (config-router-af)#neighbor 1001:22:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:23:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:23:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:23:ffff:ffff::1 description iBGP con Router7
Router4 (config-router-af)#neighbor 1001:23:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:30:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:30:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:30:ffff:ffff::1 description iBGP con Router8
Router4 (config-router-af)#neighbor 1001:30:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:31:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:31:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:31:ffff:ffff::1 description iBGP con Router9
Router4 (config-router-af)#neighbor 1001:31:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:33:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:33:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:33:ffff:ffff::1 description iBGP con Router10
Router4 (config-router-af)#neighbor 1001:33:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:40:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:40:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:40:ffff:ffff::1 description iBGP con Router11
Router4 (config-router-af)#neighbor 1001:40:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:41:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:41:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:41:ffff:ffff::1 description iBGP con Router12
Router4 (config-router-af)#neighbor 1001:41:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:42:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:42:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:42:ffff:ffff::1 description iBGP con Router13
Router4 (config-router-af)#neighbor 1001:42:ffff:ffff::1 activate
Router4 (config-router-af)#
Router4 (config-router-af)#neighbor 1001:43:ffff:ffff::1 remote-as 10
Router4 (config-router-af)#neighbor 1001:43:ffff:ffff::1 update-source loopback 0
Router4 (config-router-af)#neighbor 1001:43:ffff:ffff::1 description iBGP con Router14
Router4 (config-router-af)#neighbor 1001:43:ffff:ffff::1 activate
```

P. ¿Por qué es necesario *update-source loopback 0* en iBGP?

Utilice *show bgp ipv6 summary* para verificar el estado de las conexiones con los vecinos iBGP IPv6. Si la sesión iBGP no esta arriba y/o no recibe actualizaciones, trabaja con el equipo de ruteo de la conexión vecina para hacer un diagnostico.

22. **Prueba de Sanidad.** Recuerde utilizar los siguientes comandos para asegurar que esta recibiendo la información que debe recibir:

```
show ipv6 ospf              : ver información general de OSPF IPv6
show ipv6 ospf interface    : ver la lista de interfaces OSPF IPv6 que ve el ruteador
show ipv6 ospf neighbor     : ver la lista de vecinos OSPF IPv6 que ve el ruteador
show ipv6 ospf database     : ver la base de datos del estado de enlaces que el ruteador ha
                            : aprendido para OSPF IPv6
show bgp summary            : ver la lista de peers iBGP IPv6 que ve el ruteador
show bgp ipv6 unicast       : ver la lista de caminos BGP IPv6 que ve el ruteador
show ipv6 route             : ver todas las rutas IPv6 que el ruteador tiene instalado
```

P. ¿Existen rutas que se ven con ***show bgp ipv6***? ¿Sino, por que? ¿Hay rutas marcadas con "B" cuando hace ***show ipv6 route***?

23. Agrega Redes con BGP. Cada equipo de ruteo usará BGP para anunciar el bloque de direcciones asignado a ellos anteriormente en este modulo. Por ejemplo, el equipo del ruteador 1 agregará:

```
Router1 (config)#router bgp 10
Router1 (config-router)#address-family ipv6
Router1 (config-router-af)#network 1001:10::/32
```

Utilice *show bgp ipv6* en el ruteador del vecino para ver si esta anunciando su red via BGP.

P. ¿Se ve la red en BGP? ¿Sino, por que?

Agrega una ruta estática para el bloque CIDR (Classless Inter Domain Routing). Por ejemplo en el ruteador 1 utilice:

```
Router1 (config)#ipv6 route 1001:10::/32 Null0
```

P. ¿Aparece la red en BGP del vecino? Utilice el comando ***show bgp ipv6 neighbor <dirección IP del vecino> advertised-routes*** para ver que esta exportando al otro ruteador. Físicamente visite uno de los ruteadores de los vecinos para verificar su tabla de BGP. Explica lo que ve.

P. ¿Se ve la red en la tabla de "forwarding" del ruteador? Utilice el comando ***show ip route*** para ver la tabla de "forwarding" local. ¿Sino, por que?

24. Agregue los siguientes comandos a BGP:

```
Router1 (config)#router bgp 10
Router1 (config-router)# address-family ipv6
Router1 (config-router)# no synchronization
```

P. ¿Aparece la red en BGP del vecino? Utilice el comando ***show ip route*** para ver la tabla de "forwarding". ¿Qué hace el comando *no synchronisation* en BGP? ¿Cómo afecta la tabla de "forwarding" del ruteador?

Nota: A partir de la versión IOS 12.3, sincronización esta deshabilitado por omisión y ya no aparece en la configuración de BGP.

Punto de Verificación #2 : *Llame al asistente del laboratorio para verificar la conectividad.*

25. **Traceroute a todos los ruteadores.** Una vez que hace ping a todos los ruteadores, prueba haciendo trace a las rutas de todos los ruteadores usando el comando *trace x.x.x.x*. Por ejemplo, el equipo de ruteador 1 teclea:

```
Router1# trace 1001:41:ffff:ffff::1
```

para hacer trace al ruteador 12. Si el trace expira el tiempo debido a destino no alcanzable, es posible interrumpir el *traceroute* usando la secuencia de break de Cisco CTRL-^.

P. ¿Por qué algunos trace muestran múltiples direcciones IP por salto?

R. Si existe un o mas caminos de igual costo, OSPF va a "balancear" el trafico entre esos caminos.

```
Router1>trace 1001:41:ffff:ffff::1

Type escape sequence to abort.
Tracing the route to 1001:41:ffff:ffff::1

  1 1001:10:ffff::2   4 msec
    1001:10:ffff:2::2 0 msec
    1001:10:ffff::2   0 msec
  2 1001:42:ffff::2   4 msec
    1001:11:ffff:2::2 4 msec
    1001:42:ffff::2   0 msec
  3 1001:43:ffff::2   4 msec *  4 msec
Router1>
```

26. **Otras funcionalidades de OSPF y BGP.** Revise la documentación o utilice el comando help o tecleando*?* para ver otros comandos *show* en OSPF y BGP.