

## Módulo 2 – Práctica de Configuración Básica de eBGP

**Objetivo:** Simular cuatro ISPs diferentes utilizando una combinación de OSPF, BGP interno (iBGP) y BGP externo (eBGP).

**Prerrequisitos:** Módulo 1

Topología:

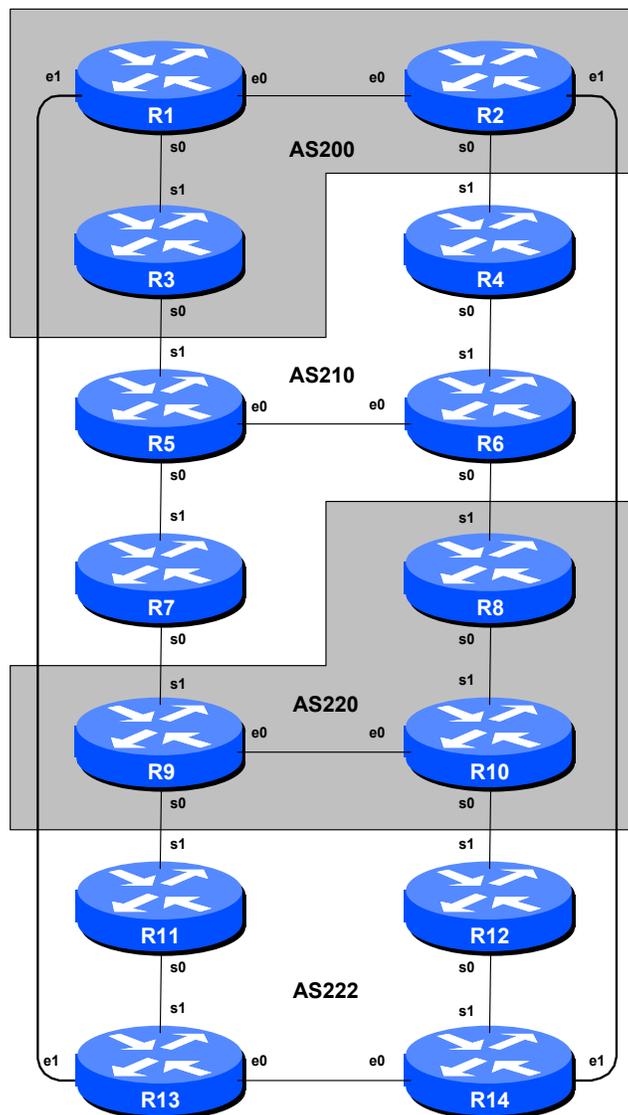


Figura 1 – Números de AS para BGP

martes, julio 20, 2004

## Notas del Laboratorio

El propósito de este módulo es familiarizar al estudiante con la configuración de BGP externo (eBGP). eBGP es utilizado para definir la relación entre diferentes sistemas autónomos en una red de IP. El taller estará dividido en cuatro redes diferentes, y los equipos que pertenecen a cada una de las redes trabajarán juntos como parte del mismo ISP. Cada AS tiene dos conexiones a sus ASs vecinos, y esta configuración será utilizada en gran parte de este taller.

La conectividad mostrada en los diagramas representa los enlaces entre los diferentes ASs. Se asume que todos los enrutadores dentro del mismo sistema autónomo están físicamente conectados directamente, como se muestra en la Figura 1.

## Ejercicios de Laboratorio

1. Conectar los enrutadores como se muestra en la figura no. 1. Todos los enrutadores dentro de un AS deben estar físicamente conectados y respondiendo. La relación entre los diferentes ASs se muestra en la Figura 2 y representa una visión similar a la del “mundo real”.

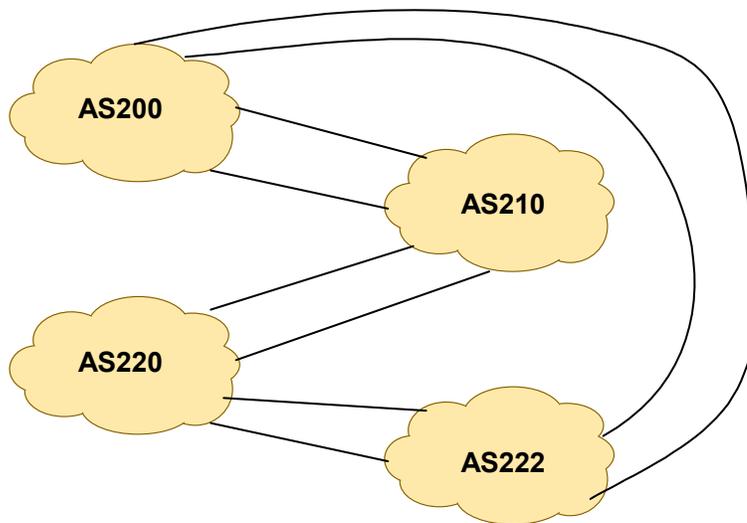


Figura 2 – Relación Entre ASs

2. Las direcciones utilizadas por los enlaces entre los enrutadores deberán ser las mismas que se utilizaron en el Módulo 1.
3. **Reconfigure OSPF y BGP.** En cada enrutador, elimine los procesos de OSPF y BGP, que se crearon en el Módulo 1, utilizando los siguientes dos comandos:

```
Router1 (config)# no router bgp 100
```

```
Router1 (config)# no router ospf 100
Router1 (config)# no ipv6 router ospf 100
Router1 (config)# exit
```

Estos comandos eliminarán la configuración de OSPF y BGP para comenzar desde cero en este módulo.

- 4. Configure un Número de Sistema Autónomo.** Aunque este paso no es un requisito para la configuración de BGP, el uso del comando *autonomous-system* mantiene de número de AS asignado, lo cual ayuda a los técnicos trabajando en la solución de problemas. Cada equipo de trabajo deberá utilizar este comando en su enrutador, utilizando su Nuevo número de AS (ver Figura 1). Por ejemplo:

```
Router1 (config)# autonomous-system 200
```

- 5. Configure OSPF en los enrutadores dentro del mismo AS.** Dentro de cada AS, configure los procesos de enrutamiento de OSPF. Esto quiere decir que las subredes utilizadas en los enlaces entre los enrutadores dentro del AS, deberá ser configurada en los procesos de OSPF utilizando el comando *network* dentro de OSPF. Todos los enrutadores dentro de un AS, estarán dentro de la misma *area 0* de OSPF y utilizarán el mismo número de identificación (ID) de OSPF. Por ejemplo, el Equipo de Trabajo 1, con dos interfaces en el mismo AS, deberá configurar su enrutador de la siguiente forma:

```
Router1 (config)# router ospf 200
Router1 (config-router)# network 200.200.4.0 0.0.0.3 area 0      ! eth0/0
Router1 (config-router)# network 200.200.5.0 0.0.0.3 area 0      ! ser0/0
Router1 (config-router)# network 200.200.6.0 0.0.0.3 area 0      ! eth0/1
Router1 (config-router)# network 200.200.7.224 0.0.0.0 area 0    ! loop0
Router1 (config-router)# passive-interface loopback 0
Router1 (config-router)# passive-interface ethernet 0/1
Router1 (config-router)# log-adjacency-changes
Router1 (config-router)# exit
Router1 (config)# ipv6 router ospf 200
Router1 (config-rtr)# redistribute connected
Router1 (config-rtr)# log-adjacency-changes
Router1 (config-rtr)# exit
```

Notas:

- *Passive-interface* previene que el proceso de OSPF trate de establecer adyacencias en las redes de DMZ. Este comando **DEBE** ser utilizado para cada interfase en la que no se quiere o debe correr OSPF. En el caso de IPv6, en lugar de definir una interfase como pasiva durante la configuración del proceso de OSPFv3, no se define el proceso durante la configuración de la interfase (como se había visto durante el módulo 1).
- El número que sigue al comando “*router ospf*” es el número de identificación (ID) del proceso de OSPF y tiene significado únicamente dentro del enrutador (por lo que se puede utilizar cualquier número). Sin embargo, para este laboratorio recomendamos que ID del proceso de OSPF sea el mismo que el número de AS (que es lo que un buen número de ISPs hace).

martes, julio 20, 2004

- 6. Asegurarse de que hay conectividad.** Verificar las rutas vía OSPF. Asegurarse de que se pueden ver todas las subredes/prefijos dentro de su AS. Haga un ping a todas las interfaces de loopback de los enrutadores dentro de su AS. Utilice los comandos “*show ip ospf neighbor*” y “*show ip route*”. Si no puede ver los otros enrutadores dentro de su AS, va a tener problemas cuando trate de configurar BGP en los próximos pasos
- 7. Grabar la configuración.** No se olvide de grabar la configuración en NVRAM!

**Chequeo #1** : consulte con los asistentes de laboratorio para verificar su conectividad.

- 8. Configure una sesión de iBGP entre los enrutadores en el mismo AS.** Use la dirección de la interfase de loopback para las sesiones de iBGP. También utilice el comando *network* de BGP para integrar los bloques CIDR, asignados a cada Equipo de Trabajo, para que sean anunciados por BGP.

```
Router1 (config)# router bgp 200
Router1 (config-router)# no synchronization
Router1 (config-router)# network 200.200.4.0 mask 255.255.252.0
Router1 (config-router)# neighbor 200.200.11.224 remote-as 200
Router1 (config-router)# neighbor 200.200.11.224 update-source loopback 0
Router1 (config-router)# neighbor 200.200.11.224 description iBGP Link a R2
Router1 (config-router)# neighbor 200.200.19.224 remote-as 200
Router1 (config-router)# neighbor 200.200.19.224 update-source loopback 0
Router1 (config-router)# neighbor 200.200.19.224 description iBGP Link a R3
Router1 (config-router)# no auto-summary
Router1 (config-router)# neighbor FEC0:200:8:11::1 remote-as 200
Router1 (config-router)# neighbor FEC0:200:8:11::1 update-source loopback 0
Router1 (config-router)# neighbor FEC0:200:8:11::1 description iBGP ipv6 a R2
Router1 (config-router)# neighbor FEC0:200:16:19::1 remote-as 200
Router1 (config-router)# neighbor FEC0:200:16:19::1 update-source loopback 0
Router1 (config-router)# neighbor FEC0:200:16:19::1 description iBGP ipv6 a R3
Router1 (config-router)# address-family ipv6
Router1 (config-router-af)# network FEC0:200:4::/48
Router1 (config-router-af)# neighbor FEC0:200:8:11::224 activate
Router1 (config-router-af)# neighbor FEC0:200:16:19::224 activate
Router1 (config-router-af)# exit
Router1 (config-router)# exit
Router1 (config)# ip route 200.200.4.0 255.255.252.0 Null0 250
Router1 (config)# ipv6 route FEC0:200:4::/48 Null0 250
```

**P:** Necesita utilizar el comando *no synchronization* de BGP? Por qué?

**R:** La red de un ISP es una red de **transito**. Esto quiere decir que el ISP acepta paquetes de otros ISPs con los que tiene sesiones de BGP, los transmite a través de su backbone, y al final los pasa hacia otro AS o ISP para que lo acerque a su destino final. Para asegurarse que los enrutadores

internos al AS puedan transmitir los paquetes de tránsito (desde el enrutador de entrada hacia el enrutador de salida), todos los enrutadores que corren BGP en el borde deben esperar a que el anuncio del prefijo de la subred arribe a través del IGP (puesto que todos estos enrutadores participan en el mismo IGP) antes anunciarlo en las sesiones externas de BGP. El proceso descrito mas arriba se denomina *sincronización*. En otras palabras, los enrutadores internos deben tener conocimiento, vía un IGP, de los prefijos que los enrutadores del borde aprendieron vía iBGP.

Se debe considerar que este proceso aplica a ambientes donde las rutas aprendidas a través de BGP son redistribuidas en el IGP. Un ISP típico, normalmente no haría esto puesto la tabla de enrutamiento del Internet son bastante grandes. En su lugar, el ISP corre iBGP en una malla completa (o utiliza reflectores de rutas) entre todos los enrutadores en el backbone. En este tipo de ambiente, el proceso de sincronización debe ser deshabilitado.

**P.** Por qué se necesita el comando *no auto-summary* en BGP?

**R.** Por defecto los prefijos inyectados en BGP son automáticamente sumariados al prefijo de **clase completa (classful)** mas cercano. Como en el Internet no se utilizan las direcciones de clase, el proceso de agregación automática debe ser deshabilitado. Por ejemplo, si la agregación automática está habilitada y un ISP con un sistema autónomo está utilizando prefijos de direcciones de lo que antes se conocía como un bloque de clase A, BGP anunciaría un prefijo /8 en lugar del bloque de direcciones realmente en uso. Aunque en este laboratorio solo estaremos utilizando bloques de direcciones de lo que antes se conocía como clase C y por lo tanto no se requiere el utilizar el comando *no auto-summary*, es una buena práctica común de que este comando sea parte de la configuración de BGP en todos los enrutadores de un ISP.

**9. Verifique la conectividad de BGP interno (iBGP).** Utilice los comandos de visualización de BGP para verificar que se están recibiendo las rutas anunciadas por todos los enrutadores dentro de su AS.

**10. Configure la sesión de eBGP.** Utilice la Figura 1 para determinar los enlaces entre los diferentes ASs. Para los enlaces entre dos ASs se utilizarán las direcciones de las interfases punto-a-punto, no las direcciones de las interfaces de loopback.

```
Router1 (config)# router bgp 200
Router1 (config-router)# neighbor 200.200.6.2 remote-as 222
Router1 (config-router)# neighbor 200.200.6.2 description eBGP to Router13
Router1 (config-router)# neighbor FEC0:200:4:6::2 remote-as 222
Router1 (config-router)# neighbor FEC0:200:4:6::2 description eBGP ipv6 a Router13
Router1 (config-router)# address-family ipv6
Router1 (config-router-af)# network FEC0:200::/32
Router1 (config-router-af)# neighbor FEC0:200:4:6::2 activate
Router1 (config-router-af)# exit
Router1 (config-router)# exit
Router1 (config)# ipv6 route FEC0:200::/32 Null0 250
```

martes, julio 20, 2004

Utilice los comandos de visualización de BGP para verificar que se están enviando y recibiendo los anuncios de BGP de los vecinos.

**P.** Por qué no se debe utilizar las interfaces de loopback para las sesiones de eBGP?

**R.** La dirección de IP de la interfase de loopback del enrutador no es conocida por los vecinos de BGP externo, y por lo tanto los vecinos no tienen forma de comunicarse y establecer la sesión.

**P.** Cuál comando de visualización de BGP permite ver el estado de la conexión de BGP con los vecinos?

**R.**

**IPv4:** Trate *show ip bgp neighbor x.x.x.x* – el resultado del comando presenta información detallada sobre el estado de la sesión con el vecino. Este comando también tiene sub-comandos que permiten ver información más específica sobre la sesión.

**IPv6:** Trate *show bgp ipv6 neighbor x::x::x::x::x::x* – al igual que el comando para IPv4, el resultado presenta información detallada sobre el estado de la sesión con el vecino. Este comando también tiene sub-comandos que permiten ver información más específica sobre la sesión.

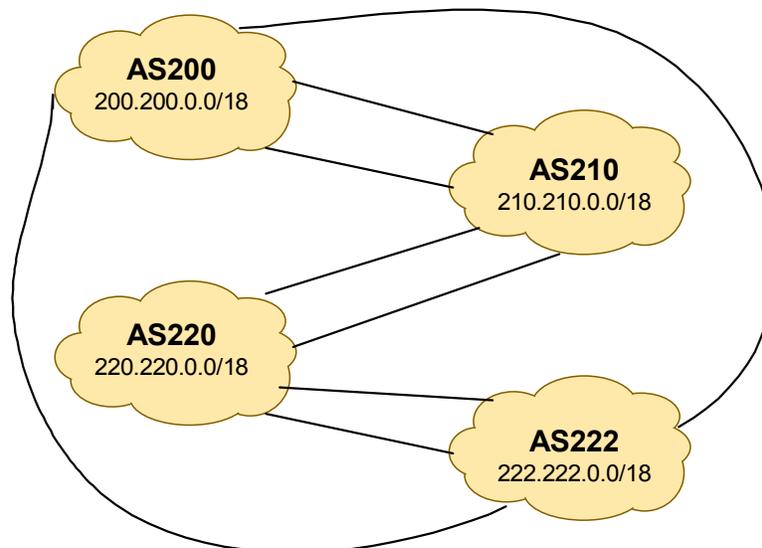


Figure 3 – Aggregates for each ASN

**P.** Qué comando de visualización de BGP permite ver cuales prefijos están siendo anunciados hacia un vecino y cuales prefijos se están recibiendo desde un vecino de BGP?

**A.**

**IPv4:** Trate `show ip bgp neighbor x.x.x.x routes` – el resultado del comando muestra las rutas que han sido aprendidas desde el vecino luego de haber evaluado las políticas de entrada. Si se reemplaza el parámetro `routes` con `received-routes`, se pueden ver los prefijos que están siendo recibidos desde el vecino antes de que las políticas sean aplicadas. De igual forma, si se reemplaza el parámetro `routes` con `advertised-routes` se pueden los prefijos anunciados hacia el vecino luego de que las políticas han sido aplicadas.

**IPv6:** Trate `show bgp ipv6 neighbor x:x:x:x:x:x:x routes` – el resultado es similar al del comando utilizado para IPv4. Al igual que en IPv4, también se pueden visualizar los prefijos anunciados y recibidos.

- 11. Agregar los bloque CIDR de cada uno de los ASs.** Los bloques CIDR /22 que pertenecen a cada uno de los equipos de trabajo, pueden ser agregados en un bloque CIDR mayor /18. Esto permite que los ISPs tengan bloques pequeños diseminados en su red pero agregarlos al momento de anunciarlos hacia afuera de su AS.

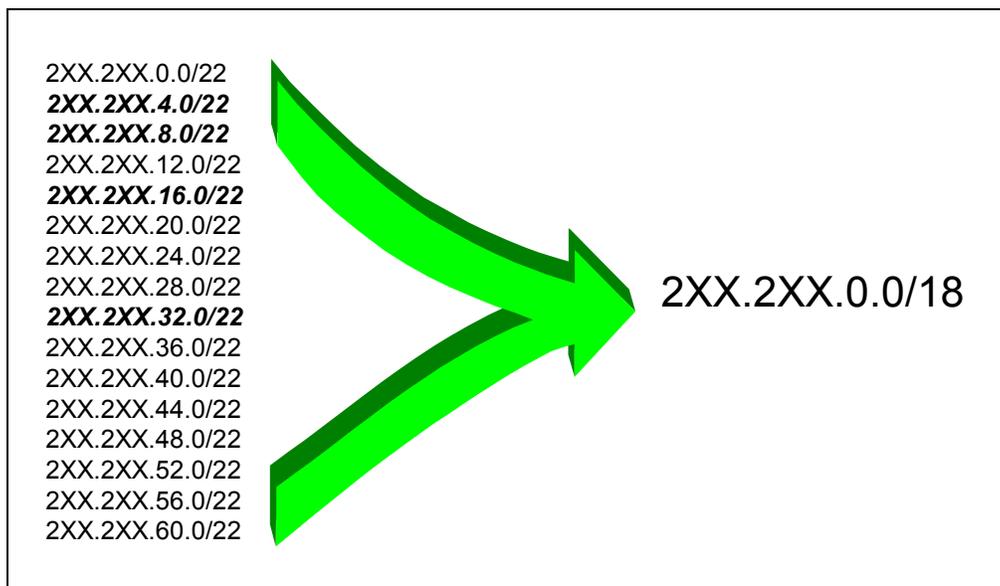


Figure 4 – Aggregating all potential /22s into a /18

**P.** Cómo se puede agregar automáticamente un grupo de bloques CIDR pequeños en uno más grande al momento de anunciarlo hacia los vecinos vía BGP? **Sugerencia:** Revisar la documentación de BGP.

martes, julio 20, 2004

## R. Configure:

```
Router1(config)# router bgp 200
Router1(config)# aggregate-address 200.200.0.0 255.255.192.0
```

Escriba ? después del comando para ver que opciones están disponibles para el comando.

- 12. Verifique las rutas y caminos que se han aprendido.** Ejecute comandos *traceroute* hacia las estaciones especificadas por el instructor.

***Chequeo #2 :*** consulte con los asistentes de laboratorio para verificar su conectividad. Utilice los comandos “*show ip route sum*”, “*show ip bgp sum*”, “*show ip bgp*”, “*show ip route*”, and “*show ip bgp neigh x.x.x.x routes | received-routes | advertised-routes*”. Deberá haber 13 prefijos específicos y 4 prefijos agregados (uno por cada ISP).

**[Recuerda que para IPv6 se debe intercambiar el orden de las palabras claves *ip* y *bgp* ]**

- 13. (Opcional)** Utilice el comando *debug ip bgp update* para ver los mensajes de actualización luego de haber re-inicializado la sesión de BGP.

- 14.** Utilice el comando de BGP *aggregate-address* para sumarizar todos los anuncios entre los vecinos de eBGP. Luego de implementado, la tabla de enrutamiento de BGP solo debería tener el prefijo de iBGP generado localmente (puesto que todos los otros enrutadores dentro del AS también implementaron la opción de *summary-only*), la ruta agregada de los demás enrutadores dentro del AS, y los tres prefijos agregados por los otros ISPs en el laboratorio.

```
Router1(config)# router bgp 200
Router1(config)# aggregate-address 200.200.0.0 255.255.192.0 summary-only
```

***Chequeo #3 :*** consulte con los asistentes de laboratorio para verificar que el proceso de agregación está funcionando correctamente. Utilice los comandos “*show ip route sum*”, “*show ip bgp sum*”, “*show ip bgp*”, “*show ip route*”, and “*show ip bgp neigh x.x.x.x routes | received-routes | advertised-routes*”. Deberá haber un prefijo específico, generado localmente, y 4 prefijos agregados (uno por cada ISP).

**[Recuerda que para IPv6 se debe intercambiar el orden de las palabras claves *ip* y *bgp* ]**

- 15.** Examine el *origen (origin)* de los prefijos. ¿Cuál es el tipo de origen para los prefijos agregados?

- 16.** Elimine la opción de agregación.

```
Router1(config)# router bgp 200
Router1(config)# no aggregate-address 200.200.0.0 255.255.192.0 summary-only
```

```
Router1(config)# aggregate-address 200.200.0.0 255.255.192.0
```

17. Examine el *origen (origin)* de los prefijos. ¿Cuál es el tipo de origen para los prefijos agregados?

### ***Preguntas de Repaso***

1. ¿Cuántos tipos de origen (**origin**) existen en BGP?
2. Mencione los tipos de origen. **Sugerencia:** *Revisar la documentación de BGP.*
3. ¿Para que es utilizada la información de origen?

martes, julio 20, 2004

## ***NOTAS DE CONFIGURACIÓN***

La documentación es crítica. Usted deberá salvar y documentar la configuración en cada punto de chequeo y al final de este módulo.