

Modulo 4 – Laboratorio sobre Estrategias Multihoming

Objetivo: Demostrar algunas de las opciones de configuración y políticas de enrutamiento disponibles en topologías Multihoming (conectividad con más de un AS o Sistema Autónomo).

Prerrequisito: Módulo 2

Topología :

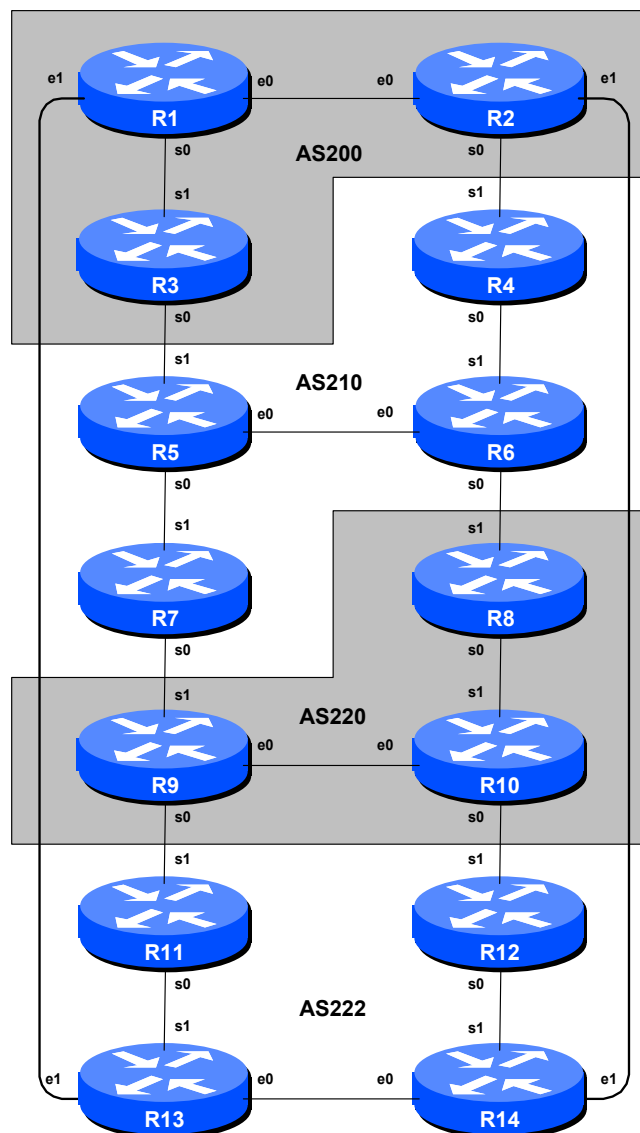


Figura 1 – Números de AS en BGP

Notas

Este módulo demuestra cómo un AS puede usar el parámetro LOCAL PREFERENCE para controlar múltiples caminos asignados de enrutamiento saliente, y cómo usar los parámetros AS PATH y MEDs (Discriminadores o Métricas de Múltiple salida) para determinar rutas asignadas para enrutamiento o tráfico entrante. Estos parámetros se constituyen en herramientas muy poderosas para los ISPs con el fin de controlar cómo las conexiones de Peering o de vecindad serán utilizadas. Revise la documentación de BGP para obtener más información acerca del proceso de selección de rutas de BGP y los valores por defecto y prioridades de los atributos LOCAL PREF y METRIC.

Antes de empezar este módulo, mantenga la topología y configuraciones usadas en Módulo 2. Esto requiere el levantamiento de todas las configuraciones de filtros y configuraciones de comunidad examinados en Módulo 3.

Consejo: Recuerde, si cualquier configuración en un router no está en uso, **deberá ser quitada**. La configuración existente normalmente da lugar a detección de errores tardíos y de depuración de las configuraciones, en casos de notar problemas de enrutamiento u otras fallas de la red.

Los enlaces mostrados en la Figura 1 representan la conectividad entre los AS's. Se asume que todos los routers dentro de un AS se conectan con otros.

Ejercicio de Laboratorio

1. Publicar la ruta agregada del AS

- Asegúrese que su AS está enviando un prefijo agregado para todas las rutas en el AS, junto con las rutas más específicas usando el comando *aggregate-address*.

Ejemplo:

AS 200 anunciará 200.200.0.0/16 y sus subredes al AS 210 y AS 222.

AS 222 anunciará 222.222.0.0/16 y sus subredes a AS 200 y AS 220.

Etc...

- Revise las tablas de enrutamiento y ejecute pruebas de *ping & traceroute* para confirmar que existe conectividad.
- Pruebe conectividad y enrutamiento, deshabilitando enlaces a los Vecinos externos y luego repitiendo el comando Traceroute, el cual debería mostrar la ruta alternativa calculada por BGP cuando la ruta primaria falla.

Consejo: Incluya *soft-reconfiguration* en los vecinos eBGP de su ruteador. La configuración de su ruteador debería ser la misma que al final del módulo 3, pero sin las configuraciones de comunidad, los *route-maps* y las listas de comunidades.

Punto de Control #1: Llame a su instructor de Laboratorio y muestre lo siguiente:

ij Salida de “**show ip route**” y “**show ip bgp**”

ii Resultado de ‘**ping**’ y ‘**trace**’ a varios destinos dentro de la red.

iii Resultado de comandos ‘**ping**’ y ‘**trace**’ después que el enlace primario falla.

- 2. Arreglos del Módulo 3.** Si el módulo anterior completado fue el Módulo 3, la configuración del router necesita ser verificada substancialmente antes de que pueda iniciar esta práctica. Los pasos siguientes muestran lo que se requiere exactamente.

Ejemplo: Router R1

```
Router1#conf t
Router1(config)#router bgp 200
!
! Primero quite BGP dampening
!
Router1(config-router)#no bgp dampening
!
! Ahora quite el route-map de su vecino BGP
!
Router1(config-router)#no neighbor 200.200.6.2 route-map infiltrer in
Router1(config-router)#no neighbor FEC0:200:4:6::2 route-map infiltrer in
!
! Ahora quite el community-tag del comando network
!
Router1(config-router)#no network 200.200.4.0 mask 255.255.252.0 route-map
community-tag
Router1(config-router)#network 200.200.4.0 mask 255.255.252.0
Router1(config-router)#no network FEC0:200:4::/48 route-map community-tag
Router1(config-router)#network FEC0:200:4::/48
!
! Quite los route-maps
!
Router1(config)#no route-map community-tag
Router1(config)#no route-map infiltrer
!
! Quite la lista de comunidades
!
Router1(config)#no ip community-list 1
!
! Esa es la configuración tal como debería estar.
!
Router1(config)#end
!
```

Thursday, September 23, 2004

```
! Ahora reinicie el peering BGP para que la política tenga efecto
!  
Router1#clear ip bgp 200.200.6.2 soft  
Router1#clear bgp ipv6 FEC0:200:4:6::2 soft
```

3. Objetivo del Módulo:

El objetivo del módulo es demostrar cómo lograr un flujo de tráfico particular utilizando tres métodos diferentes. Estos tres métodos involucran modificación de políticas para tráfico de salida, y dos maneras de modificar la política de tráfico entrante. El lector debe revisar la presentación de BGP dada previamente a este módulo como una forma de recordar cómo influir o cambiar las opciones de selección de rutas usando las políticas de BGP.

El siguiente diagrama muestra los flujos de tráfico que son deseados entre ruteadores en particular y sus respectivos Sistemas Autónomos.

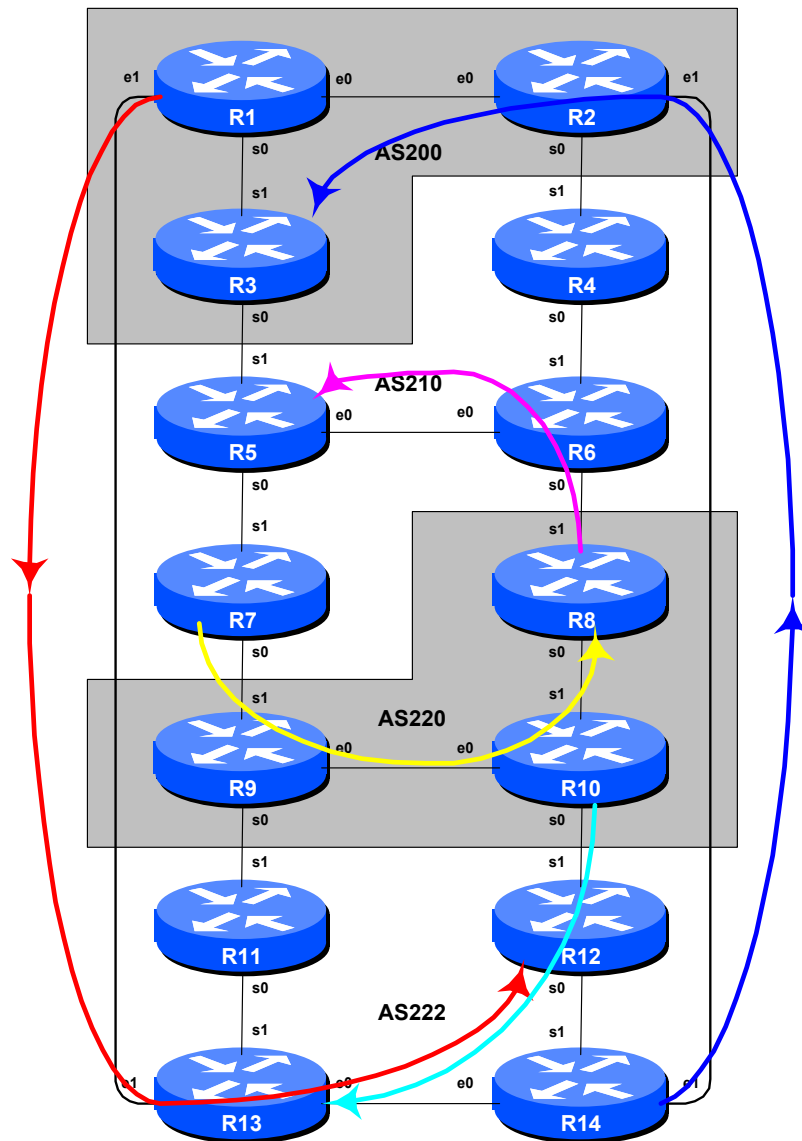


Figura 2 – Rutas Preferidas

Seis rutas diferentes para el manejo de tráfico están siendo implementadas. Las flechas de la figura #2 muestran cómo debe ser configurado dicho tráfico. Cada flecha se origina en un router de borde o frontera en un AS, y termina en un router ubicado en otro AS. Esto significa o representa el flujo de tráfico deseado entre los dos sistemas. Cada uno de los siguientes pasos tiene una descripción de cómo puede ser implementado el flujo de tráfico representado por las flechas.

Si en cualquier momento tiene dudas acerca de la configuración requerida, consulte el CD con la documentación de Cisco o pregunte a los instructores.

4. Implemente las siguientes políticas de Salida:

Discuta entre los equipos dentro del mismo AS y negocie con sus AS's vecinos cómo implementar cada una de las siguientes políticas en sus ruteadores. Es importante que los caminos auxiliares o redundantes funcionen. Basado en el método convenido, configure las rutas primarias siguientes:

AS 200:

- Todo el tráfico **PARA** 222.222.8.0/22 y FEC0:222:8::/48 (R12) debe salir del AS 200 via Router R1 solamente.

AS 210:

- Todo el tráfico **PARA** 220.220.4.0/22 y FEC0:220:4::/48 (R8) debe salir del AS 210 via Router R7 solamente.

AS 220:

- Todo tráfico **PARA** 210.210.8.0/22 y FEC0:210:8::/48 (R5) debe salir del AS 220 via Router R8 solamente.
- Todo tráfico **PARA** 222.222.16.0/22 y FEC0:222:16::/48 (R13) debe salir del AS 220 via Router R10 solamente.

AS 222:

- Todo tráfico **PARA** 200.200.16.0/22 y FEC0:200:16::/48 (R3) debe salir del AS 222 via Router R14 solamente.

Note que sólo estamos intentando definir el flujo de tráfico saliente. El camino del retorno no tiene ninguna política aplicada, y el ruteador aplica un proceso de decisión de ruta normal.

Consejos:

- ¿Recuerda que en el paso 1 el ruteador fue configurado para anunciar la ruta agregada así como las redes específicas en cada AS? Por consiguiente, y basados en este hecho, use la "preferencia local" internamente para influir en la ruta de salida fuera de su sistema autónomo. Ponga el router preferido a un valor más alto que el valor predeterminado, y los ruteadores menos preferidos a un valor más bajo que el valor predeterminado.
- Utilizar filtros de rutas no es una buena forma de conseguir las políticas planteadas. Usted necesitará permitir una ruta alternativa de re-enrutamiento en caso de que ocurran fallas. Utilizando LOCAL PREFERENCE se permite esto.
- Dibujar la topología de su sistema autónomo y el bloque de direcciones asignadas en una hoja en blanco. Discutir dentro de su equipo de trabajo y dentro de su propio AS, qué equipo debería estar aplicando la configuración como Frontera del sistema Autónomo. Es importante definir esta estrategia antes de ingresar la configuración en el ruteador.

Las configuraciones del ejemplo indicado a continuación deben usarse como la guía para la configuración del ruteador de cada equipo de trabajo. Note que un ruteador en cada AS tendrá que poner la preferencia local alta, los demás ruteadores en el AS pondrán la preferencia local baja. El objetivo de hacer esto es por redundancia de configuración. Por ejemplo, si el ruteador 7 pierde su configuración de la *local-preference* debido a algún error del operador, la preferencia local baja puesta en los otros tres ruteadores asegurará que todavía se llevarán a cabo las políticas de tráfico requeridas. Es bastante común para muchos ISPs tener más de una configuración para llevar a cabo una política particular - una configuración primaria, y una configuración secundaria "inversa" en otros ruteadores que podrían verse afectados.

Configuración de Ejemplo para el AS210 (usando el parámetro LOCAL_PREF):

Router 7:

```
ip prefix-list R8-prefix permit 220.220.4.0/22
!
route-map set-local-pref-high permit 10
  match ip address prefix-list R8-prefix
  set local-preference 200
!
route-map set-local-pref-high permit 20
!
router bgp 210
  neighbor 220.220.9.1 remote-as 220
  neighbor 220.220.9.1 route-map set-local-pref-high in
!
```

Router 4,5,6:

```
ip prefix-list R8-prefix permit 220.220.4.0/22
!
route-map set-local-pref-low permit 10
  match ip address prefix-list R8-prefix
  set local-preference 50
!
route-map set-local-pref-low permit 20
!
router bgp 210
  neighbor x.x.x.x remote-as ASN
  neighbor x.x.x.x route-map set-local-pref-low in
!
```

Haga lo mismo para IPv6:

Router 7:

```
ip prefix-list R8-v6-prefix permit FEC0:220:4::/48
!
route-map set-local-pref-high permit 10
```

Thursday, September 23, 2004

```
match ip address prefix-list R8-v6-prefix
set local-preference 200
!
route-map set-local-pref-high permit 20
!
router bgp 210
neighbor FEC0:220:32:9::1 remote-as 220
address-family ipv6
neighbor FEC0:220:32:9::1 activate
neighbor FEC0:220:32:9::1 route-map set-local-pref-high in
!
```

Punto de Control #2: Llame a su instructor y muestre lo siguiente:

ij) En cada ruteador de un sistema autónomo se hará un TRACE hacia destinos seleccionados; este deberá mostrar los paquetes salientes como se especifica en el ejercicio indicado.

ii) Explicar al instructor la configuración usada para lograr el resultado deseado. Muestre la salida de los comandos “show ip bgp”, y “show ip bgp x.x.x.x” para las redes configuradas con Local Preference de 200. Muestre la salida de un TRACE de acuerdo a las instrucciones.

iii) Antes de continuar espere la aprobación del instructor.

- 5. Quitar la configuración del paso anterior.** Antes de continuar es importante que la configuración ingresada en los pasos previos sea quitada. Esto implica quitar los *route-maps*, *prefix-lists* y la configuración de cada vecino para establecer la preferencia local. Todos los equipos de trabajo deberían hacer esto, y luego reestablecer los peerings de eBGP.
- 6. Implementar las siguientes políticas entrantes utilizando MEDs.** Este paso introduce uno de los dos métodos para aplicar políticas de tráfico entrante. Aquí se utilizan MEDs, mientras que el siguiente paso introduce el concepto del parámetro AS PATH. Así como en el paso previo, lea las instrucciones de forma cuidadosa, discútalas dentro de su equipo y de su sistema autónomo, y cómo usted va a llevar a cabo a lo siguiente.

El ejemplo en este paso logra exactamente el mismo flujo de tráfico entre los sistemas autónomos vecinos, como en el paso anterior para las redes en cuestión - recuerde que la preferencia local se usa por un AS para influenciar en las rutas de tráfico saliente, mientras que se usan MEDs para influir en las rutas de tráfico entrante. Refiérase a Figura 2 para tener una mejor idea del flujo de tráfico....

AS 200:

- Todo el tráfico HACIA 200.200.16.0/22 (R3) desde cualquier parte en el AS 222 debe entrar al AS 200 a través del enlace R14 – R2. (**Consejo:** Esto significa que el ruteador R1 debe anunciar la ruta 200.200.16.0/22 hacia AS 222 con una métrica más alta que la equivalente anunciada desde R2)

AS 210:

- Todo el tráfico HACIA 210.210.8.0/22 (R5) desde cualquier parte en el AS 220 debe ingresar al AS 210 a través del enlace R8 – R6. (**Consejo:** Esto significa que el ruteador R7 debe publicar 210.210.8.0/22 al AS 220 con una métrica mayor que la publicada desde R6).

AS 220:

- Todo el tráfico hacia 220.220.4.0/22 (R8) desde cualquier parte en AS210 debe entrar al AS 220 por medio del enlace R7 – R9. (**Consejo:** Esto significa que R8 debe publicar la ruta 220.220.4.0/22 al AS 210 con una métrica superior que la equivalente publicada desde R9).

AS 222:

- Todo el tráfico hacia la red 222.222.8.0/22 (R12) desde cualquier parte en AS 200 debe ingresar a AS 222 por medio del enlace R1 – R13. (**Consejo:** Esto significa que el ruteador R14 debe publicar la red 222.222.8.0/22 a AS 200 con una métrica mayor que la equivalente publicada desde R13.)
- Todo el tráfico hacia la red 222.222.16.0/22 (R13) desde cualquier parte en el AS 220 debe ingresar al AS 222 por medio del enlace R10 – R12. (**Consejo:** Esto significa que el ruteador R11 debe publicar 222.222.16.0/22 a el AS 220 con una métrica mayor que la publicada desde R12.)

Configuración de ejemplo para el AS210 (usando MED).**Router 6:**

```
ip prefix-list R5-prefix permit 210.210.8.0/22
!
route-map set-med-low permit 10
  match ip address prefix-list R5-prefix
  set metric 10
!
route-map set-med-low permit 20
!
router bgp 210
  neighbor 210.210.17.2 remote-as 220
  neighbor 210.210.17.2 route-map set-med-low out
```

Router 7:

```
ip prefix-list R5-prefix permit 210.210.8.0/22
!
route-map set-med-high permit 10
  match ip address prefix-list R5-prefix
```

Thursday, September 23, 2004

```
    set metric 50
    !
route-map set-med-high permit 20
    !
router bgp 210
    neighbor 220.220.9.1 remote-as 220
    neighbor 220.220.9.1 route-map set-med-high out
```

Para IPv6:

Router 6:

```
ipv6 prefix-list R5-v6-prefix permit FEC0:210:8::/48
!
route-map set-med-low permit 10
    match ip address prefix-list R5-v6-prefix
    set metric 10
!
route-map set-med-low permit 20
!
router bgp 210
    neighbor FEC0:210:16:17::2 remote-as 220
    address-family ipv6
        neighbor FEC0:210:16:17::2 activate
        neighbor FEC0:210:16:17::2 route-map set-med-low out
```

Notar que los equipos de trabajo con los ruteadores 3, 4, 5 y 10 tienen solamente que quitar la configuración que se agregó en el paso anterior. Ellos no necesitan configurar MEDs como se indica en el párrafo anterior, porque ellos no tienen Peerings o vecinos que requieran alteraciones en la política de tráfico entrante para su respectivo AS.

Punto de Control #3: Llame a su instructor y muestre lo siguiente:

ij Cada ruteador en su respectivo AS deberá hacer un ‘traceroute’ a destinos seleccionados, el cual deberá mostrar los paquetes salientes de su AS como se especifica en el ejercicio indicado arriba.

ii Explicar su configuración utilizada para lograr los resultados deseados al instructor. Muestre la salida de los comandos “show ip bgp”, y “show ip bgp x.x.x.x” para las redes con MED configurado en 50. Además muestre el resultado de un trace de acuerdo a las instrucciones.

7. Quitar la configuración utilizada en el paso anterior. Antes de avanzar al siguiente paso, es importante que la quite configuración que se ingresó en el paso previo. Esto involucra quitar la configuración de los *route-maps*, *prefix-lists* y la de cada vecino que establecieron los MEDs.

Todos los equipos de trabajo deberán hacer esto y luego reestablecer sus relaciones de vecinos de eBGP.

- 8. Implementar las siguientes políticas de tráfico entrante usando el método de AS PATH.** Este paso introduce el segundo método para poder influenciar en las políticas de tráfico entrante. Al igual que en el paso anterior, lea primero las instrucciones, y luego trate las mismas dentro de su grupo de trabajo y dentro de su AS, y luego estará listo para implementar lo siguiente.

El ejemplo en este paso tiene exactamente el mismo flujo de tráfico entre sistemas autónomos vecinos al igual que en el paso anterior para las redes mostradas en la topología. Refiérase a la figura 2 para recordar el modelo del flujo de tráfico...

AS 200:

- Todo el tráfico hacia 200.200.16.0/22 (R3) desde cualquier lugar en la topología de laboratorio implementada debe ingresar al AS 200 a través del enlace R14 – R2. (**Consejo:** Esto significa que R1 y R3 deben publicar la red 200.200.16.0/22 con un valor de AS PATH mayor que las otras redes en el AS 200. R2 necesita publicar la red 200.200.16.0/22 con un valor mayor de AS path en su vecindad con R4.)

AS 210:

- Todo el tráfico hacia la red 210.210.8.0/22 (R5) desde cualquier parte de la topología de laboratorio implementada debe ingresar al AS 210 por medio del enlace entre R8 – R6. (**Consejo:** Esto significa que R4, R5 y R7 deben publicar la red 210.210.8.0/22 con un valor de AS path mayor que las otras redes dentro del AS 210.)

AS 220:

- Todo el tráfico hacia la red 220.220.4.0/22 (R8) desde cualquier parte de la topología de laboratorio implementada debe ingresar al AS 220 por medio del enlace entre R7 – R9. (**Consejo:** Esto significa que los ruteadores R8 y R10 deben publicar la red 220.220.4.0/22 con un valor de AS path mayor que las otras redes en el AS 220. R9 necesita publicar la red 220.220.4.0/22 con un valor de AS path mayor en su relación de vecindad con R11.)

AS 222:

- Todo el tráfico hacia la red 222.222.8.0/22 (R12) desde cualquier parte de la topología de laboratorio implementada debe ingresar al AS 222 a través del enlace R1 – R13. (**Consejo:** Esto significa que R11, R12 y R14 deberán publicar la red 222.222.8.0/22 con n valor de AS path mayor que las otras redes dentro del AS 222.)
- Todo el tráfico hacia la red 222.222.16.0/22 (R13) desde cualquier parte de la topología de laboratorio implementada debe ingresar al AS 222 a través del enlace R10 – R12. (**Consejo:** Esto significa que los ruteadores R11, R13 y R14 deberán publicar la red 222.222.16.0/22 con un valor de AS path mayor que las otras redes dentro del AS 222.)

Thursday, September 23, 2004

El parámetro AS_PREPEND comúnmente es utilizado por ISPs pequeños que son multihoming hacia sus proveedores. Esto representa una especie de convención en Internet de agregar al menos dos sistemas autónomos cuando se utiliza el parámetro AS_PREPEND. Más común todavía, cuando 3 AS's son agregados, especialmente si el ISP de subida tiene enlaces con un tercero.

Ejemplo de configuración para Router R8 (usando AS PATH prepend):

```
ip prefix-list R8-prefix permit 220.220.4.0/22
!
route-map set-as-path permit 10
  match ip address prefix-list R8-prefix
  set as-path prepend 220 220 220
!
route-map set-as-path permit 20
!

router bgp 220
  neighbor 210.210.17.1 remote-as 210
  neighbor 210.210.17.1 route-map set-as-path out
!
```

IPv6:

```
ipv6 prefix-list R8-v6-prefix permit FEC0:220:4::/48
!
route-map set-as-path permit 10
  match ip address prefix-list R8-v6-prefix
  set as-path prepend 220 220 220
!
route-map set-as-path permit 20
!

router bgp 220
  neighbor FEC0:210:16:17::1 remote-as 210
  address-family ipv6
    neighbor FEC0:210:16:17::1 activate
  neighbor 210.210.17.1 route-map set-as-path out
!
```

Notar que el equipo con el Router 6 tiene solamente que quitar la configuración que se adicionó en el paso anterior. Ellos no requieren configurar AS path prepends como se indica arriba porque ellos no tienen vecindades que requieran alteraciones en su política de tráfico entrante para su AS.

Punto de Control #4: Llame a su instructor y muestre los siguiente:

if Cada ruteador en un AS hará un 'traceroute' a destinos seleccionados, el cual deberá mostrar paquetes salientes de su AS de acuerdo al ejercicio mencionado.

ii] Explicar al instructor la configuración utilizada para lograr el resultado deseado. Muestre los resultados de los comandos “show ip bgp”, y “show ip bgp x.x.x.x” para las redes cuyo parámetro AS path length ha sido incrementado. Muestre además el resultado de el TRACE según las instrucciones dadas.

*iii] Como el AS Path prepend cambió la tabla de BGP y de enrutamiento, ¿Puede la decisión ser sobrescrita usando cualquier otra configuración de BGP dentro de su AS ? **Respuesta:** revisar las reglas de selección de rutas de BGP dadas en la presentación.*

9. Resumen:

Este modulo ha mostrado muchas vías en las que podemos cambiar las políticas del comportamiento del tráfico entrante y saliente.

P: ¿Cuál es la diferencia en los efectos de los resultados mostrados en los pasos 4 y 5 ?

R: AS PATH prepend afecta los anuncios de enrutamiento entre dos sistemas autónomos, y es visible desde cualquier parte, incluso fuera de los dos AS's que están haciendo uso de la información del Prepend. Los MEDs solamente se aplican entre múltiples vecinos del mismo sistema autónomo. Si el AS vecino está anunciando el AS local hacia adelante, la métrica configurada corresponde al AS vecino y no al AS local.

Consulte la documentación de BGP para más información. Hay muchas variaciones posibles en los ejemplos mostrados en esta práctica. Recuerde los siguientes puntos:

- *local preference* es usado para modificar políticas dentro de un AS
- Los MEDs son utilizados para modificar las políticas de tráfico sobre múltiples enlaces entre el AS local y sus vecinos inmediatos.
- El parámetro *AS path prepend* es utilizado para influenciar en las políticas externas en una escala global (que incluye a los AS's vecinos inmediatos).

Preguntas de Revisión

Thursday, September 23, 2004

Notas de Configuración

La documentación es crítica! Ud. debería registrar la configuración en cada uno de los puntos de control, así como la configuración al final de esta práctica.