Módulo 9 – Puntos de Intercambio de Internet (IXP)

Objetivo: Módulo opcional para demostrar el uso de BGP en los Puntos de Intercambio de Internet (IXP).
Prerrequisitos: Módulos 1 al 7 y las presentaciones de BGP

Topología

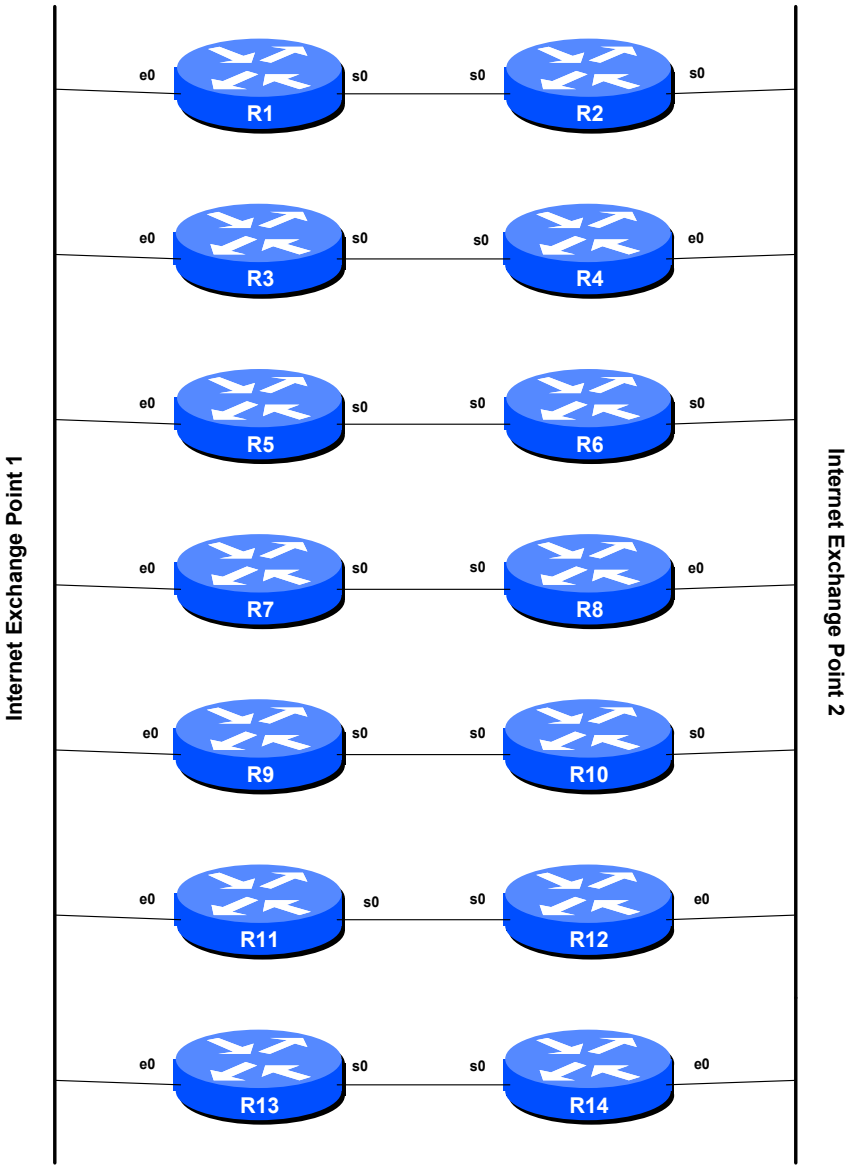

Figura 1 – Diagrama IXP

INTRODUCCIÓN:
Este módulo presenta algunos de los conceptos usados en la mayoría de los Puntos de Intercambio de Internet (IXP). Para propósitos del taller, el dispositivo de intercambio es un switch Catalyst 2924XL 10/100. Cada ruteador es un ISP diferente, con diferente AS. Cada ISP tiene una conexión al punto de intercambio (acceso a Internet), y una conexión con otro ISP a través de un enlace directo (escenario muy común).

Puntos importantes a considerar:
- SOLO usará la conexión con el IXP para llegar a las redes pertenecientes a los ISP que se conectan al mismo IXP
- NO USE la conexión IXP para enviar tráfico a redes pertenecientes a los ISP que se conectan con diferente IXP. Ese tráfico debe ser enviado por el enlace privado.

Por ejemplo, tomando como referencia la Figura 1, para enviar tráfico a R10, R1 no deberá usar la conexión ethernet al IXP. R1 usará la conexión ethernet IXP para enviar tráfico a las redes pertenecientes a R3, R5, R7, R9, R11 y R13.

Se explicarán dos métodos. El primero usa rutas tradicionales y filtros AS-path, mientras que el segundo usa comunidades BGP. Cualquier opción puede ser seleccionada, o ambas pueden ser investigadas.

- Rutas y filtros AS-path tienden a ser más complejos de configurar y mantener. Sin embargo, dan un mejor control de lo que va y viene de una red.
- Muchos ISP prefieren usar comunidades BGP para un control más detallado de las políticas de ruteo. La configuración es menos compleja y generalmente fácil de comprender y mantener.
- Comunidades, rutas y filtros AS-path son usados en la vida real. La política dentro de una red y la transmisión de datos a similares puede ser controlado a través de comunidades BGP, pero se usan filtros de rutas adicionalmente para asegurar que no existan fallas en las rutas externas. Las Comunidades son usadas para intercambiar información entre sistemas autónomos, pero la mayoría de ISPs prefieren controlar lo que escucharán de sus similares usando rutas y filtros AS-path.

Los dos métodos presentados aquí tienen el mismo resultado final. No existe un IXP típico, por lo que no se pretende demostrar la operación de uno. Hoy en día cada IXP en Internet usa su propia versión de infraestructura, modelo de intercambio de información y esquema de direccionamiento.

Consejo: Este módulo usa muchas de las técnicas que han sido cubiertas en los módulos previos de este taller. Haciendo uso de estas técnicas notará que la configuración es mucho más sencilla. Si tiene dudas, pregunte al instructor, o revise la documentación de BGP.

1. **Construya la red:** El primer paso es construir la red para este módulo. La Figura 1 muestra los requerimientos. Todos los ruteadores **Impares** son asignados al IXP 1 y todos los ruteadores **Pares** son asignados al IXP 2. Todos los ruteadores tienen dos conexiones, una conexión directa

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

al ruteador conectado al otro IXP y otra conexión al switch Ethernet que interconecta todos los ruteadores asignados a un IXP.

El instructor del laboratorio asignará dos switches Ethernet para ser usados como los dos IXP. Use el cable Ethernet para conectar su ruteador al IXP asignado. Si ya tiene un enlace con un ruteador conectado con el otro IXP, entonces está listo. Si no, busque un cable ethernet o un cable serie, y conecte su ruteador con un ruteador conectado al otro IXP.

2. **Configuración básica del ruteador:** Ahora que la red está físicamente construida, configure el ruteador como lo hizo en los pasos 1 al 5 del Módulo 1. Fíjese en el orden – conexión física, funcionalidad básica, seguido de la configuración LAN y WAN.

Punto de Control #1: *Llame al instructor del laboratorio y muéstrele como la red fue construida y enséñele la configuración del ruteador que haya hecho.*

3. **Asignaciones AS y loopback:** Las siguientes, son las asignaciones AS:

R1	**AS 101**	**R2**	**AS 202**
R3	**AS 103**	**R4**	**AS 204**
R5	**AS 105**	**R6**	**AS 206**
R7	**AS 107**	**R8**	**AS 208**
R9	**AS 109**	**R10**	**AS 210**
R11	**AS 111**	**R12**	**AS 212**
R13	**AS 113**	**R14**	**AS 214**

Configure el ruteador con el AS asignado usando los comandos *autonomous-system* y *router bgp*. Los siguientes bloques de direcciones son asignados a cada ruteador. Cada ruteador debe tener rutas estáticas, sentencias de redes BGP y direcciones de loopback configuradas para el bloque de red:

R1	**210.101.4.0/22**	**R8**	**220.208.4.0/22**
R2	**220.202.4.0/22**	**R9**	**210.109.4.0/22**
R3	**210.103.4.0/22**	**R10**	**220.210.4.0/22**
R4	**220.204.4.0/22**	**R11**	**210.111.4.0/22**
R5	**210.105.4.0/22**	**R12**	**220.212.4.0/22**
R6	**220.206.4.0/22**	**R13**	**210.113.4.0/22**
R7	**210.107.4.0/22**	**R14**	**220.214.4.0/22**

Y para IPv6:

R1	**FEC0:210:101::/48**	**R8**	**FEC0:220:208::/48**
R2	**FEC0:220:202::/48**	**R9**	**FEC0:210:109::/48**
R3	**FEC0:210:103::/48**	**R10**	**FEC0:220:210::/48**
R4	**FEC0:220:204::/48**	**R11**	**FEC0:210:111::/48**
R5	**FEC0:210:105::/48**	**R12**	**FEC0:220:212::/48**
R6	**FEC0:220:206::/48**	**R13**	**FEC0:210:113::/48**
R7	**FEC0:210:107::/48**	**R14**	**FEC0:220:214::/48**

Ejemplo: Router R1

Configure las rutas estáticas para 4 redes /24 del bloque 210.101.4.0/22. Las cuales son usadas simplemente para propagar la tabla de rutas BGP en el ruteador, y representan redes de clientes conectadas, por ejemplo:

```
ip route 210.101.4.0 255.255.255.0 Null0
ip route 210.101.5.0 255.255.255.0 Null0
ip route 210.101.6.0 255.255.255.0 Null0
ip route 210.101.7.0 255.255.255.0 Null0
```

Configure además la interfaz loopback:

```
interface loopback 0
ip address 210.101.7.224 255.255.255.255
```

y configure BGP:

```
router bgp 101
 network 210.101.4.0
 network 210.101.5.0
 network 210.101.6.0
 network 210.101.7.0
```

Similarmente, para IPv6:

```
ipv6 route FEC0:210:101:4::/64 Null0
ipv6 route FEC0:210:101:5::/64 Null0
ipv6 route FEC0:210:101:6::/64 Null0
ipv6 route FEC0:210:101:7::/64 Null0

interface loopback 0
ip address FEC0:210:101:7::224/128

router bgp 101
 network FEC0:210:101:4::/64
 network FEC0:210:101:5::/64
```


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

```
network FEC0:210:101:6::/64
network FEC0:210:101:7::/64
```

Nota: La interfaz loopback no es usada como tal en este módulo, es usada como un punto de referencia para los comandos ping y trace que se usarán luego. (Es una buena práctica configurar siempre la interfaz loopback en el ruteador – recuerde que nunca falla.) Use el espacio final /28 del /22 asignado al ruteador.

4. **Enlace Privado con el ISP vecino:** Acuerde una subred IP para ser usada en el enlace privado entre usted y su vecino AS. Por ejemplo, R1 y R2 necesitan establecer una dirección IP para el enlace serie entre ellos. Por ejemplo, podrían usar 210.101.5.0/30.

   Configure la interfaz del enlace privado y revise la conectividad usando ping.

5. **Configure las interfaces en los IXP:**

   IXP 1 Ethernet: Use la subred 201.201.201.0 255.255.255.240 para el rango de direccionamiento y asigne las siguientes direcciones a la interfaz Ethernet del router:

   R1: 201.201.201.1,
   R3: 201.201.201.3,
   R5: 201.201.201.5,
   Etc…

   Para IPv6, utilice la subred FEC0:201:201:201::/64

   IXP 2 Ethernet: Use la subred 202.202.202.0 255.255.255.240 para el rango de direccionamiento y asigne las siguientes direcciones a la interfaz Ethernet del router:

   R2: 202.202.202.2,
   R4: 202.202.202.4,
   R6: 202.202.202.6, Etc…

   Para IPv6, utilice la subred FEC0:202:202:202::/64

6. Determine a cuál IXP está asignado su router y averigüe la información de los otros ruteadores que pertenecen al mismo. En otras palabras, es necesario saber acerca de los ruteadores que van a ser propagados por sus compañeros en el mismo IXP.

7. Configure la interfaz ethernet en el IXP y verifique la conectividad a los otros ruteadores usando ping.

8. **Bandera Route Dampening:** Configure la bandera Route Dampening en el proceso BGP. Observe la tabla de rutas BGP durante el tiempo del modulo, y recolecte estadísticas.

Punto de Control #2: *Llame al instructor del laboratorio y demuestre que usted puede hacer ping al ISP privado y al IXP al cual usted está conectado.*

METODO UNO – Rutas y Filtros AS-Path

9. **Configurando filtros y grupos de vecinos:** Configure un grupo de vecinos (peer-group) BGP que incluya todos los vecinos que pertenecen al mismo IXP. Este grupo debe incluir la directiva *soft-reconfiguration* para no permitir la reinicialización de las sesiones BGP con los vecinos.

10. **Anunciando un ISP local agregado:** Configure el proceso BGP para propagar una ruta **agregada** que representa todas las rutas estáticas configuradas en el ruteador. Por ejemplo, R1 generará una ruta integrada para cubrir el bloque de red 210.101.4.0/22. **Consejo:** use el comando bgp *network x.x.x.x mask y.y.y.y*.

11. **Anunciando el IXP agregado:** Configure el proceso BGP para propagar una ruta **agregada** que representa todos los ruteadores en un mismo punto de intercambio al cual usted está conectado. Por ejemplo, R4 generará una ruta integrada para 220.0.0.0/8. **Consejo:** use el comando bgp *aggregate-address x.x.x.x y.y.y.y*.

12. **Política de Ruteo en el IXP:** Establecida la conectividad física y la configuración local, el siguiente paso es aplicar algunas políticas de ruteo de entrada y salida en el IXP.

    - Configure un filtro de **salida** para los vecinos dentro del mismo IXP, **SOLO** propague las rutas pertenecientes a usted. Por ejemplo, R1 **solo** propagará 210.101.4.0/22. **Consejo:** use el comando *distribute-list* para filtrar redes específicas del bloque /22.

    - Configure un filtro de **entrada** para cada uno de sus vecinos IXP, **SOLO** acepte rutas que pertenezcan a ellos. Por ejemplo, R1, R5, R7, R9, R11 y R13 **solo** aceptan 210.103.4.0/22 de R3, etc. **Consejo:** use el comando *distribute-list* para filtrar los anuncios de rutas de sus vecinos.

    Hay dos maneras de aplicar esos filtros. Una, es configurando una línea por cada red específica a ser bloqueada en una lista de acceso, lo cual es tedioso y difícil de mantener a medida que el ISP crece. La otra manera, que es la más indicada, es configurando una lista de acceso que contenga la red y máscara exacta a ser propagada.

    Nota Importante:

Estas listas de distribución requieren el uso de listas de acceso extendidas, para lograr que la red y máscara exactas sean configuradas. Usando listas de acceso simples, todas las redes que coincidan con la lista de acceso serán permitidas. Por ejemplo, si:

```
access-list 1 permit 210.101.4.0 0.0.3.255
router bgp 101
neighbor 201.201.201.3 distribute-list 1 out
```

es configurado en el Ruteador R1, en la comunicación con R3, las cuatro redes /24 y la red /22 originadas por R1 serán propagadas a R3. Esto conlleva al término que usan los ISP *leaking of specific routes* y es considerado una mala práctica en la comunidad de Internet. (Rutas específicas pueden ser propagandas in circunstancias particulares, por ejemplo para lograr balanceo de carga o una lograr una política de rutas. En general, la propagación de redes compuestas, y de subredes específicas es considerada una mala práctica y contribuye al crecimiento desmedido de las tablas de rutas de Internet.)

Sin embargo, las listas de acceso extendidas pueden ser usadas para especificar la máscara y red a ser filtradas, tal como se indica en el siguiente ejemplo, el cual logra el resultado deseado:

```
access-list 101 permit ip host 210.101.4.0 host 255.255.252.0
router bgp 101
neighbor 201.201.201.3 distribute-list 101 out
```

Este formato de access-list 101 solo permite filtrar la red 210.101.4.0 con la máscara 255.255.252.0. Las redes que no tengan exactamente la máscara específica, no serán consideradas, y por lo tanto, serán ignoradas. Por ejemplo, la red 210.101.4.0 con máscara 255.255.255.0 no coincide y por lo tanto, no es anunciada a los vecinos BGP.

Para mayor información de listas de acceso extendida, consulte el CD de Documentación.

Adicional: el comando bgp *aggregate-address x.x.x.x m.m.m.m summary-only* podría ser usado aquí. ¿Ve usted algún inconveniente en usar este comando?

13. **Política de Ruteo para vecinos privados:** Con la comunicación IXP asegurada, es necesario aplicar políticas de ruteo a todos los vecinos privados.

    - Configure un filtro de **salida** para propagar **SOLO** la ruta completa que representa el IXP y nada más. Por ejemplo, R1 debe propagar solo 210.0.0.0/8 a R2, nada más.

    - Configure un filtro de **entrada** para recibir **SOLO** la ruta completa que representa las rutas en el otro IXP y nada más. Por ejemplo, R1 debe recibir solo 220.0.0.0/8 de R2, y nada más.

    Recuerde la recomendación anterior acerca de las listas de acceso del paso anterior. Puede ser usada como un efecto positivo aquí también.

Punto de Control #3: *Llame al instructor del laboratorio y muestre la siguiente información. Cada ruteador en un IXP debe tener en sus tablas de ruteo:*

- *Sus propias rutas*
- *Rutas específicas para todos sus vecinos en el IXP*
- *Una ruta completa para los otros ruteadores para todos los ruteadores en el mismo IXP*
- *Una ruta completa para los otros ruteadores para todos los ruteadores en el otro IXP*

i] *Realice una traza a un destino perteneciente a un vecino en el mismo IXP y muestre que la traza usa el IXP para llegar al destino. Por ejemplo, para que R1 alcance 210.109.4.1, el paquete debe usar la conexión Ethernet al IXP.*
ii] *Realice una traza a un destino perteneciente a un vecino del otro IXP y muestre que el camino seguido no usa el IXP local para llegar al destino. Por ejemplo, para que R1 alcance 220.110.4.1, el paquete no debe usar la conexión Ethernet IXP, sino que deberá usar el enlace al ruteador R2 para alcanzar su destino.*

METODO DOS: Filtros basados en Comunidad BGP

Nota: Si continua desde el Método Uno, recuerde borrar los mapas de rutas y filtros que no se aplican. Recuerde, que toda la configuración que no es usada, **deberá ser borrada**.

14. **Configurando comunidades y grupos de vecinos:** Configure un **grupo de vecinos** eBGP para incluir todos los vecinos que pertenecen al mismo IXP. Este grupo debe incluir las directivas *soft-reconfiguration* y *send-community*.

    - Cada ruteador en IXP 1 deberá etiquetar sus propias rutas con una comunidad *AS*:200. En otras palabras, R1 etiquetará la ruta 210.101.4.0/22 con la comunidad 101:200; R3 etiquetará la ruta 210.103.4.0/22 con la comunidad 103:200, etc…

    - Cada ruteador en el IXP 2 deberá etiquetar sus propias rutas con una comunidad *AS*:400. En otras palabras, R2 etiquetará la ruta 220.202.4.0/22 con la comunidad 202:400; R4 etiquetará la ruta 220.204.4.0/22 con la comunidad 204:400, etc…

    Recuerde usar el comando *BGP community new-format*, para mostrar las comunidades con el formato indicado anteriormente.

15. **Anunciando la red local ISP agregada:** Configure el proceso BGP para propagar la ruta **agregada** que representa todas las rutas estáticas configuradas en el ruteador. Por ejemplo, R1 generará una colección para cubrir el bloque de red 210.101.4.0/22. **Consejo:** para hacer esto, use *network x.x.x.x mask y.y.y.y route-map <map-name>*.

16. **Anunciando el IXP agregado:** Configure el proceso BGP para propagar la ruta **agregada** que representa todas las rutas presentes en el punto de intercambio al cual está conectado. Por ejemplo, R4 generará una ruta agregada para 220.0.0.0/8. **Consejo:** para hacer esto, use *aggregate-address x.x.x.x y.y.y.y attribute-map <map-name>*.

    Asigne la comunidad *AS*:100 para el IXP1 agregado y *AS*:300 para el IXP2 agregado. Por ejemplo, el ruteador R4 conectado al IXP 2 generará una ruta agregada para 220.0.0.0/8 con la comunidad 204:300.

17. **Agrupación de comunidades:** Eventualmente todas las rutas agregadas que pertenecen a los ruteadores en el IXP1 tendrán la comunidad *AS*:200 y el agregado representando todas las rutas en IXP1 [210.0.0.0/8] el cual es propagado a los vecinos del IXP2 que tendrán la comunidad *AS*:100. Así mismo, todos los ruteadores en el IXP2 tendrán la comunidad *AS*:400 y el agregado representando todas las rutas en IXP2 [220.0.0.0/8] el cual es propagado a los vecinos en IXP2 que tendrán la comunidad *AS*:300.

18. **Políticas de Ruteo en el IXP:** Establecida la conectividad física y la configuración local, el siguiente paso es aplicar algunas políticas de ruteo de entrada y salida en el IXP.

    - Configure un route-map de **salida** para los vecinos del mismo IXP, **SOLO** propague rutas pertenecientes a usted. Por ejemplo, R1 **solo** propagará 210.101.4.0/22.
    - Configure un route-map de **entrada** para cada uno de los vecinos del mismo IXP, **SOLO** acepte rutas que pertenezcan a ellos. Por ejemplo, R1, R5, R7, R9, R11 y R13 **solo** aceptan 210.103.4.0/22 de R3, etc.

19. **Políticas de Ruteo para Vecinos Privados:** Con la comunicación IXP asegurada, es necesario aplicar políticas de ruteo a todos los vecinos privados.

    - Configure un route-map de **salida** para propagar SOLO la ruta completa que represente al IXP y nada más. Por ejemplo, R1 debe propagar solo 210.0.0.0/8 a R2, y nada más.

    - Configure un route-map de **entrada** para recibir SOLO la ruta completa que representa al IXP y nada más. Por ejemplo, R1, debe recibir 220.0.0.0/8 de R2, y nada más.

      Consejo: Es el momento de usar la comunidad que fue usada antes para los agregados. Por ejemplo, el agregado 210.0.0.0/8 tiene la comunidad *AS*:100 asociada. Por lo tanto, configure un route-map para usar esta comunidad para seleccionar el agregado para implementar la política anterior.

Punto de Control #4: *Llame al instructor del laboratorio y muestre la siguiente información. Cada ruteador en el IXP debe tener en las tablas de rutas lo siguiente:*

- *Sus propias rutas*

- *Rutas específicas para todos sus vecinos en el IXP*
- *Un agregado para todos los ruteadores en el mismo IXP con la comunidad correcta*
- *Un agregado para todos los ruteadores en el otro IXP con la comunidad correcta*

i] *Realice una traza a un destino perteneciente a un vecino en el mismo IXP y muestre que la traza usa el IXP para llegar al destino. Por ejemplo, para que R1 alcance 210.109.4.1, el paquete debe usar la conexión Ethernet al IXP.*
ii] *Realice una traza a un destino perteneciente a un vecino del otro IXP y muestre que el camino seguido no usa el IXP local para llegar al destino. Por ejemplo, para que R1 alcance 220.110.4.1, el paquete no debe usar la conexión Ethernet IXP, sino que deberá usar el enlace al ruteador R2 para alcanzar su destino.*

20. Filtrado usando listas de acceso y comunidades: Muchos ISP prefieren usar filtros AS-path y filtros para las rutas de entrada además del uso de comunidades.

P. ¿Por qué cree que éste es el caso?
R. Los filtros de entrada controlan lo que la red del ISP puede **recibir**. Si un ISP confía solamente en los filtros de comunidad, está confiando en que los ISP vecinos tengan configurados correctamente sus comunidades. Muchos de los ISP no corren el riesgo y protegen cualquier filtro basado en comunidades con filtros de entrada extras. Esos filtros contienen la red que el ISP vecino anuncia, así como también las redes contenidas en el RFC1918 (espacio de direcciones privadas), la red predeterminada, sus propias redes, y otras que pueden ser bloqueadas. Revise el documento IOS Essentials for ISP para mayor información acerca de las redes del RFC1918 y de los filtros de entrada para ISP.

P. ¿Qué configuración adicional es requerida para implementar filtros de entrada en el ejemplo anterior adicional a los filtros basados en comunidad?
R. El comando *distribute-list* debe ser añadido al bloque *bgp neighbor* en los eBGP vecinos. A continuación un ejemplo para la comunicación entre R1 y R3 en el IXP1:

```
router bgp 101
 neighbor IXP1-peers peer-group
 neighbor IXP1-peers send-community
 neighbor IXP1-peers soft-reconfiguration inbound
 neighbor IXP1-peers route-map IXP1-peers-out out
 neighbor 201.201.201.3 remote-as 103
 neighbor 201.201.201.3 peer-group IXP1-peers
 neighbor 201.201.201.3 distribute-list 103 in
 neighbor 201.201.201.3 route-map R3-in in
 . . .
access-list 103 permit ip 210.103.4.0 0.0.3.255 255.255.252.0 0.0.3.255
access-list 103 deny ip any any
```


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

Punto de Control #5: *Llame al asistente del laboratorio y demuestre los cambios necesarios que usted debe realizar.*

NOTAS DE CONFIGURACIÓN

¡La documentación es crítica! Deberá llevar un registro de la configuración en cada **Punto de Control**, y también al final del módulo.

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