

Cartilla resumida de comandos y parámetros Cisco para la configuración de BGP

Introducción

Daremos un resumen de los comandos que pueden resultar útiles para configurar y utilizar BGP, con especial énfasis en los que resulten útiles para el laboratorio

Para una guía completa de la configuración de BGP en Cisco, pueden consultar el capítulo correspondiente a BGP de la “Cisco IOS IP Routing Protocols Configuration guide”,

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080446e5f.html, o la guía correspondiente a la versión de IOS que utilicen

Para una referencia completa de las opciones de todos los comandos, pueden consultar los capítulos correspondientes a BGP de la “Cisco IOS IP Routing Protocols Command Reference”,

http://www.cisco.com/en/US/products/ps6350/products_command_reference_book09186a008042def8.html

Hay dos formatos de configuración de BGP, el “histórico” (Cisco lo denomina “NLRI Configuration CLI”) y el modo “Address Family”. También se cuenta con el modo híbrido, donde la configuración de IPv4 se mantiene en el formato histórico y se puede agregar configuración de direcciones VPNv4 (VPNs con MPLS). Los comandos son similares, excepto que los específicos de IPv4 son precedidos por “address-family ipv4 unicast” cuando estamos en modo “Address Family” (AFI de aquí en más)

Configuración de BGP, configuración de vecinos.

Lo primero que debemos definir, es el proceso de ruteo bgp, con nuestro número de sistema autónomo.

Luego debemos definir, para cada vecino, el número de sistema autónomo y los parámetros y políticas que corresponden a cada vecino. Recordemos que BGP no posee ningún mecanismo de descubrimiento de vecinos, los vecinos deben ser configurados explícitamente.

router bgp <AS>

Inicia el proceso correspondiente al protocolo BGP, con número de sistema autónomo local <AS>

Dentro de la configuración de “router bgp”:

router-id <IP>

Opcional. Configura la identidad de el enrutador. Si no se configura, el enrutador elegirá una de sus IPs (ver algoritmo en las notas del curso)

bgp log-neighbor-changes

Opcional. Indica que se guarde log de los cambios que ocurran en las sesiones BGP. Útil para debug

timers bgp <keepalive> <holdtime>

Opcional. Indica los timers (hold time y keepalive) que queremos utilizar por defecto.

(no) auto-summary

Opcional. Deshabilitado por defecto en versiones recientes (o sea, por defecto “no auto-summary”). Deshabilita la generación de rutas sumarizadas automáticamente a la clase correspondiente. En modo AFI, aparece dentro del address-family

(no) synchronization

Opcional. Deshabilitado por defecto en versiones recientes. Ignora el requerimiento de no publicar una ruta por BGP hasta que no se encuentre disponible en el IGP (protocolo interior). En modo AFI, aparece dentro del address-family

neighbor <IP> remote-as <AS>

Define al peer con dirección <IP>, indicando su número de sistema autónomo.

neighbor <IP> description <texto>

Opcional. Descripción del vecino. Hace más legible la configuración.

neighbor <IP> ebgp-multihop <n>

Opcional. Indica que el peer de BGP externo no se encuentra directamente conectado, sino que puede encontrarse hasta “n” saltos de distancia

neighbor <IP> update-source <interface>

Opcional. Indica que la IP origen para comunicarse con el peer <IP> sea la de la interfaz <interface>. También indica para BGP externo cual será la IP anunciada como “next hop”

neighbor <IP> next-hop-self

Opcional. Para un peer BGP interno, indica que el next-hop a anunciar se cambie por la IP propia.

neighbor <IP> route-reflector-client

Opcional. Indica para un peer BGP interno, que este es un cliente de reflector, o sea que el enrutador “reflejará” las rutas internas desde y hacia este vecino.

neighbor <IP> shutdown

Pasa la sesión al estado “Idle”, o sea, el enrutador ni intenta establecer la sesión ni acepta intentos del peer de establecer la sesión. Para volver a activar la sesión, utilice “no neighbor <IP> shutdown

neighbor <IP> password 7 <password>

Para utilizar autenticación TCP-MD5 en la sesión con el vecino, con la password dada.

Generación de prefijos

Para generar prefijos, podemos hacerlo redistribuyendo los prefijos aprendidos por otro protocolo, o mediante el comando “network”

Un caso particular es la ruta por defecto, que puede generarse independientemente para cada vecino

En el caso de estar trabajando en modo “Address Family”, esta configuración se encuentra bajo “address-family ipv4”

neighbor <IP> default-originate

Opcional. Envía al peer <IP> la ruta por defecto por BGP. En modo AFI, dentro de address-family ipv4

network <Red> mask <Máscara>

Opcional. En caso de existir el prefijo Red/Máscara en la tabla de ruteo, realiza su publicación mediante BGP. Es común agregar una ruta estática (posiblemente de menor peso que las existentes) que apunte el prefijo a una interfaz Null, en caso de ser el único equipo que tiene conectividad con el prefijo dado

redistribute <connected|static|rip|ospf|etc>

redistribute <connected|static|rip|ospf|etc> [process-id] route-map <mapa>

Opcional. Permite publicar en BGP rutas aprendidas mediante otro protocolo (o estáticas o directamente conectadas). En caso de utilizar un route-map, este permite seleccionar qué rutas importar, y cambiarle atributos.

Políticas de ruteo

Recordar que, luego de realizar cualquier cambio en la política de ruteo, la o las sesiones BGP involucradas se deben resetear. Para ello, siguiendo lo visto en el teórico, realizar **clear ip bgp <IP del vecino> soft [in/out]**. Si no se indica in o out, se realizará en ambas direcciones.

Filtrado básico

Para realizar un filtrado básico, dependiendo solamente del as-path y/o de los prefijos anunciados, se pueden utilizar las access-lists, las prefix-list, y las as-path access-list

Un “prefix-list” tiene el siguiente formato:

ip prefix-list <nombre> [seq n°] <permit|deny> <red/máscara> [ge n°] [le n°]

<nombre> es una string arbitraria (caracteres y números) que identifican la lista

La palabra “seq”, seguida de un entero, permite ordenar las entradas de la prefix-list.

Si uno no indica la secuencia, el router automáticamente suma 5 al último número de secuencia utilizado

permit o deny indican si los prefijos indicados se dejarán pasar o se filtrarán

La palabra “ge”, opcional, indica “todas las subredes del prefijo dado con igual o más bits de máscara que los indicados

La palabra “le”, opcional, indica “todas las subredes del prefijo dado con igual o menos bits de máscara que los indicados

Un as-path access-list tiene el siguiente formato:

ip as-path access-list <numero> <permit | deny> <expresión regular>

El número (1-199 en versiones viejas, 1-500 en versiones nuevas), identifica distintas entradas de la misma as-path access-list

permit o deny indica si los prefijos cuyo as-path sea seleccionado por la expresión regular serán “aceptados” o “rechazados”

La expresión regular sigue el formato visto en el teórico

Tanto las prefix-list como las as-path access-list pueden aplicarse en la dirección “in” o “out”. “in” significa que se aplicará para seleccionar qué prefijos aceptaré de los que me publica un vecino. “out” significa que se aplicará para seleccionar cuáles de los prefijos que conozco publicaré hacia un determinado vecino.

```
router bgp <as>
  address-family ipv4
  neighbor <IP> prefix-list <nombre> <in|out>
  neighbor <IP> filter-list <numero> <in|out>
```

Filtrado avanzado. Modificación de atributos

La forma de realizar filtros más avanzados, así como de modificar los atributos asociados a un prefijo, es mediante route-maps. Referirse a las notas del teórico o a las referencias.

Aplicación de un route-map

```
router bgp <as>
  address-family ipv4
  neighbor <IP> route-map <nombre> <in|out>
```

Aplica el route-map dado por <nombre> al vecino dado por <IP> en la dirección in o out

Un route-map está conformado por uno o más bloques con la siguiente sintaxis:

```
route-map <nombre> <permit|deny> <numero>
  match <condiciones>
  set <cambios de atributos>
```

El nombre permite agrupar varias entradas que conforman un único route-map

El número indica el orden de los distintos bloques de un mismo route-map, y permite insertar/borrar bloques.

permit|deny indica la acción que se realizará sobre los prefijos que se seleccionen mediante el match. Permit indica que se “dejarán pasar”, deny indica que serán filtrados. Set no tiene sentido si la acción es “deny”

El bloque match es el que indica bajo qué criterios se seleccionarán los prefijos para aplicarles la acción. Puede estar vacío, en cuyo caso se seleccionan todos los prefijos. Si hay más de un “match” en el mismo bloque del route-map, deben machear todos

El bloque set es el que indica la acción a realizar. Puede haber más de uno en un bloque, en cuyo caso se aplicarán todos.

Algunas condiciones para el match:

as-path access-list – seleccionar en base a un as-path access-list

prefix-list o access-list – seleccionar de acuerdo al prefijo

community-list – seleccionar de acuerdo a las comunidades presentes

local-preference – seleccionar de acuerdo a la local-preference que tiene la ruta

Algunas acciones para el set:

set as-path prepend - agregar “prepends” al as-path
set community – setear o agregar comunidades
set comm-list – borrar comunidades
set dampening – setear valores de dämpening
set ip next-hop – cambiar el next-hop
set local-preference – cambiar la local-preference
set origin – cambiar el atributo “origin” del prefijo

Manejo de comunidades

Por defecto, Cisco no propaga el atributo “community”. Para permitir trabajar con comunidades, se debe habilitar explícitamente su envío a los vecinos

```
router bgp <as>  
neighbor <IP> send-community
```

Para modificar las comunidades asociadas a una ruta, se debe utilizar un route-map, como se vió en el teórico.

```
route-map <nombre> permit <numero>  
match <critério>  
set community [additive] <numero de comunidad>  
o  
set comm-list <numero> delete
```

La primer forma setea una o varias comunidades a los prefijos seleccionados por el route-map. La palabra “additive”, que es opcional, indica que se agreguen las comunidades dadas sin borrar las que ya tuviera el prefijo

La segunda forma se utiliza para borrar comunidades, donde el número indica una community-list

Para actuar en base a una comunidad, se puede seleccionar dentro de un route-map basándose en una community-list.

```
ip community-list [extended] nombre permit <comunidad>
```

permite seleccionar en base a la comunidad indicada. Puede haber varias entradas con el mismo nombre

```
route-map <nombre> permit <nº>  
match community <nombre-commlist>  
set .....
```

Algunos comandos para ver el estado de BGP, rutas, vecinos, etc.

Comandos show útiles:

```
show ip bgp
```

Muestra la tabla de rutas interna de BGP

show ip bgp <IP o prefijo>

Muestra información más detallada de una entrada en la tabla de rutas interna de BGP

show ip bgp regexp <expresión regular>

Muestra información de la tabla de rutas interna de BGP, mostrando solamente aquellas rutas cuyo as-path machee con la expresión regular dada

show ip bgp summary

Muestra un resumen de las conexiones BGP

show ip bgp neighbors

Muestra el estado de todos los peers ipv4

show ip bgp neighbors <IP>

Muestra detalles del estado del peer dado por la dirección IP

show ip bgp neighbors <IP> advertised-routes

Muestra las rutas efectivamente propagadas hacia el peer con IP dada

show ip bgp neighbors <IP> routes

Muestra las rutas recibidas y aceptadas del peer IP (o sea, luego de filtrar)

show ip bgp community [community-number]

Muestra las rutas que tienen alguna comunidad, o el número de comunidad dado.

Referencias y documentos interesantes

Troubleshooting BGP

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009478a.shtml

Route-Maps for IP Routing Protocol Redistribution Configuration

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008047915d.shtml