REDES

PRÁCTICA 8

"ENRUTAMIENTO BGP"

INTEGRANTES:
GONZÁLEZ MORA ERIKA GISELLE
OLIVARES MENÉZ GLORIA OLIVA
GRUPO: 2CV16

ÍNDICE

1. Introducción

1.1. Protocolo BGP

En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol)1 es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo o AS. Cada uno tendrá conexiones o sesiones internas (iBGP), así como sesiones externas (eBGP).

El protocolo de puerta de enlace de frontera (BGP) es un ejemplo de protocolo de puerta de enlace exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGP4 es la primera versión que admite encaminamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de puerta de enlace internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda o retardo. En cambio, BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

1.2. Mensajes BGP

Existen cuatro tipos de mensajes BGP que son los siguientes:

- **OPEN:** se utiliza para el establecimiento de una sesión BGP una vez haya sido establecida la conexión TCP. Se suelen negociar

ciertos parámetros que caracterizan a esa sesión. Por ejemplo, es muy posible que los miembros de la sesión no tengan la misma versión de BGP por lo que es importante indicar el número de versión en este mensaje.

- **UPDATE:** es un mensaje de actualización, de mucha importancia en las operaciones de BGP ya que contiene los anuncios de nuevos prefijos. Se generarán mensajes de actualización cada vez que se determine una nueva mejor ruta para cierto destino o haya una modificación sobre alguna existente.

- **KEEPALIVE:** una vez que la sesión BGP está activa se envía periódicamente un mensaje para mantener viva la conexión o KEEPALIVE para confirmar que el otro extremo sigue estando activo en la sesión BGP. Generalmente se acuerda un tiempo máximo de espera durante el intercambio inicial de mensajes OPEN. El KEEPALIVE suele ser aproximadamente una vez cada tercio del tiempo de espera, pero no más de una vez cada segundo. Los mensajes KEEPALIVE no se deben generar si el tiempo de espera es cero ya que en ese caso se entiende que la sesión es completamente fiable.

- **NOTIFICATION:** se envía al cerrar una sesión BGP y esto sucede cuando ocurre algún error que requiera el cierre de la misma. De modo que es un mensaje que no permite informar nada.

1.3. Formato de los paquetes

Los paquetes BGP tienen una cabecera de 19 bytes, consistente en los siguientes campos:

- Un campo de 16 bytes de Marcado (Marker): para detectar la pérdida de sincronización o autenticación de mensajes BGP entrantes.

- Un campo de 2 bytes de Longitud de Paquete (Length): que especifica la longitud del mensaje BGP en bytes (la longitud no puede ser menor a los 19 bytes de la cabecera sin datos ni mayor a 4096).

- Un campo de 1 byte de Tipo (Type): que indica el tipo de mensaje.

Los datos que siguen a la cabecera del paquete pueden ser de 0 hasta 4.077 bytes, para dar una longitud máxima posible de 4.096.

2. Desarrollo

En esta práctica No. 7, realizamos la simulación de una topología en Cisco Packet Tracer, usando enrutamiento BGP

Configuración de la Topología

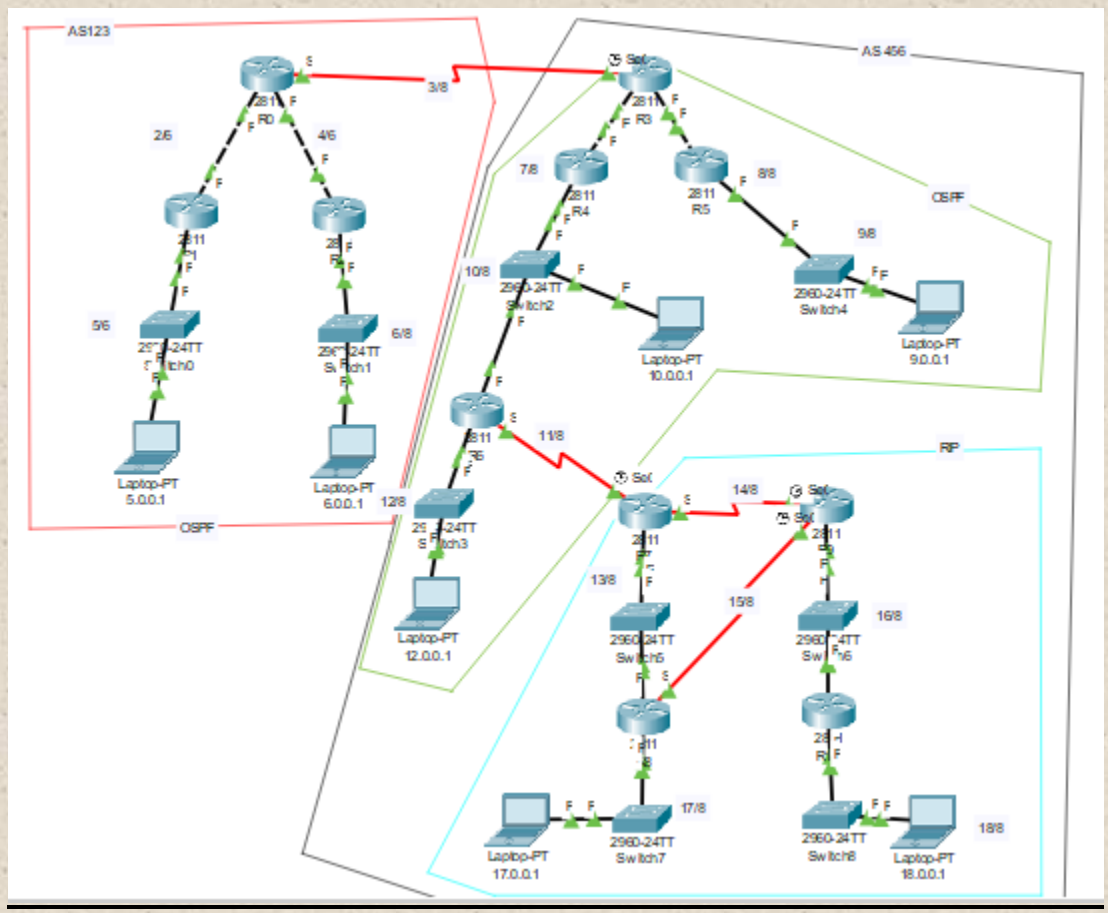
Usamos estos dispositivos para la topología:

ROUTER

SWITCH

LAPTOP

TOPOLOGÍA



Configuración BGP del router R0

Router0>enable

Router0#hostname R0

R0# config t

R0(config)#

R0(config)#router ospf 10 -- Configuración OSPF

R0(config-route)#log-adjacency-changes

R0(config-route)#redistribute bgp 123 subnets

R0(config-route)#network 2.0.0.0 0.255.255.255 area 0

R0(config-route)#network 4.0.0.0 0.255.255.255 area 0

R0(config-route)#exit

R0(config)#router bgp 123

R0(config-route)#bgp log-neighbor-changes

R0(config-route)#syn

R0(config-route)#neighbor 3.255.255.253 remote-as 456

R0(config-route)#network 2.0.0.0

R0(config-route)#network 4.0.0.0

R0(config-route)#network 5.0.0.0

R0(config-route)#network 6.0.0.0

R0(config-route)#redistribute ospf 10 match internal external 1 external 2

R0(config-route)#exit

R0(config)#exit

R0#wr ----------> Guardar la configuración

Sucesivamente, todos los routers se configuraron de manera similar.

Pruebas

Para poder probar la conectividad, hicimos varias pruebas por el *command prompt*.

-Mostrando la tabla de enrutamiento del R3

```
B    2.0.0.0/8 [20/0] via 3.255.255.254, 00:00:00
C    3.0.0.0/8 is directly connected, Serial0/3/1
B    4.0.0.0/8 [20/0] via 3.255.255.254, 00:00:00
B    5.0.0.0/8 [20/0] via 3.255.255.254, 00:00:00
B    6.0.0.0/8 [20/0] via 3.255.255.254, 00:00:00
C    7.0.0.0/8 is directly connected, FastEthernet0/0
C    8.0.0.0/8 is directly connected, FastEthernet0/1
O    9.0.0.0/8 [110/2] via 8.255.255.253, 00:31:59, FastEthernet0/1
O    10.0.0.0/8 [110/2] via 7.255.255.253, 00:31:59, FastEthernet0/0
O    11.0.0.0/8 [110/66] via 7.255.255.253, 00:31:59, FastEthernet0/0
O    12.0.0.0/8 [110/3] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 13.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 14.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 15.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 16.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 17.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
O E2 18.0.0.0/8 [110/20] via 7.255.255.253, 00:31:59, FastEthernet0/0
```

-Configuración R3

```
router ospf 10
 log-adjacency-changes
 redistribute bgp 456 subnets
 network 8.0.0.0 0.255.255.255 area 0
 network 7.0.0.0 0.255.255.255 area 0
!
router bgp 456
 bgp log-neighbor-changes
 no synchronization
 neighbor 3.255.255.254 remote-as 123
 network 0.0.0.0 mask 0.255.255.255
 network 7.0.0.0
 network 8.0.0.0
 network 9.0.0.0
 network 10.0.0.0
 network 11.0.0.0
 network 12.0.0.0
 network 13.0.0.0
 network 14.0.0.0
 network 15.0.0.0
 network 16.0.0.0
 network 17.0.0.0
 network 18.0.0.0
 redistribute ospf 10 match internal external 1 external 2
```

-Configuración del R7

```
router ospf 10
 log-adjacency-changes
 redistribute rip subnets
 network 11.0.0.0 0.255.255.255 area 0
!
router rip
 version 2
 redistribute ospf 10 metric 1
 network 11.0.0.0
 network 13.0.0.0
 network 14.0.0.0
```

-Conectividad ping de la laptop 5.0.0.1 a 18.0.0.1

```
C:\>ping 18.0.0.1

Pinging 18.0.0.1 with 32 bytes of data:

Reply from 18.0.0.1: bytes=32 time=13ms TTL=120
Reply from 18.0.0.1: bytes=32 time=12ms TTL=120
Reply from 18.0.0.1: bytes=32 time=40ms TTL=120
Reply from 18.0.0.1: bytes=32 time=13ms TTL=120

Ping statistics for 18.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 40ms, Average = 19ms
```

-Conectividad ping de la laptop 6.0.0.1 a 9.0.0.1

```
Packet Tracer PC Command Line 1.0
C:\>ping 9.0.0.1

Pinging 9.0.0.1 with 32 bytes of data:

Reply from 9.0.0.1: bytes=32 time=10ms TTL=124
Reply from 9.0.0.1: bytes=32 time=1ms TTL=124
Reply from 9.0.0.1: bytes=32 time=11ms TTL=124
Reply from 9.0.0.1: bytes=32 time=12ms TTL=124

Ping statistics for 9.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms
```

-Prueba tracert 5.0.0.1 a 9.0.0.1

```
C:\>tracert 9.0.0.1

Tracing route to 9.0.0.1 over a maximum of 30 hops:

  1    2 ms      0 ms      0 ms      5.255.255.254
  2    0 ms      0 ms      0 ms      2.255.255.254
  3    2 ms      1 ms      10 ms     3.255.255.253
  4    12 ms     5 ms      1 ms      8.255.255.253
  5    0 ms      2 ms      11 ms     9.0.0.1

Trace complete.
```

3. Conclusiones

González Mora Erika Giselle

Las simulaciones implementadas de este protocolo demostraron que BGP es un protocolo fiable que se adapta a cualquier escenario, como así también que funciona correctamente, por lo que no me sorprende su uso masivo en la actual Internet. Se puede observar que depende pura y exclusivamente de las configuraciones realizadas sobre IP, es decir, sin una configuración previa de red en los routers de todas sus conexiones y redes enlazadas es imposible que este protocolo

funcione. Evidentemente, si los routers no conocen a qué y en donde están conectados no pueden correr un protocolo de encaminamiento. La configuración de este protocolo debe ser hecha paso a paso en forma ordenada y metódica, ya que cualquier alteración produce errores de conexión volviendo imposible el correcto funcionamiento. Finalmente, lo más importante que aprendí en la práctica 8, es que el protocolo cuando detecta inconvenientes en el sistema, rápidamente cambia su configuración de encaminamiento para solucionar el problema.

Olivares Ménez Gloria Oliva

Con la realización de esta práctica pudimos poner a prueba y desarrollar de forma virtual el protocolo de enrutamiento BGP. Podemos observar que el protocolo BGP es el más utilizado actualmente y esto es debido a que es un protocolo el cual intercambia la información de enrutamiento entre sistemas autónomos, y a su vez garantiza una elección de rutas libres de bucles. Como mencioné anteriormente, es el protocolo más utilizado para enrutamiento, y esto lo podemos ver ya que es el protocolo que las compañías más importantes de ISP en Internet utilizan; esto es debido a que a diferencia de los protocolos que hemos visto anteriormente (enrutamiento estático, RIP y OSPF) no usa métricas como números de salto, ancho de banda o retardo, BGP toma decisiones de enrutamiento basándose en políticas de la red o reglas utilizadas por varios atributos de ruta BGP. Es un protocolo de enrutamiento que puede utilizarse como protocolo de comunicación entre sistemas autónomos y entre dispositivos dentro de un sistema autónomo. Vemos que es un protocolo sumamente ordenado y con el menor número de fallas debido a que cada router en primera instancia manda su tabla de enrutamiento y se encarga de estar actualizando la misma con nuevas rutas conocidas o eliminando algunas, dependiendo el caso.

4. Bibliografía

colaboradores de Wikipedia. (2020, 12 octubre). *Border Gateway Protocol*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Border_Gateway_Protocol