Universidad Rafael Landívar
Facultad de Ingeniería
Redes I
Sección 01
Catedrático: Denis Donis

TRABAJO DE INVESTIGACIÓN

Alexander Gabriel Villatoro Muñoz
Carné: 1182118

Guatemala, 9 de septiembre de 2021

BGP

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.

En las telecomunicaciones, el protocolo de puerta de enlace de frontera o *Border Gateway Protocol*, -BGP- 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.

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).

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).

El protocolo BGP se utiliza para intercambiar información mediante el establecimiento de una sesión de comunicación entre los enrutadores de frontera de los sistemas autónomos. Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP en el puerto número 179. Esta sesión debe mantenerse activa debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información. Al principio, cada router envía al vecino toda su información de encaminamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad. Además, periódicamente se envían mensajes para garantizar la conectividad.

Desde el punto de vista de su topología, se puede considerar como un gráfico de conexión de sistemas autónomos conectados mediante enlaces virtuales. En la figura a continuación se pueden ver cuatro sistemas autónomos llamados AS1, AS2, AS3 y AS4 conectados por enlaces virtuales. Es decir, que mantienen sesiones BGP sobre TCP para la comunicación entre los sistemas autónomos. Cada sistema autónomo contiene una o más redes que se identificaron como N1, N2 y N3 en AS1, y así sucesivamente. Simplemente observando la figura se puede mostrar que existe más de una ruta posible entre dos sistemas autónomos determinados. Como también es posible tener uno o más de un router de borde en el mismo sistema autónomo.

Cuando una conexión TCP se interrumpe por alguna razón, cada extremo de la comunicación está obligado a dejar de utilizar la información que ha recibido del otro extremo. En otras palabras, la sesión TCP sirve como un enlace virtual entre dos sistemas autónomos vecinos, y cuando hay una falta de intercambio de comunicación indica que el enlace virtual se ha caído. Cabe destacar que esa unión virtual tendrá más de un enlace físico que conecte a los dos enrutadores frontera, pero si una conexión virtual se cae no indica necesariamente que la conexión física se haya caído.

Para la puesta en funcionamiento de la red anterior se debe proveer de un mecanismo de intercambio de rutas que permita comunicar correctamente ambos sistemas. El protocolo BGP utiliza el protocolo de vector de caminos, en inglés, Path vector protocol para el intercambio de información de encaminamiento en la red. Se transmite una lista con identificación de los AS por los que pasa el anuncio. De esa manera se conseguirá saber cómo llegar a

cualquier dirección del prefijo propagado, así como estar preparado para cursar tráfico para cualquier dirección del prefijo.

Habilitación del Ruteo BGP

Suponiendo que se desea tener dos routers, RTA y RTB, con comunicación vía BGP. En el primer ejemplo, el RTA y el RTB están en AS diferentes. En el segundo ejemplo, ambos routers pertenecen al mismo AS.

El dato number en el comando es el número de AS del router al que se desea realizar una conexión con BGP. El dato ip-address es la dirección de salto siguiente con conexión directa para eBGP. Para iBGP, el dato ip-address es cualquier dirección IP en el otro router.

Las dos direcciones IP que utiliza en el comando neighbor de los routers de peer deben poder alcanzarse entre sí. Una manera de verificar la posibilidad de alcance es un ping extendido entre las dos direcciones IP. El ping extendido fuerza al router que hace el ping a utilizar como origen la dirección IP que especifica el comando neighbor. El router debe utilizar esta dirección en lugar de la dirección IP de la interfaz de la cual pasa el paquete.

- *Clear ip bgp address*
    - *El dato address es la dirección de vecino.*

- *Clear ip bgp **
    - *Este comando borra todas las conexiones de vecinos.*

De forma predeterminada, las sesiones de BGP comienzan con el uso de la versión 4 de BGP y negocian de forma descendente las versiones anteriores, en caso de ser necesario. Usted puede prevenir las negociaciones y forzar la versión de BGP que los routers utilizan para comunicarse con un vecino.

Ejecute este comando en el modo de configuración de router:

neighbor {ip address | peer-group-name} version value

IS-IS

IS-IS -*Intermediate System to intermediate System*- es un protocolo de estado de enlace, o SPF -*shortest path first*-, que básicamente maneja un mapa para enrutar paquetes mediante la convergencia de la red. Es también un protocolo de Gateway interior -*IGP*-. Este protocolo está descrito por el RFC 1142. En este se refiere a que IS-IS fue creado con el fin de crear un acompañamiento a CNS -*Protocol for providing the Connectionless-mode Network Service*-.

Las principales características de IS-IS son las siguientes:

1. Es parte de la suite de protocolos de ISO (no TCP/IP).
2. Protocolo de enrutamiento por estado de enlace.
3. Protocolo de enrutamiento classless.
4. Utiliza CLNS y CLNP para brindar un servicio de entrega de datos no orientado a la conexión.
5. Métrica: Costo.
   En IOS es un valor fijo por interfaz.
   Por defecto = 10.
6. Balancea tráfico entre rutas de igual métrica. 4 por defecto, máximo 16.
7. Algoritmo de selección de la mejor ruta: Dijkstra (primero la ruta libre más corta).
8. ID en la tabla de enrutamiento en IOS: i.
9. Distancia Administrativa en IOS: 115.
10. Utiliza LSPs para mantener actualizada la información de enrutamiento.
11. Período de actualización de paquetes hello (IIH): 10 segundos.
12. Soporta sumarización manual de rutas.
13. Utiliza una dirección CLNS como Router ID.
14. Permite la división de la red en múltiples áreas.

Distingue 3 tipos de routers (o sistemas intermedios):

1. Routers Level 1
2. Routers Level
3. Routers Level 1-2

Tablas de información que mantiene el protocolo:

1. Base de datos de adyacencias.
2. Base de datos topológica.

Tipos de redes que diferencia:

1. Broadcast.
2. Point-to-Point.

Es un protocolo de enrutamiento interior desarrollado en los años 80 por Digital Equipment Corporation -DEC- y llamado originalmente DECnet Phase V. Después, fue adoptado por la International Organization for Standardization -*ISO*- como protocolo de enrutamiento para la Interconexión de Sistemas Abiertos -*OSI*-. Su desarrollo estuvo motivado por la necesidad de un sistema no propietario que pudiera soportar un gran esquema de direccionamiento y un diseño jerárquico.

El protocolo de encaminamiento IS-IS está pensado para soportar encaminamiento en grandes dominios consistentes en combinaciones de muchos tipos de subredes. Esto incluye enlaces punto a punto, enlaces multipunto, subredes X.25 y subredes broadcast tales como las ISO 8802 LAN. Para poder soportar dominios grandes, la previsión está hecha para que el ruteo intradominio sea organizado jerárquicamente. Un dominio grande puede ser dividido administrativamente en áreas. Cada sistema reside en exactamente un área.

Los grandes proveedores de servicios de Internet han venido usando IS-IS desde su introducción y recientemente se ha comenzado a implementar en otros mercados. IS-IS permite trabajar con Type of Service -*ToS*- para la ingeniería de tráfico.

Es un protocolo de la capa de red. Permite a sistemas intermedios *IS's* dentro de un mismo dominio cambiar su configuración e información de ruteo para facilitar la información de encaminamiento y funciones de transmisión de la capa de red.

Configuraciones

Router 1

interface Loopback0

ip address 192.200.1.1 255.255.255.255

interface Ethernet0

ip address 192.200.12.1 255.255.255.0

ip router isis

router isis

passive-interface Loopback0

net 49.0001.1720.1600.1001.00

Router 2

interface Loopback0

ip address 192.200.2.2 255.255.255.255

Interface Ethernet0

ip address 192.200.12.2 255.255.255.0

ip router isis

Interface Serial0

ip address 192.200.23.1 255.255.255.252

ip router isis

router isis

passive-interface Loopback0

net 49.0001.1720.1600.2002.00

Router 3

interface Loopback0

ip address 192.200.3.3 255.255.255.255

Interface Serial0

ip address 192.200.23.2 255.255.255.252

ip router Isis

router isis

passive-interface Loopback0

net 49.0001.1234.1600.2231.00

HTTP

Hypertext Transfer Protocol (HTTP) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web. Sigue el clásico modelo cliente-servidor, en el que un cliente establece una conexión, realizando una petición a un servidor y espera una respuesta del mismo. Se trata de un protocolo sin estado, lo que significa que el servidor no guarda ningún dato (estado) entre dos peticiones. Aunque en la mayoría de casos se basa en una conexión del tipo TCP/IP, puede ser usado sobre cualquier capa de transporte segura o de confianza, es decir, sobre cualquier protocolo que no pierda mensajes silenciosamente, tal como UDP.Una transacción HTTP consiste básicamente en:

1. Conexión: establecimiento de una conexión del cliente con el servidor.
2. Solicitud: envío por parte del cliente de un mensaje de solicitud al servidor.
3. Respuesta: envío por parte del servidor de una respuesta al cliente.
4. Cierre: fin de la conexión por parte del cliente y el servidor.

Los métodos más importates de HTTP (especialmente para hacer aplicaciones REST) son GET, POST, PUT, DELETE y HEAD.

1. GET: se emplea para leer una representación de un recurso en un formato concreto, como json o HTML.
2. POST: se emplea cuando se envía información en un *body*, normalmente con formularios.
3. PUT: se emplea normalmente para actualizar contenido.
4. DELETE: elimina un recurso.
5. HEAD: es similar a GET, pero el servidor no devuelve contenido en la respuesta. De este modo, solo interesa el código de respuesta.

Al abrir una página web específica, el intercambio informativo entre el explorador web y el servidor donde reside la información establecerá de qué manera debe transmitirse la información, en qué lugar están las imágenes y en qué orden se me mostrarán, etc. Este intercambio de comandos de solicitud y códigos de respuesta da como resultado la representación en la computadora

de la misma información contenida originalmente en el servidor, que puede estar a miles de kilómetros de distancia.

Con HTTP se establecen criterios de sintaxis y semántica informática (forma y significado) para el establecimiento de la comunicación entre los diferentes elementos que constituyen la arquitectura web: servidores, clientes, proxies.

Se trata de un protocolo «sin estado», es decir decir que no lleva registro de visitas anteriores, sino que siempre empieza de nuevo. La información relativa a visitas previas se almacena en estos sistemas en las llamadas *cookies*, almacenadas en el sistema cliente.

Este protocolo establece las pautas a seguir, los métodos de petición (llamados verbos) y cuenta con cierta flexibilidad para incorporar nuevas peticiones y funcionalidades, en especial a medida que se avanza en sus versiones.

Considerando que la Internet es poco más que una compleja red de intercambio de información entre computadores a distancia, este tipo de herramientas digitales son clave en establecer las bases para ordenar y facilitar la transmisión de la información.

El funcionamiento de HTTP se basa en un esquema de petición-respuesta entre el servidor web y el agente usuario -*user agent*- o cliente que realiza la solicitud de transmisión de datos. Un cliente puede ser un explorador determinado, cuando intentamos abrir una página web, o los rastreadores web -*webcrawlers*- o arañas web, que las inspeccionan.

A ellos, el servidor brinda una respuesta estructurada de modo puntual y dotada de una serie de metadatos, que establecen las pautas para el inicio, desarrollo y cierre de la transmisión de la información. Estos son los «métodos de petición», es decir, los comandos que disparan la ejecución de recursos determinados, cuyos archivos residen en el servidor.

Los HTTP *headers* son la parte central de los HTTP *requests* y *responses*, y transmiten información acerca del navegador del cliente, de la página solicitada, del servidor, etc. Son esquemas de llave-valor que contienen información sobre un *request* y el navegador. Aquí también se encuentran los datos de las *cookies*.

Persistentes: Son conexiones TCP que permanecen abiertas entre operaciones hasta que el cliente o el servidor decide cerrarlas, pero también se ve afectada por el límite de conexiones que para ese momento el servidor esté soportando

Las conexiones persistentes reducen el uso de memoria, el uso de CPU, la congestión de la red, la latencia, y en general mejoran la respuesta de una página con el tiempo.

No persistentes: Son conexiones que se cierran después de cada transacción.

Estas conexiones pueden ser paralelas para mejorar el rendimiento, por lo que un navegador puede realizar x conexiones al mismo tiempo en vez de ir realizando una conexión tras otra (en serie), que habitualmente alargaría el tiempo de conexión.

DNS

Los DNS se encuentran en todos lados estos lo que realizan es que cuando se busque acceder a un contenido desde un navegador este se conecte a la IP del servidor y accedamos al contenido. Pero que es lo que sucede nosotros como usuarios finales generalmente no conocemos la IP del servidor de aplicaciones, por lo tanto, un servidor DNS funciona como un diccionario de distintas IPs con sus respectivos nombres públicos.

Esto le permite a una solicitud que cuando una llega una red de DNS este resuelve su solicitud y lo redirecciona y si en dado caso no conoce el dominio ingresado este es redirigido a otro y así sucesivamente.

Básicamente esto es una tecnología imprescindible por sus distintas configuraciones y paquetes.

Jerarquía de nombre de dominio:

La jerarquía es como un árbol donde la solicitud que se le realiza al servidor DNS procede a ingresar por un nodo raíz el cual concede acceso a toda la jerarquía de DNS.

Cuando un servidor recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de una donde considere adecuada para la solicitud.

La jerarquía depende de cada infraestructura, pero es notable que el DNS es escalable por que la resolución de los nombres de host se distribuye entre varios servidores.

DNS Root Servers

Los Root Servers son una parte crucial de la red, estos servidores son responsables por la funcionalidad de los DNS de internet ya que ellos son los primeros en la resolución de nombres y transiciones.

Estos se encuentran ordenados a través de distintas zonas geográficas donde cada uno es la raíz de cada zona, hasta la cima de la jerarquía.

DNS Request Process

Para el proceso de realizar una solicitud al DNS suceden los siguientes pasos:

1 – Solicitar información al Web site:

En este punto es cuando se solicita a través del navegador un dominio, luego de esto la computadora busca por la IP asociada con el DNS local que posee, si no lo posee realizara una consulta al DNS del buscador por default.

2 – Contactar el DNS Server recursivo:

Cuando la información no se encuentra en la computadora local este solicitara a un DNS recursivo si cuenta con la dirección solicitada y mostrara el website solicitado.

3 – Consultar los DNS Servers Autoritarios:

Si un DNS Server recursivo no puede resolver la solicitud se envía a uno de estos servidores Autoritarios.

4 – Acceso al DNS Record:

Para este punto se debe acceder a la IP del sitio web solicitado, el servidor autoritario le pasara el resultado al DNS recursivo para que este lo almacene de igual manera.

Después de un tiempo los DNS recursivos solicitaran una actualización por medio del Acceso al DNS Record.

5 – Paso final:

La información regresa al origen de la solicitud con el contenido encontrado, y las direcciones IPs de los dominios para que se queden almacenadas dentro de la cache de la computadora.

Record Types

Un registro de DNS es una instrucción que provee información acerca de un dominio incluida su IP asociada junto con el dominio para manejar su información.

- **Tipos:**

- A: El registro donde se guarda la IP
- AAAA: Contiene la IPv6 de la dirección solicitada
- CNAME: Pasa el dominio o subdominio
- MX: Indicar un servidor de correos
- TXT: Son notas que lleva el registro
- NS: Nombre del DNS que respondió
- SOA: Información sobre el dominio
- SRV: Puerto específico del dominio
- PTR: Provee el nombre del dominio en una búsqueda inversa

DNS Zones

Una DNS zone es una porción de los distintos dominios separados por punto de resolución.

Entonces cada zona se divide dependiente del .com, .net, .link. org, etc. Cada uno represente una diferente zona de DNS en la cual están conectados por los Root Servers y poseen como una puerta principal a los dominios .com.

Caso de implementación

Cooperativa de Telecomunicaciones Cochabamba Ltda. (COMTECO)

En el 2010 la cooperativa tomo la desión de desplegar IPv6 en su red, por lo que observo que los ruteadores de borde y los DNS operaban en IPv6 pero no contaban que el tipo de registro era AAAA, porque con el tiempo la organización tomo la decisión de adaptar su infraestructura de DNS hacia un clúster de DNS.

Con esto mejoraron el mejor manejo de sus transacciones y tráfico, tanto interno como externo.