Grupo 1. Prof. Gabriela Barrantes
20 de junio de 2017

pseudoBGP

Fase I

1. Descripción

Se pretende codificar parte del comportamiento de enrutamiento en sistemas autónomos (AS) para estudiar sus efectos en la calidad de servicio ofrecida.

2. Fase I

A realizar en pares de grupos. El objetivo de esta fase es experimentar con comunicación con sockets TCP, y operacionalizar las actualizaciones de pseudoBGP. Cada grupo va a representar un sistema autónomo con uno o más "enrutadores" de pseudoBGP (procesos servidores). Una red de relaciones entre estos enrutadores debe ser creada de tal manera que al final cada enrutador externo tenga una tabla de enrutamiento pseudoBGP consistente.

3. Reglas del juego

Se definen las reglas de creación de "enrutadores", conexión de vecinos, e intercambio de información de alcanzabilidad

3.1. Creación de "servidor".

Para arrancar un enrutador pseudoBGP, deben comunicarle su propia dirección IP y máscara, su número de sistema autónomo (2 bytes). El "enrutador" debe escuchar con TCP en el puerto 57809, y enviar desde el puerto que dinámicamente le asigne el sistema operativo.

El enrutador debe contar con una interfaz de operador que permita digitar una lista inicial de destinos alcanzables, cada uno de los cuales se especifica con un número IP de red, una máscara, y una lista de sistemas autónomos (especificados por números de 2 bytes) que se deben seguir a partir del sistema autónomo en el que se encuentra el enrutador para llegar al destino.

3.2. Adquisición de vecinos/ Desconexión

Al inicio, un enrutador no conoce a nadie y va a adquirir "vecinos" de forma dinámica. Se definen dos formas de adquirir/perder vecinos.

3.2.1. Adquisición de vecinos via interfaz

Se decide agregar un vecino a través de una interfaz con un operador humano en el servidor. Se debe poder indicar que se conecte con otro enrutador pseudoBGP para que se conviertan en "vecinos". Para esto, se le debe indicar la dirección IP y la máscara del servidor con el que se va a conectar. Usando esta misma interfaz se debe poder desconectar un vecino.

- Una vez leída la dirección del futuro vecino, se envía una solicitud de conexión: un paquete que contiene lo siguiente:

- 1 byte con valor 1 (solicitud de conexión)
- 2 bytes con el número de sistema autónomo del solicitante
- 4 bytes con el número IP del servidor solicitante
- 4 bytes con la máscara de red del servidor solicitante

-
- Se espera una respuesta del futuro vecino indicando su conformidad:
  - 1 byte con valor 2 (conexión como vecino aceptada)
  - 2 bytes con el número de sistema autónomo del vecino
  - 4 bytes con el IP del vecino
  - 4 bytes con la máscara del vecino

- Si no se ha recibido una respuesta luego de 5 segundos, se asume que el servidor no está dispuesto a convertirse en vecino y se informa al operador que ese servidor **no aceptó** convertirse en vecino.

- Si ocurre cualquier otro tipo de error, se informa al operador que no se logró establecer comunicación con el vecino.

3.2.2. Adquisición de vecinos via mensaje recibido en el puerto pseudoBGP

Se pude recibir la solicitud por parte de otro erutador pseudoBGP. De momento se obviarán elementos de autenticación.

- Se procede cuando se recibe un mensaje conteniendo lo siguiente:
  - 1 byte con valor 1 (solicitud de conexión)
  - 2 bytes con el número de sistema autónomo del solicitante
  - 4 bytes con el número IP del servidor solicitante
  - 4 bytes con la máscara de red del servidor solicitante

  y se debe responder indicando conformidad:
  - 1 byte con valor 2 (conexión como vecino aceptada)
  - 2 bytes con el número de sistema autónomo del vecino
  - 4 bytes con el IP del vecino
  - 4 bytes con la máscara del vecino

De momento, no se contemplarán casos en que la conexión deba ser rechazada.

3.2.3. Desconexión de vecinos

Para desconectar vecinos, se deben enviar una solicitud con valor 3 en el primer byte, e incluye todos los demás campos identificando al solicitante de desconexión. No se pueden rechazar solicitudes de desconexión. En un cierre limpio, el vecino al que se le solicita desconexión debe responder con el mismo mensaje, pero con un valer de 4 en el primer byte. Si el mensaje confirmando desconexión no ha llegado en 5 segundos, la conexión se cierra de todas maneras. Si se recibe una actualización de un vecino oficialmente desconectado, se debe ignorar la actualización y volver a enviarle el mensaje de desconexión. No existen cierres por eventos externos. Un vecino sigue siendo vecino eternamente a menos que se reciba un mensaje de desconexión. La decisión original de desconectar proviene de la interfaz de operador del enrutador.

3.2.4. Intercambio de información de alcanzabilidad

Los mensajes solo pueden intercambiarse entre vecinos y van a llegar de forma asincrónica.

Cada mensaje está compuesto de:

- Identificador de sistema autónomo de origen (2 bytes)
- La cantidad de destinos incluidos en la actualización (4 bytes)
- Una lista de destinos indicados como una red IP (4 bytes) y su máscara de red (4 bytes). Inmediatamente luego de la máscara de red de cada destino, debe aparecer:
    - La cantidad de sistemas autónomos incluidos en la lista (2 bytes)
    - Una lista de uno o más sistemas autónomos que se deben seguir (cada AS debe estar especificado por un número de 2 bytes).

Los mensajes de alcanzabilidad no se confirman, únicamente son usados para actualizar las tablas de enrutamiento.

Cada enrutador debe enviar su información de alcanzabilidad cada 30 segundos a todos sus vecinos, o cuando el operador se lo indique.

4. Estructuras internas

Cada enrutador pseudoBGP debe contener dos tablas de enrutamiento:

- La tabla de vecinos, que debe especificar el ip y máscara del vecino y el sistema autónomo del vecino (2 bytes). Se debe guardar en una bitácora el registro de construcción de esta tabla, con timestamps, incluyendo momento en que se constituyó en vecino, origen (operador o mensaje), momento en que se desligó como vecino.
- La tabla de alcanzabilidad que relaciona la información de alcanzabilidad intercambiada con dirección IP de los vecinos. Se debe mantener una bitácora de actualizaciones de esta tabla también.

5. Testing

Deben crear al menos tres enrutadores pseudoBGP por sistema autónomo (por grupo), cada uno con una lista inicial de alcanzabilidad de al menos 5 redes IP. Diagramen una red de vecinos intra y extra sistema autónomo, y conéctentlos. Verifiquen que el diagrama esperado de conexión efectivamente corresponda a las tablas de enrutamiento internas. Verifiquen que las tablas de alcanzabilidad también sean consistentes luego de que el sistema se estabilice.

6. Entregables

- Código fuente y código ejecutable del enrutador pseudoBGP
- Documentación de uso del programa
- Documentación de las pruebas.

Fecha de entrega: 27 de junio de 2017.