Redes de Computadoras

Curso 2024

Grupo 03

Informe - Obligatorio 02

Autores:
Antonio González
Dumas Bentancur
Jerónimo Jacques

Supervisor:
Leonardo Vidal

18 de noviembre de 2024

Índice

1. Introducción

Este trabajo consta de 3 partes, donde la primera parte se basará en el desarrollo de una función de reenvío de un router con tabla de enrutamiento estático, realizando las pruebas en el mismo escenario que en el obligatorio 1. Luego, la segunda parte se desarrollará la función de enrutamiento de un router mediante el protocolo PSWOSPF para que el router pueda generar su tabla de reenvío automáticamente basándose en las rutas anunciadas por otros routers de la red. Por último, la tercera parte consiste en una evaluación de nuestra solución completa, evaluando las funcionalidades requeridas en partes anteriores así como también los casos de errores contemplados.

2. Parte 3

2.1. Documentación de la evaluación a nuestra solución

Para analizar el correcto funcionamiento de nuestra solución se utilizará tcpdump y wireshark. Todas las capturas están en la carpeta CapturasOb2 y cada una de ellas sera referenciada en este documento por su nombre.

2.1.1. Funcionamiento general de PWOSPF

Para comenzar, analizaremos el correcto funcionamiento de los Hello Packet´s, tanto su envío como la recepción de los mismos. Para ello nos basaremos fundamentalmente en el router 1 y analizaremos todas sus interfaces. Primero vemos la interfaz 1 (eth1) que esta capturada en el archivo vh1e1t.pcap, en la misma se puede apreciar el correcto funcionamiento del envío de hellos, ya que estos son enviados cada cierto tiempo relativamente constante, donde este se parece mucho a OSPF_DEFAULT_HELLOINT que es 5 segundos que es el tiempo que debe de pasar para que una interfaz envié un mensaje hello por todas sus interfaces.

Además notar, que aunque wireshark no reconoce el protocolo OSPWF, podemos notar que el paquete es enviado desde la interfaz eth1 del router 1 (que tiene

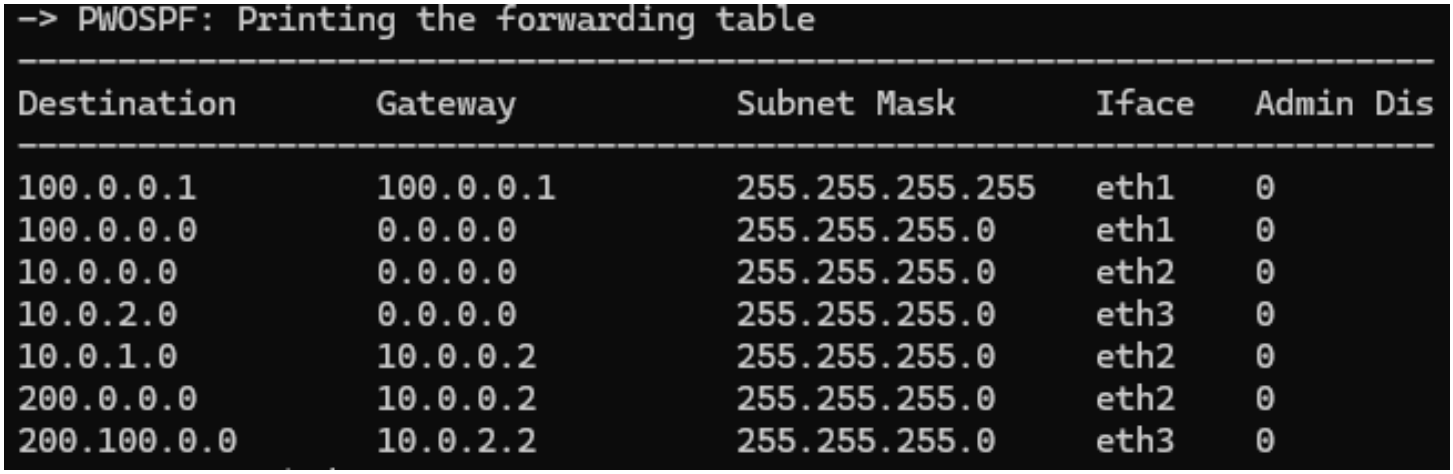
IP 100.0.0.50) a la dirección IP del broadcast, donde la misma es 224.0.0.5.

También, viendo capturas de las demás interfaces del mismo router (vh1e3t.pcap,vh1e2t.pcap) se puede ver que, en el cabezal del protocolo OSPWF, el router Id de todas las interfaces coincide y es 100.0.0.50 que es correcto ya que la misma es la dirección de las interfaces mayor de todas las interfaces del router 1, y por como esta seleccionado el router Id en el código esto coincide.

Por otro lado, viendo las capturas de las interfaces eth2 y eth3 (vh1e3t.pcap, vh1e2t.pcap) podemos notar que ambas reciben paquetes Hello, ya que estas si poseen vecinos, no como la interfaz eth1 que la misma no recibía Hello's ya que esta no posee routers vecinos (su único vecino es el cliente que no envía estos mensajes). Notar que la captura fue realizada tiempo despues de que los routers comiencen a funcionar, por lo tanto no se captura el momento de cuando el vecino es añadido a la lista de vecinos por la llegada del primer hello del mismo ya que se puede notar que siempre que llega un hello no se envian LSU.

A su vez, en la captura vh1e2t.pcap, al final, se puede ver el correcto funcionamiento de la recepción de paquetes LSU, en este caso, primero es el router 1 quien envía un paquete LSU mediante esta interfaz a todos lo vecinos de esta misma, luego este recibe los paquetes LSU de la interfaz 10.0.0.2 que es su vecino, y ese paquete LSU recibido es reenviado a todas las interfaces menos por la que llegó, que es la que estamos analizando, con esto podemos corroborar el funcionamiento del envío de los LSU ya estos deben ser enviados cada 30s aproximadamente y esto se cumple ya que son enviados en el tiempo 0.05 y luego reenviados en el tiempo 30.06 como así lo muestra la captura.

Aquí se puede ver la tabla de forwarding generada por el router 1, la cual queda igual la generada por el binario entregado.



```
-> PWOSPF: Printing the forwarding table
------------------------------------------------------------------------
Destination       Gateway          Subnet Mask       Iface   Admin Dis
------------------------------------------------------------------------
100.0.0.1         100.0.0.1        255.255.255.255   eth1    0
100.0.0.0         0.0.0.0          255.255.255.0     eth1    0
10.0.0.0          0.0.0.0          255.255.255.0     eth2    0
10.0.2.0          0.0.0.0          255.255.255.0     eth3    0
10.0.1.0          10.0.0.2         255.255.255.0     eth2    0
200.0.0.0         10.0.0.2         255.255.255.0     eth2    0
200.100.0.0       10.0.2.2         255.255.255.0     eth3    0
```

2.1.2. Pruebas con biblioteca RPC realizada en el Ob1

En esta misma captura se puede ver el trafico de los paquetes los cuales corresponden a nuestra aplicación de test cliente con nuestro servidor, test servidor, donde todos los paquetes son dirigidos (tienen la dirección IP de destino) hacia el servidor con dirección IP 200.0.0.10, esto concuerda con la topología dada, ya que es esta interfaz (la de la captura), la eth2, por la que el router 1 debe salir para llegar en menos saltos al servidor con la dirección IP antes mencionada, por lo tanto en esta parte podemos concluir que la tabla de enrutamiento para llegar a los servidores se esta formando de manera correcta.

Lo mismo podemos decir sobre todos los paquetes que son dirigidos hacia el servidor con dirección IP 200.100.0.15 (tanto los enviados por el cliente hacia el servidor como los enviados por el servidor hacia el cliente), donde los mismos son capturados unicamente por la interfaz eth3 (vh1e3t.pcap).

2.1.3. Pruebas para generar mensajes ICMP error

Por otro lado, para corroborar el funcionamiento de nuestros routers a la hora de tener que responder, ya sea porque el paquete que recibieron tenía como destino a alguno de sus interfaces o el paquete que recibieron no podía ser reenviado y se debe responder con un ICMP de error, debemos de fijarnos en la captura con nombre vh1e1noex.pcap, donde la misma esta dedicada a una ejecución donde se

corrió ping con distintas interfaces las cuales generaban error ya que no existen. Esta captura es sobre la interfaz eth1 del router 1, que es la que esta conectada con el cliente.

Se puede observar el paquete ICMP echo request generado por el cliente y enviado hacia la interfaz inexistente, luego se nota que no hay respuesta echo reply al echo request enviado por el cliente si no que hay un mensaje ICMP host unreachable enviado por la interfaz 10.0.0.2, la cual corresponde a la interfaz eth1 del router 2. Podemos notar que el enrutamiento es correcto ya que la dirección a la cual se quería hacer el ping era perteneciente a la misma subred del servidor 1, o sea el enrutamiento se hizo correctamente por el router 2.

Por otro lado, capturando los mensajes por las interfaces del router 1 como mencionamos anteriormente y del cliente (clientenoex.pcap) podemos notar que nuestros routers, en especial el router 2 que es donde se realiza la prueba, responden manera correcta frente al intento de reenvío de un paquete a una dirección inexistente ya que se genera el ICMP host unreachable adecuado y este es enviado a quien mando el paquete original que causo error, en este caso el cliente, que es recibido por el mismo como así se puede notar en la captura.

Además, en la captura se puede apreciar que el mensaje ICMP Host Unreachable recibido contiene los primeros bytes del mensaje ICMP echo reply que causo el error, pudiendo identificar el paquete por la dirección IP de origen y destino del mismo. Lo mismo puede ser notado en estas capturas, más adelante, cuando se intenta hacer ping en un caso similar a una interfaz inexistente pero de la subred correspondiente al enlace entre el router 1 y el router 2, donde el router 1 es el encargado de notar que la dirección no existe y formar y enviar el paquete ICMP Host Unreachable, como así lo demuestran las capturas ya que el mismo es enviado con IP origen igual al de la interfaz eth1 del router 1 (100.0.0.50).

2.1.4. Pruebas con ping y traceroute a interfaces existentes

Distinto es el caso de cuando el cliente intenta realizar ping a una interfaz existente (como se ve en las capturas capAntesYPingBienVHost12.pcap, capAntesYPingBienVHost12.pcap, capAntesYPingBienVHost13.pcap, capAntesYPingBienCliente.pcap, donde las primeras corresponden al las tres 3 interfaces del host1 y la última al cliente) en esta red, si el ping es hacia alguno de los servidores se puede notar que cada router por el que pasa disminuye el TTL como así lo debe de hacer y ademas recibe, analiza y reenvía los ICMP echo request y echo reply de manera adecuada. A su vez, cuando se hace ping a alguna interfaz de un router este siempre construye y envía el mensaje ICMP echo reply de manera adecuada.

Luego en la captura clientTR.pcap se puede observar el correcto funcionamiento al ejecutar el comando traceroute desde el cliente al router 2 (fijando que se envíen un solo mensaje por cada TTL y limitando el TTL hasta 3), dado que se ve como salen del cliente los 3 mensajes UDP hacia el router 2 con TTL 1, 2 y 3 respectivamente. Y se puede ver que al primero el router 1 le responde con un ICMP Time exceeded, y a los otros el router 2 les responde con mensajes ICMP Port Unreachable como es debido.

2.1.5. Pruebas de caída y recuperación de routers con la nueva topología

Pasamos ahora a las pruebas con la nueva topología, donde la misma esta compuesta por 5 routers en vez de 3 como lo hacia la topología anterior. Para estas pruebas ejecutamos ping antes y después de la perdida y recuperación de distintos routers.

Para esta parte capturamos al cliente y las tres interfaces del router 1 (las capturas son topoNueva3Cliente.pcap, topoNueva3VH11.pcap, topoNueva3VH12.pcap y topoNueva3VH13.pcap). Podemos notar que la ejecución de ping cuando están todos los routers funcionando al servidor 150.150.0.2 sigue la ruta adecuada ya que en el router 1 sale por la interfaz eth2 que va hacia el router 2, para luego seguir por el 2, y luego el 4 para llegar finalmente al servidor (esto último no se ve en la

captura pero lo vimos en los vhosts).

De la misma forma sucede cuando se ejecuta ping al otro servidor, el de dirección 100.100.0.2, donde podemos notar que el paquete es capturado por la interfaz eth3 y no la eth2, por lo tanto el enrutamiento es por la ruta de abajo (router 1, router 3, router 5 y luego servidor server2). Esto se puede corroborar con la tabla de enrutamiento generada e impresa en cada uno de los routers.

En ambos casos anteriores se ve que el TTL es 61, es decir, da 3 saltos antes de llegar al destino. Una vez se baja el router 2, podemos notar que al hacer ping al servidor server1 ahora el paquete ICMP echo request en vez de ser capturado por la interfaz eth2 es capturado por la interfaz eth3, por lo tanto podemos asegurar que sigue una ruta distinta, donde ademas el cliente recibe el ICMP echo reply enviado por el servidor (con TTL 60 ya que da un salto más), por lo tanto podemos asegurar que nuestros routers son capaces de recuperarse ante la caída de alguno de ellos para obtener una nueva ruta hacia destinos los cuales antes eran accedidos mediante el router caído.

También probamos de hacerle un ping a la interfaz del router 4 directamente conectada al router caído y vuelve a suceder que en el router 1 el ICMP eco request sale por la interfaz eth3 en vez de la eth2, pudiendo llegar a su destino y respondiendo con un eco reply que llega al cliente.

Una vez se levanta nuevamente el router 2 se puede notar en la captura que al hacer ping al servidor server1 ahora nuevamente el paquete ICMP echo request y el echo reply son capturados por la interfaz eth2 del router (y el TTL vuelve a 61) lo que nos da la idea de que el enrutamiento volvió a ser el de antes de la caída, por lo tanto la recuperación es correcta.

Todo lo mencionado anteriormente sucede de manera análoga frente a la caída del router 3 y el intento de envió de paquetes al servidor server2. Todas estas pruebas nos dan a entender que el funcionamiento de nuestra implementación de la función de enrutamiento de un router mediante el protocolo PSWOSPF funciona de manera correcta en la inicialización de cada uno de los routers así como

también es capaz de reponerse frente a la caída de alguno de los routers encontrando y calculando nuevas rutas para llegar a todos los destinos posibles.

En todos los casos mencionados anteriormente se cumple que, antes del envío de paquetes cada interfaz, hay veces que, se pregunta por la dirección MAC de próximo salto que da el paquete, esto corrobora el correcto funcionamiento de las consultas ARP, las cuales son realizadas cuando el mapeo <dirección IP, dirección MAC> no esta en la tabla ARP del router, es por ello que las solicitudes no son realizadas siempre.