**Informe Obligatorio 3**

**Redes de Computadoras 2012**

**INCO – Facultad de Ingeniería – UdelaR**

**Noviembre 2012**

Grupo 59

Álvaro Acuña – CI: 3826062-8

Gabriel Centurión – CI: 2793486-8

Germán Mamberto – CI: 3187102-8

Fernando Mangino – CI: 3621009-1

Tabla de contenido

[Objetivo 3](#_Toc339206233)

[Laboratorio de Routing y Forwarding (rip) 3](#_Toc339206234)

[Laboratorio de Routing y Forwarding (ospf) 3](#_Toc339206235)

[Laboratorio de Bridging (two-switches) 3](#_Toc339206236)

Objetivo

Laboratorio de Routing y Forwarding (rip)

La configuración y presentación detallada de este laboratorio se encuentra disponible en la *Wiki*

*de Netkit → Official Labs → Basic Topics*.

a) Instale el laboratorio RIP [5], arranque la ejecución y siga las instrucciones detalladas en

[6].

b) Antes de levantar el demonio zebra inicie una captura de paquetes completos con

tcpdump en TODAS las interfaces de **r1** en el archivo

/hosthome/ripd.startup.r1.cap; una vez iniciada la captura, proceda a levantar

los demonios zebra en **r1**, **r2**, **r3**, **r4**. Luego de levantados todos los demonios, espere 30

segundos y cierre el archivo de captura.

c) Abra el archivo ripd.startup.r1.cap con wireshark y consulte en [7] para

responder lo siguiente:

1. ¿Cuál es el contenido de los mensajes *Request*?

2. ¿Cuál es la dirección de destino de los mensajes *Request*? ¿Por qué?

3. ¿Cuál es el *Next Hop* especificado en las entradas de un comando *Response*? ¿Por

qué?

4. Especifique cómo visualizar la información de mensajería de RIP utilizando la utilidad

debug del demonio ripd. Implemente el debug en **r1** y capture los mensajes en el

archivo /hosthome/ripd.log.r1.cap.

d) Siga adelante con el laboratorio según lo especificado en [6].

e) Conéctese al demonio zebra en **r3** con el comando telnet localhost zebra.

Utilizando el comando sh ip route identifique los *Next Hop* para las redes

100.1.0.12/30 y 100.1.0.0/30. Identifique la distancia administrativa y la métrica en los

números entre corchetes [120/2]; comente.

f) ¿Por qué es necesario agregar una ruta estática a 100.1.0.0/16 en **r5**?

g) ¿Por qué se instala una ruta por defecto en **r4**? ¿Por qué se redistribuye en RIP?

h) Especifique las modificaciones que debeía realizar en la configuración **r5** para que el

comando ping 193.204.161.1 ejecutado en cualquiera de los routers **r1**..**r4** sea

exitoso. Impleméntelo y compruebe. Almacene los archivos del laboratorio modificado en

el directorio IRC-lab\_rip.

Laboratorio de Routing y Forwarding (ospf)

Dado el ejemplo anterior (con las modificaciones especificadas en el apartado h), cambie el

protocolo de *routing* de RIP a OSPF con una única área de *backbone*.

a) ¿Se puede hacer desde en línea (sin re-levantar el laboratorio)? Justifique su respuesta.

Almacene los archivos del laboratorio modificado en el directorio IRC-lab\_ospf.

b) Una vez que cambie a OSPF, siga las mismas instrucciones detalladas en [6] para el

laboratorio RIP, pero ahora sabiendo que el protocolo de *routing* utilizado es OSPF.

c) Antes de levantar el demonio zebra inicie una captura de paquetes completos con

Página 2 de 4

Redes de Computadoras Obligatorio 3-2012

tcpdump en TODAS las interfaces de **r1** en el archivo

/hosthome/ospfd.startup.r1.cap; una vez iniciada la captura, proceda a levantar

los demonios zebra en **r1**, **r2**, **r3**, **r4**. Luego de levantados todos los demonios, espere 30

segundos y cierre el archivo de captura.

d) Abra el archivo ospfd.startup.r1.cap con wireshark y consulte en [8] para

responder lo siguiente:

1. Describa las características de los mensajes *LS Request, LS Update y LS*

*Acknowledge.*

2. ¿Cuál es la dirección de destino de los mensajes *Hello*? Por qué?

3. ¿Cuáles son los *Router ID* para **r1**..**r4**?

4. Consulte el archivo de log del ospfd en **r1** y comente sobre el proceso *DR-Election*.

¿Cuál es el rol del *DR* y el *Backup-DR*?

e) Siga adelante con el laboratorio según lo especificado en [6].

f) ¿Cómo se redistribuye la ruta por defecto hacia **r5** en OSPF? Verifique que se propague

efectivamente en **r1**..**r3**.

g) Conéctese al demonio ospf en **r3** con el comando telnet localhost ospfd.

Utilizando el comando sh ip ospf route identifique las rutas externas de OSPF tipo 2

(E2). Comente el resultado.

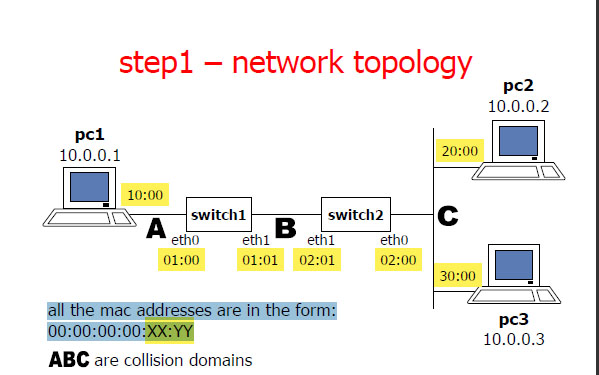
h) Conéctese al demonio zebra en **r3** con el comando telnet localhost zebra.

Utilizando el comando sh ip route identifique los *Next Hop* para las redes

100.1.0.12/30 y 100.1.0.0/30. Compare con el resultado obtenido para el protocolo RIP y

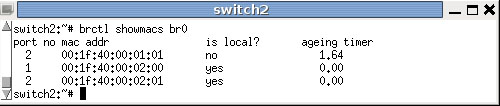
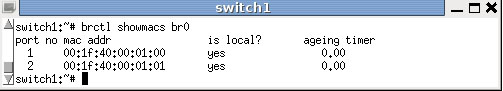
comente.

Laboratorio de Bridging (two-switches)

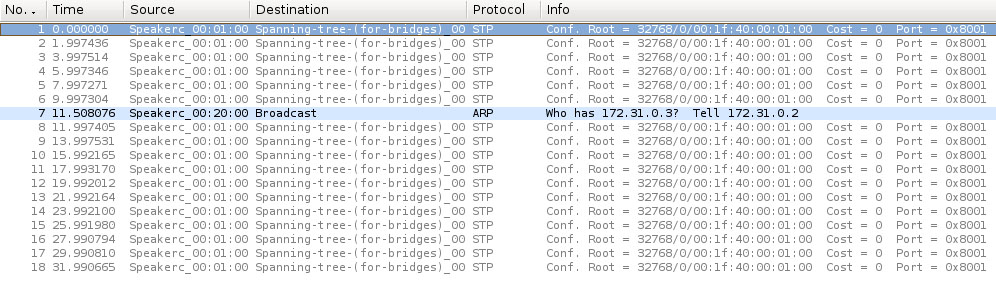
**a) Instale el laboratorio de Bridging [9] e inicie la ejecución.**  
    Para ejecutar entro al directorio y ejecuto lstart. Esto crea varias maquinas virtuales según la topología de la red que representan shitches y pcs en este caso.  
  
**b) Vincule el contenido del archivo lab.conf con la topología de red que aparece en la diapositiva 3 de la presentación [10].**  
  
  
  
pc1[0]="A"  
switch1[0]="A"  
pc1 y switch1 están conectados al mismo dominio de colisión "A"  
  
pc2[0]="C"  
pc3[0]="C"  
switch2[0]="C"  
  
pc2 y pc3 se encuentran conectados al switch2 por el  dominio de colisión “C”  
  
switch1[1]="B"  
switch2[1]="B"  
  
switch1 y switch2 están conectados al mismo dominio de colisión “B”  
  
**c) Utilizando el comando ifconfig verifique que el plan de numeración (tanto IP como MAC) es el documentado en la misma diapositiva.**  
  
Ejecuto ifconfig para pc1, pc2 y pc3 analizando la IP (inet addr) y la MAC (HWadd) comprobando que son iguales. Para Switch1 y Switch2 hago lo mismo verificando la dirección MAC de las interfaces (eth0 y eth1)  
Las direcciones MAC son de la forma:00:00:00:00:XX:YY  
  
Este es el resultado de la ejecución del comando que coincide con la imagen de la diapositiva

|  |  |  |
| --- | --- | --- |
|  | **IP (inet addr)** | **MAC (HWadd)** |
| **PC1** | 10.0.0.1 | 10:00 |
| **PC2** | 10.0.0.2 | 20:00 |
| **PC3** | 10.0.0.3 | 30:00 |
| **Switch1** |  | eth0 = 01:00 y eth1 =01:01 |
| **Switch2** |  | eth0 = 02:00 y eth1 =02:01 |

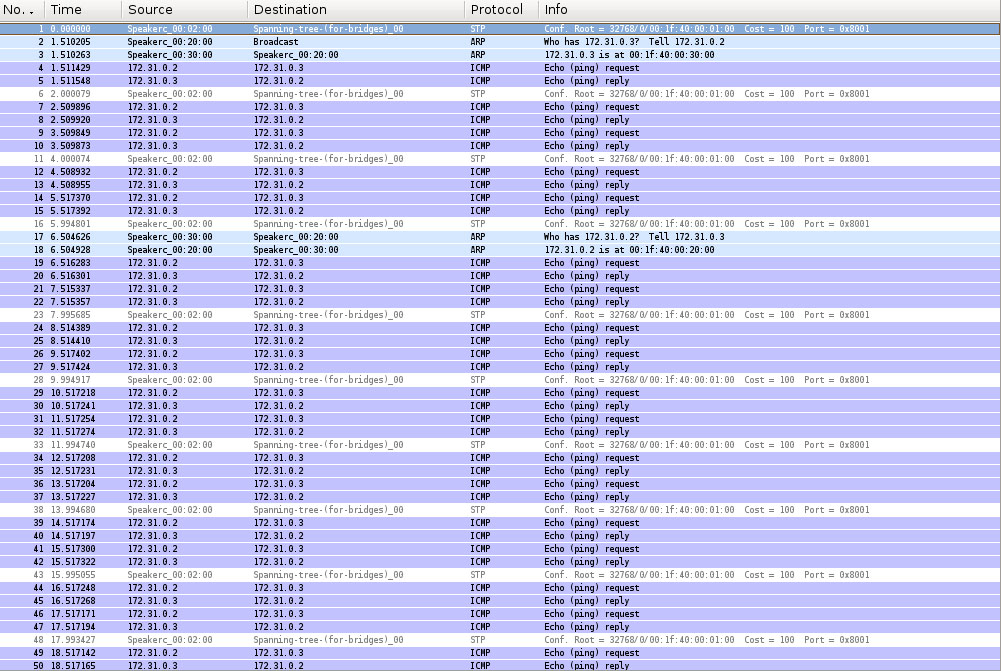
**d) Modifique el plan de numeración IP de toda la red de forma que pertenezcan al prefijo 172.31.0.0/24 manteniendo el valor del último byte de cada dirección IP según el plan de numeración que aparece en la diapositiva 3.**  
  
Para esto utilizo el comando: “ifconfig eth0 IP up” en cada una de las PCs  
  
**Para PC1:** ifconfig eth0 172.31.0.1 up  
**Para PC2:** ifconfig eth0 172.31.0.2 up  
**Para PC3:** ifconfig eth0 172.31.0.3 up  
  
**e) Modifique las direcciones MAC de toda la red de forma que se emulen tarjetas de red fabricadas por la empresa Speakercraft Inc.**  
  
La OUI del fabricante Speakercraft es: 00:1F:40 esto lo voy a utilizar como prefijo de las direcciones MAC utilizando el comando “ifconfig eth0 hw ether MAC\_ADDRESS” para modificar la dirección MAC.  
  
**ref:** [**http://mac.freenetworks.org/ouis/7946-mac-address-001F40**](http://mac.freenetworks.org/ouis/7946-mac-address-001F40)  
  
**pc1:** ifconfig eth0 hw ether 00:1F:40:00:10:00  
**pc2:** ifconfig eth0 hw ether 00:1F:40:00:20:00  
**pc3:** ifconfig eth0 hw ether 00:1F:40:00:30:00  
  
**Switch1 eth0:** ifconfig eth0 hw ether 00:1F:40:00:01:00  
**Switch1 eth1:** ifconfig eth1 hw ether 00:1F:40:00:01:01  
  
**Switch2 eth0:** ifconfig eth0 hw ether 00:1F:40:00:02:00  
**Switch2 eth1:** ifconfig eth1 hw ether 00:1F:40:00:02:01  
  
  
**f) Documente los comandos utilizados para realizar las dos partes anteriores.**  
Ya fueron comentados en las partes correspondientes.  
  
**g) A partir de aquí, documente y analice los cambios relevantes en el contenido de las tablas**  
**de direcciones MAC de los switches de la topología, antes y después de cada comando**  
**ejecutado.**  
**1. Genere tráfico desde pc2 hacia pc3 (mediante el comando ping) pero previamente y**  
**utilizando el comando tcpdump, capture el tráfico en pc1 y en pc3 en los archivos**  
**/hosthome/ping.pc1.g1.cap y /hosthome/ping.pc3.g1.cap**  
**respectivamente. Luego de unos 15 segundos de estar generando tráfico, detenga el**  
**ping y las capturas. Analice con wireshark las capturas realizadas y explique el**  
**comportamento observado.**  
  
Para obtener las tablas de direcciones MAC a utilizo el comando: brctl showmacs br0 para ambos swittches  
Estas son las tablas iniciales para switch1 y switch2:

  
  
  
**Capturando tráfico en pc1 y pc3**  
  
**Para pc1:** tcpdump –i eth0 –w /hosthome/ping.pc1.g1.cap   
**Para pc3:** tcpdump –i eth0 –w /hosthome/ping.pc3.g1.cap   
  
**Genero trafico usando el comando ping desde pc2 hacia pc3**  
  
ping 172.31.0.3  (esto se ejecuta en pc2)  
  
**Luego utilizo wireshark para analiza el contenido de los archivos generados.**

**Para pc1:**

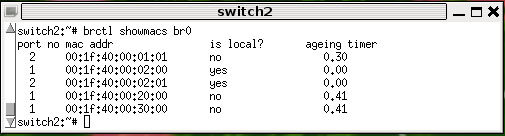
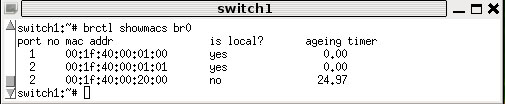
  
  
Todos los paquetes menos el numero 7 están usando el protocolo Spanning Tree que sirve para gestionar los bucles en la topología  red, este protocolo utiliza paquetes  llamados BPDU (Bridge Protocol Data Units). Cuando se dan estos bucles puede pasar de que se reenvíen indefinidamente los paquetes broadcast creando un bucle infinito que consumiría mucha ancho de banda pudiendo degradar la red en muy poco tiempo  
  
El paquete número 7 es un ARP request desde PC2 preguntando quién tiene la IP 172.31.0.3. Este paquete se envía por broadcast a toda la red.

**Para pc2:**

  
  
**Diferenciamos los distintos tipos de paquetes que se ven aquí:**

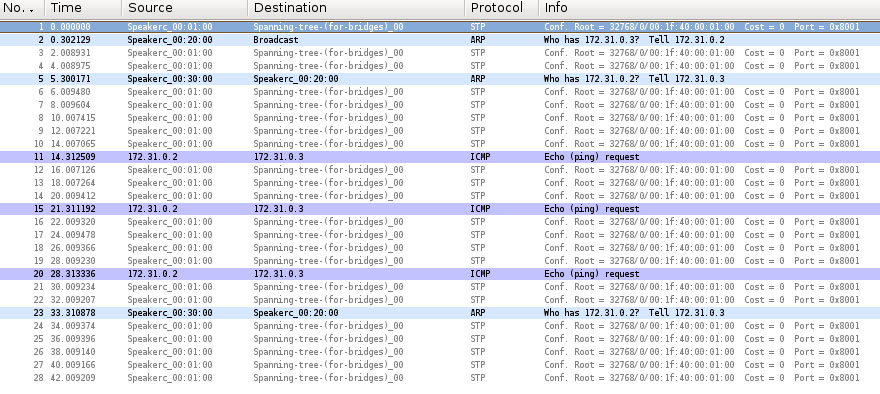
* Están los BPDU  utilizados por el protocolo Spanning Tree, si nos fijamos la columna source podemos saber la MAC del origen que en este caso es switch2.
* Los paquetes ICMP son producidos por el ping desde PC2 a PC3.
* Tambien observamos los paquetes  ARP request y ARP reply. El primero pregunta por broadcast a que dirección MAC pertenece una IP y el segundo le responde, pudiendo ser la propia maquina u otra que la conozca.

Por ejemplo en la fila 2,3: PC2 pregunta por 172.31.0.3 y es PC3 quien contesta.  
En la fila 17,18:  PC3  pregunta por 172.31.0.2, y es PC2 quien contesta  
  
Esto hace que las tablas de direcciones MAC de los switches se actualicen con las MAC de PC2 y PC3  
  
  
**Observemos las tablas ahora:**

  
  
  
Switch1 ahora conoce a pc2, hay que tener en cuenta que el trafico generado por pc3 es filtrado por el switch2  
  
Switch2 ahora conoce a pc2 y pc3  
  
pc1 no es conocido por ningún switch ya que el único mensaje que le llega es un  ARP request de PC2 en broadcast. Luego de que Switch2 conoce a pc2 y a pc3  este filtra el contenido de estas pc al resto de la red.  
  
  
  
**2. ¿Cuál es el tiempo de vida (lifetime) por defecto de las entradas en las tablas de**  
**direcciones MAC de ambos switches? Configure su valor en 3 segundos.**  
  
Utilizo  el comando “brctl showstp br0” en ambos switches para obtener el lifetime por defecto. Este se muestra en el campo “ageing time” y es de 300 segundos.  
  
Para cambiar este valor ejecuto en ambos switches el comando: “brctl setageing br0 3” para setearlo en 3 segundos.  
  
**3. Luego que las entradas correspondientes a las direcciones MAC de los pcs hayan**  
**desaparecido de las tablas de los switches, vuelva a generar tráfico desde pc2 hacia**  
**pc3 (utilizando nuevamente el comando ping) pero ahora forzando que cada**  
**mensaje ICMP echo (Request) se envíe cada 7 segundos; previamente y utilizando**  
**nuevamente el comando tcpdump, capture el tráfico en pc1 y en pc3 en los archivos**  
**/hosthome/ping.pc1.g3.cap y /hosthome/ping.pc3.g3.cap**  
**respectivamente. Luego de unos 30 segundos de estar generando tráfico, detenga el**  
**ping y las capturas. Analice con wireshark las capturas realizadas y explique el**  
**comportamiento observado. Almacene los archivos del laboratorio modificado en el**  
**directorio IRC-lab\_two-switches.**

**Capturando tráfico en pc1 y pc3**  
  
**Para pc1:** tcpdump –i eth0 –w /hosthome/ping.pc1.g3.cap   
**Para pc3:** tcpdump –i eth0 –w /hosthome/ping.pc3.g3.cap   
  
  
**Genero trafico desde pc2 hacia pc3 cada 7 segundos**  
ping –i 7 173.31.0.3

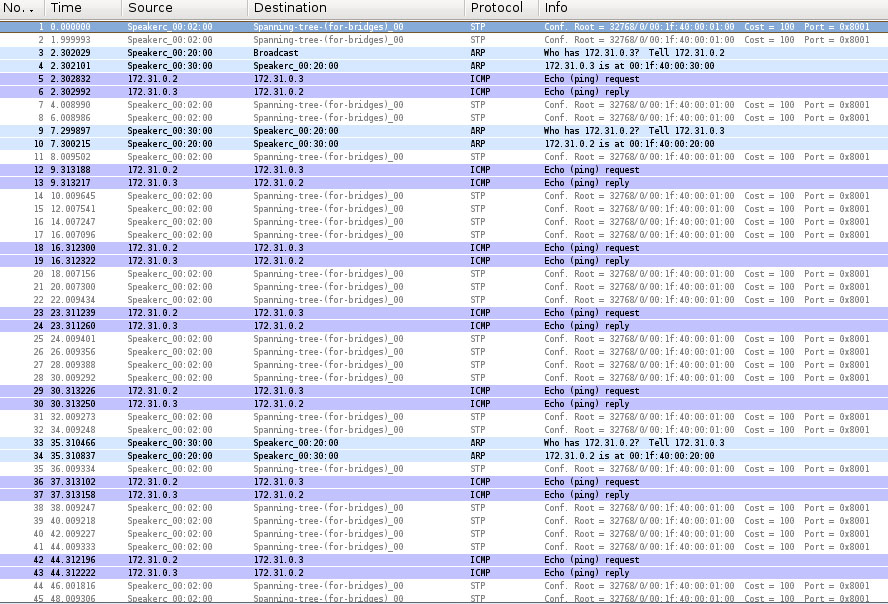
**Captura para pc1**



Se ve que cada 7 segundos se envían paquetes desde pc2 del comando ping hacia pc3 pero no se obtiene respuesta.  
  
Al cambiar el ageing time a 3 segundos la tabla se limpia en ese tiempo, mientras el  ping se realiza cada 7 segundos.  
  
Estamos capturando desde pc1 por lo que podemos ver los requests de pc2 pues al hacerlo se lo esta pidiendo al switch2, pero como switch2 ya limpio su tabla no sabe donde esta pc3 por lo que hace un broadcast a todas las maquinas (linea 2).

El response no lo ve pc1 pues cuando pc2 envío el mensaje quedo registrado en switch2, y luego pc3 envía el response a pc3 que todavía el switch no limpio la tabla por lo que solamente le llega a pc2.  
  
También vemos paquetes ARP y del Spanning Tree que ya comentamos anteriormente.

**Captura para pc3**

  
  
En este caso además de los ARP y los paquetes del spanning tree  vemos la respuesta de pc3, teniendo en cuenta que pc2 y pc3 se encuentran en el mismo domain colision ( C )