

Redes de Computadoras

REC: Reenvío, Enrutamiento y Conmutación

(*Forwarding, Routing y Switching*)

Obligatorio 3 – 2012

Facultad de Ingeniería
Instituto de Computación
Departamento de Arquitectura de Sistemas

Nota previa - IMPORTANTE

Se debe cumplir íntegramente el “Reglamento del Instituto de Computación ante Instancias de No Individualidad en los Laboratorios”, disponible en [1].

En particular está prohibido utilizar documentación de otros grupos, de otros años, de cualquier índole, o hacer público código a través de cualquier medio (foros, correo, papeles sobre la mesa, etc.).

Forma de entrega

La entrega se realizará a través de un recurso habilitado para tal fin en la plataforma EVA, que será oportunamente avisado por dicho medio. El sistema de entregas soporta múltiples entregas por grupo, llevando un histórico de las mismas. Se recomienda realizar una entrega vacía con tiempo, a los efectos de verificar que su sistema le permite entregar correctamente. Se considerará como válida la última entrega dentro del plazo asignado.

Se debe entregar un solo archivo **ob3.tar.gz** que contenga los ítems descritos en el apartado **Entregable**. Dicho archivo deberá ser generado utilizando la herramienta GNU TAR y compresión gzip. Otros formatos (bz2, rar, zip, cab, jar, etc.) no son válidos y serán rechazados.

Fecha de entrega

Los trabajos deberán ser entregados siguiendo el procedimiento descrito anteriormente antes del lunes 19 de noviembre 8:00 horas, sin excepciones. No se aceptará ningún trabajo pasada la citada fecha. En particular, no se aceptarán trabajos enviados por mail a los docentes del curso, ni entregados por cualquier otro medio.

Observaciones

Este laboratorio se realizará en una máquina virtual (VM) diferente a la que se ha utilizado en los obligatorios anteriores; la imagen iso necesaria para crear dicha VM está disponible en las computadoras de las salas linux, en el directorio `/home/redes`. Dicha imagen es una distribución de la herramienta *Netkit* (“*The poor man's system for experimenting computer networking*”) [2] basada en una versión recortada de *Knoppix 6*, que además incluye, entre otras, la herramienta *Wireshark* (*Netkit-2.7-K2.8-F5.1.iso*). Los dos archivos restantes necesarios para levantar la VM están disponibles en el EVA.

Netkit permite emular redes compuestas por diversos dispositivos de red como ejemplo computadoras, routers y switches. Los dispositivos de red son emulados como máquinas virtuales uml (*user-mode linux*) basadas en Debian, y se pueden interconectar mediante enlaces ethernet emulados. Es decir: dentro del entorno de la VM *Netkit* se levantan instancias de máquinas virtuales livianas uml que pueden representar routers, switches o sistemas finales. En [3] se puede encontrar un detalle de las prestaciones del *Netkit*.

Se recomienda estudiar la documentación de *Netkit*, comenzando por la presentación *Introduction* disponible en la *Wiki de Netkit* → *Official Labs* → *Introduction* [4].

Tanto las presentaciones como los laboratorios referenciados en el presente obligatorio se

encuentran disponibles en la Wiki de *Netkit* y copiados en el EVA.

Objetivo general del Laboratorio

Comprender los conceptos básicos de *routing*, *forwarding* y *switching* a través de la realización de laboratorios con diferentes topologías. Se debe observar, configurar, analizar y entender el comportamiento de los diferentes escenarios, y reportar resultados en la documentación.

Objetivos específicos del Laboratorio

- Comprender los conceptos básicos de *routing*, *forwarding* y *switching* así como de numeración IP, direcciones MAC, dominios de colisión y broadcast vistos en el teórico del curso.
- Entrenarse en el uso de una herramienta de emulación, en este caso, *Netkit*.
- Utilizar herramientas de captura de tráfico (para su posterior análisis), en este caso *Wireshark* y *Tcpdump*.

Se pide

1. 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 debía realizar en la configuración **r5** para que el comando `ping 193.204.161.1` ejecutado en cualquiera de los routers **r1..r4** sea exitoso. Implementelo y compruebe. Almacene los archivos del laboratorio modificado en el directorio `IRC-lab_rip`.

2. 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

- 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.

3. Laboratorio de Bridging (two-switches)

La configuración y presentación detallada de este laboratorio se encuentra disponible en la *Wiki de Netkit* → *Official Labs* → *Advanced Topics*.

- a) Instale el laboratorio de *Bridging* [9] e inicie la ejecución.
- b) Vincule el contenido del archivo `lab.conf` con la topología de red que aparece en la diapositiva 3 de la presentación [10].
- c) Utilizando el comando `ifconfig` verifique que el plan de numeración (tanto IP como MAC) es el documentado en la misma diapositiva.
- 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.
- e) Modifique las direcciones MAC de toda la red de forma que se emulen tarjetas de red fabricadas por la empresa *Speakercraft Inc*.
- f) Documente los comandos utilizados para realizar las dos partes anteriores.
- 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.pcl.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 comportamiento observado.
 - 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.
 - 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.pcl.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`.

Entregable

El archivo 'ob3.tar.gz' deberá contener lo especificado en *Documentación* y en *Configuraciones*.

Documentación

La documentación del obligatorio debe incluirse dentro del archivo de la entrega. La misma debe entregarse como un único archivo formato PDF de nombre **informeOb3grupoXX.pdf**, donde XX es el número del grupo. El mismo deberá respetar la numeración de secciones y apartados acorde a los requerimientos anteriores. En el informe debe figurar el número de grupo, nombre, apellido y número de Cédula de Identidad de cada integrante. En caso que ésto no se cumpla el obligatorio no será corregido, con la consecuente pérdida del curso para todos los integrantes del grupo. No se aceptarán otros formatos de informe [11].

Configuraciones

Un directorio por cada laboratorio con el siguiente contenido en cada caso:

- Para el laboratorio de RIP
 - `ripd.startup.rl.cap`
 - `ripd.log.rl.cap`
 - todos los archivos bajo el directorio `IRC-lab_rip`
- Para el laboratorio OSPF
 - `ospfd.startup.rl.cap`
 - todos los archivos bajo el directorio `IRC-lab_ospf`
- Para el laboratorio de BRIDGING
 - `ping.pcl.g1.cap` y `ping.pc3.g1.cap`
 - `ping.pcl.g3.cap` y `ping.pc3.g3.cap`
 - todos los archivos bajo el directorio `IRC-lab_two-switches`

La estructura de cada directorio de cada laboratorio deberá ser tal que el docente sólo deba ejecutar el comando `lstart` para correrlo, sin la necesidad de configurar nada extra.

Referencias y Bibliografía Recomendada

- [1] <http://www.fing.edu.uy/inco/pm/uploads/Ens%f1anza/NoIndividualidad.pdf>
- [2] <http://wiki.netkit.org>
- [3] <http://wiki.netkit.org/index.php/Features>
- [4] http://wiki.netkit.org/netkit-labs/netkit_introduction/netkit-introduction.pdf
- [5] http://wiki.netkit.org/netkit-labs/netkit-labs_basic-topics/netkit-lab_rip/netkit-lab_rip.tar.gz
- [6] http://wiki.netkit.org/netkit-labs/netkit-labs_basic-topics/netkit-lab_rip/netkit-lab_rip.pdf
- [7] <http://www.rfc-editor.org/rfc/rfc2453.txt>
- [8] <http://www.ietf.org/rfc/rfc2328.txt>
- [9] http://wiki.netkit.org/netkit-labs/netkit-labs_advanced-topics/netkit-labs_bridging/netkit-lab_two-switches.tar.gz
- [10] http://wiki.netkit.org/netkit-labs/netkit-labs_advanced-topics/netkit-labs_bridging/netkit-lab_two-switches.pdf
- [11] <http://www.universidad.edu.uy/renderResource/index/resourceId/4755/siteId/1>