Introducción a las Redes de Computadoras

REC: Reenvío, Enrutamiento y Conmutación

(*Forwarding, Routing y Switching*)

Obligatorio 4 – 2011

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 (news, correo, papeles sobre la mesa, etc.).

Forma de entrega

La entrega debe realizarse mediante el Moodle del curso via la *actividad* que se habilitará oportunamente. La podrán encontrar en la semana correspondiente a la entrega, con el nombre de *Entrega Laboratorio 4*. Se recomienda realizar una entrega con tiempo, a los efectos de verificar que su sistema le permite entregar correctamente. Se considerará como válida la última entrega dentro del plazo permitido. Allí podrán subir hasta tres archivos de hasta 2Mb (es el limite impuesto por los administradores del Moodle) pero con uno solo debería alcanzarles. Podrán subir y borrar archivos hasta el domingo 19 de junio a las 23:55. Por favor eviten entregas múltiples borrando los archivos que no quieran entregar.

Se debe entregar un solo archivo 'ob4.tar.gz' que contenga los ítems descritos en *Entregable* de este documento. 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, con la consecuente pérdida del curso para todos los integrantes del grupo.

Fecha de entrega

Los trabajos podrán ser entregados hasta el domingo 19 de junio a las 23:55 horas, sin excepciones. No se aceptará ningún trabajo pasada la citada fecha y hora. En particular, no se aceptarán trabajos entregados por otro medio que no sea el detallado en *Forma de entrega*.

Observaciones

Este laboratorio se realizará en una máquina virtual (VM) diferente a la que se ha utilizado en los tres 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 permite emular redes compuestas por diversos dispositivos de red como ser: computadoras, routers y switches. Los dispositivos de red son emulados como máquinas virtuales uml (*user-mode linux*) basadas en Debian. Dichas VMs se interconectan entre sí mediante un software que oficia de hub. En [3] se puede encontrar un detalle de las prestaciones del Netkit.

La imagen iso referida tambień se encuentra disponible en [4], debiéndose seleccionar, en la sección "Live CD/DVD/USB" la identificada como **Netkit live DVD/USB** (`Netkit-2.7-K2.8-F5.1.iso`) [5]. Se advierte que la misma pesa 1.1 GB.

Los dos archivos restantes para crear la VM a utilizar están disponibles en el Moodle del curso, en la misma semana que este documento y bajo el nombre *Archivos necesarios*.

Todas las ejecuciones y configuraciones para llevar adelante este laboratorio deberán ser realizadas únicamente en dicha VM. Si bien es posible contar con una interfaz gráfica para visualizar las topologías creadas, no la utilizaremos ni es necesaria para la correcta realización del mismo; por lo tanto, todo el trabajo se realizará vía línea de comandos (CLI).

Se recomienda que previo a comenzar a realizar el laboratorio se habituen a los conceptos básicos de *Netkit*. Para ello deberían recurrir a la presentación *Introduction* disponible en la *Wiki de Netkit → Official Labs → Introduction* [6].

Tanto las presentaciones como los laboratorios referenciados en el presente obligatorio y disponibles en la Wiki de *Netkit* también se encuentran disponibles en el Moodle del curso, como mecanismo de respaldo ante una posible no disponibilidad del sitio oficial.

Objetivo general del Laboratorio

Comprender los conceptos básicos de *routing*, *forwarding* y *switching* a través de la realización de laboratorios con diferentes topologías, observando, configurando, analizando, entendiendo y documentando el comportamiento de las mismas ante distintos cambios.

Objetivos específicos del Laboratorio

- Comprender desde la óptica de la realización de configuraciones en un emulador de red, 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 [7], arranque la ejecución y siga las instrucciones detalladas en [8].
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 [9] 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 [8].
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 debe realizar en **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`.

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 en línea? 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 [8] 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 [10] 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 [8].
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 *Routing* y *Forwarding* (*ospf y bgp*)

Instale el laboratorio Stub AS [11], y siga las instrucciones detalladas en [12].

a) Capture paquetes completos con `tcpdump` en la interfaz `eth0` de **as200r1** en el archivo `/hosthome/bgpd.stubas200r1.cap`, y reinicie la sesión BGP en **as20r1**. Espere 30 segundos y cierre la captura. Analice con `wireshark` y describa el contenido de los mensajes UPDATE intercambiados luego de reiniciada la sesión.

b) Transforme la red con enrutamiento OSPF y una ruta por defecto estática hacia r5 en un *Stub AS* que recibe la ruta por defecto via BGP como en [8], con las siguientes características:
   - Considere que **r1..r4** pertenecen al **AS100**, y **r5** al **AS10**. Renombre los routers **r1**..**r4** como **as100r1**..**as100r4**, y **r5** como **as10r1**.
   - Renumere el enlace **r4**-**r5** (**as100r4**-**as10r1**) con la subred 11.0.0.0/30 , que NO pertenece a AS100.
   - Configure una interfaz de **as10r1** en la subred 10.0.0.0/24.
   - Almacene los archivos del laboratorio modificado en el directorio `IRC-lab_bgp-stub-as`.

c) Inicie el demonio `zebra` en los routers del **AS100**. Inicie una captura de paquetes completos con `tcpdump` en TODAS las interfaces de **as100r4** en el archivo `/hosthome/bgpd.stubas100r4.any.cap`; una vez iniciada la captura, levante el demonio `zebra` en **as10r1**. Espere 30 segundos y cierre el archivo de captura.

d) Abra el archivo `bgpd.stubas100r4.any.cap` con `wireshark` y describa la secuencia de mensajes OSPF intercambiados.

e) Verifique que la ruta por defecto se ha propagado en todos los routers de **AS100**; compruebe la conectividad con la interfaz perteneciente a 10.0.0.0/24 de **as10r1**.

f) Conéctese al demonio `ospf` en **as100r3** con el comando `telnet localhost ospfd`. Utilizando el comando `sh ip ospf route` identifique las rutas externas de OSPF *tipo 2* (E2). Compare con el laboratorio de OSPF.

4. 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* [13] 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 [14].
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.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.
    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.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`.

Entregable

El archivo 'ob4.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 **informeOb4grupoXX.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 y, 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 [15].

Configuraciones

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

- Para el laboratorio de RIP
  - `ripd.startup.r1.cap`
  - `ripd.log.r1.cap`
  - todos los archivos bajo el directorio `IRC-lab_rip`
- Para el laboratorio OSPF
  - `ospfd.startup.r1.cap`
  - todos los archivos bajo el directorio `IRC-lab_ospf`
- Para el laboratorio BGP-OSPF
  - `bgpd.stubas200r1.cap`
  - `bgpd.stubas100r4.any.cap`
  - todos los archivos bajo el directorio `IRC-lab_bgp-stub-as`
- Para el laboratorio de BRIDGING
  - `ping.pc1.g1.cap` y `ping.pc3.g1.cap`
  - `ping.pc1.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/index.php/Download_Official
[5] http://tocai.dia.uniroma3.it/~netkit/contrib/dvd_usb_2.7-K2.8-F5.1-Knoppix6.4.4/Netkit-2.7-K2.8-F5.1.iso
[6] http://wiki.netkit.org/netkit-labs/netkit_introduction/netkit-introduction.pdf
[7] http://wiki.netkit.org/netkit-labs/netkit-labs_basic-topics/netkit-lab_rip/netkit-lab_rip.tar.gz
[8] http://wiki.netkit.org/netkit-labs/netkit-labs_basic-topics/netkit-lab_rip/netkit-lab_rip.pdf
[9] http://www.rfc-editor.org/rfc/rfc2453.txt
[10] http://www.ietf.org/rfc/rfc2328.txt
[11] http://wiki.netkit.org/netkit-labs/netkit-labs_interdomain-routing/netkit-lab_bgp-stub-as/netkit-lab_bgp-stub-as.tar.gz
[12] http://wiki.netkit.org/netkit-labs/netkit-labs_interdomain-routing/netkit-lab_bgp-stub-as/netkit-lab_bgp-stub-as.pdf
[13] http://wiki.netkit.org/netkit-labs/netkit-labs_advanced-topics/netkit-labs_bridging/netkit-lab_two-switches.tar.gz
[14] http://wiki.netkit.org/netkit-labs/netkit-labs_advanced-topics/netkit-labs_bridging/netkit-lab_two-switches.pdf
[15] http://www.universidad.edu.uy/odfpdf/