Redes de Computadoras

Obligatorio 3 – 2023

V1.5

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 el EVA.

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

Introducción

Forma de entrega

La entrega de la tarea consiste en un único archivo obligatorio3GrupoGG.tar.gz que deberá contener los siguientes archivos:

- Un documento llamado Obligatorio3GrupoGG.pdf donde se documente todo lo solicitado en la tarea. GG es el número del grupo. La documentación deberá describir claramente su solución, las decisiones tomadas, los problemas encontrados y posibles mejoras. Una clara, concisa y descriptiva documentación es clave para comprender el trabajo realizado.
- Los entregables solicitados en cada sección consistentes en los archivos de configuración (`.startup` y directorios para levantar la emulación en Kathará) que resuelven la parte del problema correspondiente así como los archivos de captura `.pcap` que considere necesarios.

La entrega se realizará en el sitio del curso, en la plataforma EVA.

Fecha de entrega

Los trabajos deberán ser entregados **antes del 12/11/2023 a las 23:30 horas**. No se aceptará ningún trabajo pasada la citada fecha y hora. En particular, no se aceptarán trabajos enviados por e-mail a los docentes del curso.

Observaciones

Este laboratorio se realizará utilizando el emulador de red **Kathará** [1] el cual permite emular redes compuestas por diversos dispositivos de red como ser: computadoras, *routers* y *switches*. Los dispositivos de red son emulados como contenedores que ejecutan dentro de una única máquina anfitriona. Dichos contenedores se interconectan entre sí mediante dominios de colisión virtuales. En [2] y [3] se puede encontrar un detalle de algunas de las prestaciones de *Kathará*.

Kathará puede ser instalado en sistemas operativos Linux, Windows o MacOS [4] y

soporta Kubernetes [5]. En este laboratorio se utilizará la máquina virtual (VM) provista [16] y en la página del curso, la cual ya contiene todos los implementos necesarios.
Todas las ejecuciones y configuraciones para llevar adelante este laboratorio deben ser realizadas en dicha VM.

Se recomienda que previo a comenzar a realizar el laboratorio se habitúen a los conceptos básicos de *Kathará*. Para ello deberían recurrir a la presentación *Introduction* disponible en su *Wiki* [6]. En [7] y [8] podrá encontrar tópicos básicos adicionales respecto a *Kathará*.

Objetivo del Trabajo

Aplicar los conceptos teóricos de la Capa de Red y Capa de Enlace: enrutamiento (*routing*), reenvío (*forwarding*) y conmutación (*switching*). Esto se logra a través de la realización de laboratorios con diferentes topologías, observando, configurando, analizando, entendiendo y documentando el comportamiento de las mismas ante distintos cambios.

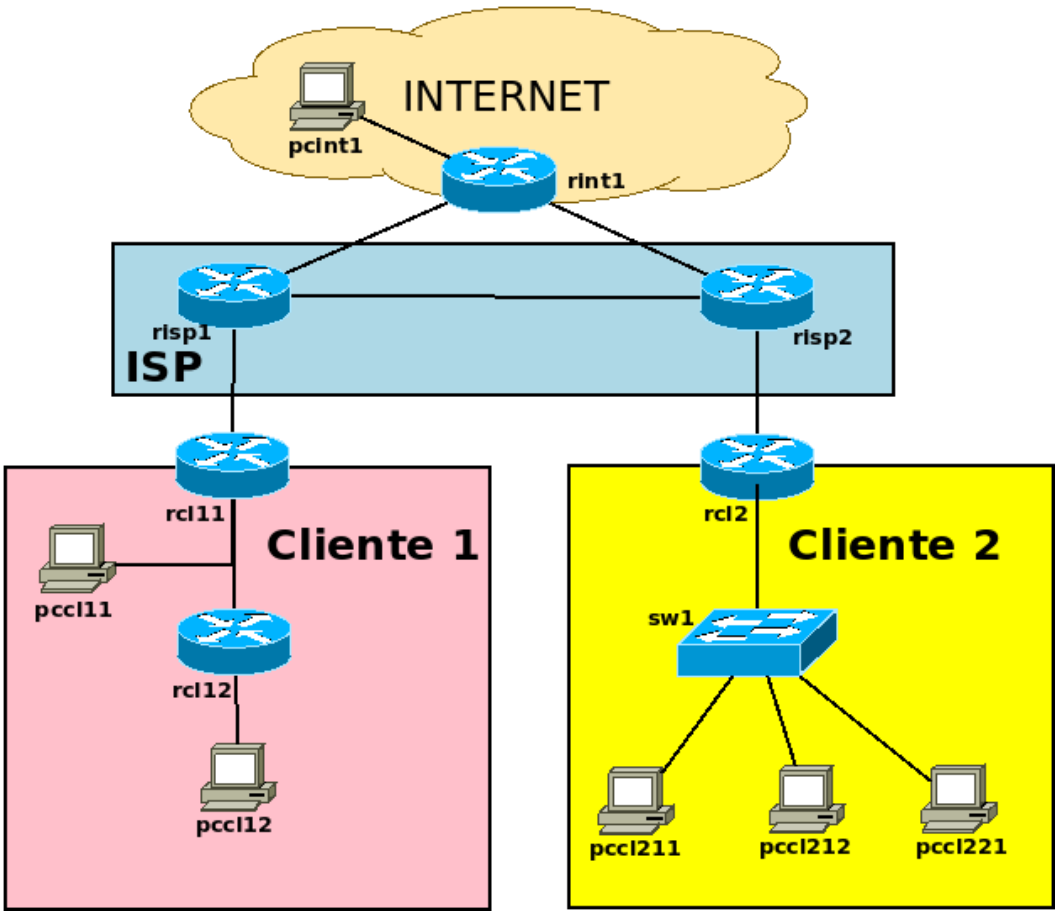
Objetivos específicos del Laboratorio

- Comprender desde la óptica de la realización de configuraciones en un emulador de red, los conceptos básicos de enrutamiento, reenvío y *switching* así como de numeración IP, direcciones MAC, dominios de colisión y *broadcast* vistos en el curso.
- Entrenarse en el uso de una herramienta de emulación, en este caso, *Kathará*.
- Utilizar herramientas de captura de tráfico (para su posterior análisis), en este caso *Wireshark* y *Tcpdump*.

Problema a resolver

Considere la Figura 1, donde se describe un proveedor de servicios de Internet (ISP), conectado a *Internet* por dos enlaces, y brinda servicio de internet a dos clientes. Asimismo se considera un *host* (pcint1) que representa un *host* cualquiera en *Internet*.

Figure 1: Topología de red



La topología presentada se encuentra en una configuración base de *Kathará* ya creada en el directorio *redes-ob3* que puede descargar del EVA del curso (en la sección de materiales). El archivo *lab.conf* contiene los enlaces mostrados en la imagen.

Es importante que para cada configuración solicitada se entienda en detalle lo realizado y las consecuencias que esto tiene en la red.

Parte 1: Numerar

Asignar direcciones IP a todos los dispositivos de la red del ISP.
El ISP dispone del prefijo 20.23.32.0/23, y sus clientes requieren:

- *Cliente 1* deberá tener disponibles una red DMZ [15] de 24 *hosts* con direcciones IP públicas y una red /24 de *hosts* con direcciones IP privadas.
- *Cliente 2* deberá disponer de dos redes de 120 *hosts* cada una, ambas con direcciones IP públicas.

Las IP asignadas a los enlaces de los *routers* del ISP deben pertenecer al espacio de redes privadas y cada enlace se le asignará una red /30.
Asimismo en *Internet* se dispone de un *host* (**pcint1**) y un *router* (**rint1**) que tienen configuradas sus interfaces con las siguientes redes: enlace con **pcint1** con la red 23.23.23.0/30, con **risp1** con la red 23.23.24.0/30 y con **risp2** con la red 23.23.25.0/30.

Entregable 1.1:

a) Identifique los dominios de colisión definidos en *lab.conf* y muéstrelos en una imagen de la topología (por ejemplo modificando la Figura 1) junto con los nombres de interfaz de cada dispositivo de red.
b) Considerando los lineamientos presentados, numerar todas las redes definidas en el ISP.
c) Considerando también los lineamientos presentados, numerar las redes de los clientes. Los enlaces **risp1-rcl11** y **risp2-rcl2** debe utilizar direcciones IP privadas.
d) Entregar un laboratorio de *Kathará* con sus respectivas carpetas y archivos con la numeración.

Esta numeración será utilizada en el resto del laboratorio por lo que es importante documentar todas las decisiones tomadas.

Parte 2: Configurar ISP

El ISP debe satisfacer los siguientes requerimientos:

- El ISP está compuesto por un *backbone* de 2 *routers* (**risp1** y **risp2**).
- Debe poder enrutar el tráfico entre todas las subredes públicas conectadas al *backbone*, y las asignadas a los clientes 1 y 2.
- El resto del tráfico se enruta a través del *router* **rint1**.
- La comunicación con *Internet* se configura a través de los *routers* **rsip1** y **risp2**, donde cada uno cuenta con un enlace que lo comunica hacia *Internet* a través del router **rint1**.

Entregable 2:

a) Configure los *routers* **risp1** y **risp2** para que ejecuten el protocolo RIP [12]. Se recomienda estudiar la documentación disponible en [10] y [11]. Debe existir conectividad total entre todos los dispositivos de la topología del ISP.
b) Capture tráfico al iniciar los "demonios" `ripd` en cada uno de los *routers* del ISP. Para esto se recomienda leer la documentación en [9]. Luego de levantados todos los demonios, espere 30 segundos y finalice la captura.
Abra el archivo con *wireshark* y analice el intercambio de mensajes RIP, los vectores intercambiados y encuentre el momento de convergencia. Documente este

análisis para uno de los routers del ISP.

c) Luego de estabilizado el protocolo:
   I. analice la tabla de *forwarding* de los *routers* (utilizando el comando `ip route`).
   II. Use la interfaz de línea de comandos (*CLI*) del demonio zebra en los *routers* (`telnet 127.0.0.1 ripd`) y ejecute `show ip rip`.
   III. Describa y explique las diferencias entre ambas informaciones.

d) Agregue las rutas estáticas necesarias en **rsip1, risp2 y rint1** para que las subredes de los clientes del ISP tengan conectividad a *Internet* (en particular, al **pcint1**).

Parte 3: Configurar Cliente 1

La configuración del Cliente 1 debe satisfacer los siguientes requerimientos:

- El enlace al ISP por medio del *rotuer* **rcl11** tendrá direccionamiento privado. El ISP le brinda el rango de direcciones IP públicas especificadas en la parte 1 y acceso a *Internet*.
- El host **pccl11** se aloja en una DMZ y tiene direccionamiento público.
- Cuenta con una LAN con direcciones privadas, donde está conectado el *host* **pccl12**. Los *hosts* en esta LAN deben poder acceder a *Internet*, a través de *Network Address Translation* (NAT).

Entregable 3.1:

a) Con los rangos de direcciones especificados en la Parte 1, realice las configuraciones necesarias en el ISP de forma de proveer acceso a la red DMZ de servidores, donde se aloja **pccl11**.

b) Realice un análisis identificando donde es necesario tener NAT configurado, así como seleccione las redes donde conviene instalar un servidor DHCP (este es un servicio que puede ser instalado en un *router*).

   Configure la red, en particular:
   - Rutas estáticas en los *routers* **rcl11** y **rcl12**.
   - Configurar NAT donde corresponda (ver Anexo 1).
   - Instalar y configurar DHCP donde convenga (ver Anexo 2).

c) Verifique experimentalmente como mínimo los siguientes puntos:
   - Comunicación entre LANs internas e Internet.
   - Comunicación entre LANs internas y red DMZ.
   - Comunicación entre red de servidores e Internet.

d) Muestre y analice mediante capturas de tráfico:
   - El funcionamiento de NAT.
   - El funcionamiento e intercambio de mensajes de DHCP.

Pregunta 3.2

Documente los dominios de *broadcast* y de colisión de las LANs del Cliente 1, y verifíquelos experimentalmente. Para esto se recomienda leer la documentación disponible en [13].

Pregunta 3.3

Suponga que se desea instalar un equipo que resuelva un servicio de *Domain Name*

System (DNS). Este equipo necesita ser configurado con una dirección IP pública. Analice fisi se requieren cambios en las configuraciones necesarios para lograr que el servicio sea accesible desde *Internet*.

Parte 4: Configurar Cliente 2

La configuración del Cliente 2 debe satisfacer los siguientes requerimientos:

- El enlace al ISP por medio del *router* **rcl2** tendrá direccionamiento privado y le brinda al cliente un rango de direcciones IP públicas especificado en Parte 1.
- Cuenta con 2 LAN virtuales (VLANs) con direccionamiento público. Para la configuración de las VLANs se recomienda revisar la sección sobre "Redes de área local virtuales (VLANs)" del libro del curso y la documentación sobre uso de switches en Kathara [13].
- Los host definidos para éste cliente son **pccl211** y **pccl212**, que pertenecen a la misma VLAN, y **pccl221**, que pertenece a otra VLAN.
- El *router* **rcl2** presenta dos enlaces hacia el *switch* **sw1** (según puede notarse en el archivo *lab.conf)*. El tráfico de cada una de las VLAN se debe transmitir por enlaces diferentes.

Entregable 4.1:

a) Configure el *switch* **sw1**, para cumplir con el funcionamiento de las VLAN propuestas.
b) Analice la conectividad con las subredes del Cliente 2, con el Cliente 1 y con *Internet*.
c) En caso de necesitar que ambas subredes del cliente no tengan comunicación entre ellas, pero tengan comunicación con *Internet*, que solución propondría.

Parte 5: Configurar BGP para el acceso a Internet

En esta parte vamos a configurar la conectividad del ISP con *Internet* utilizando el protocolo BGP en lugar de rutas estáticas. Se deben cumplir los siguientes requerimientos:

- El tráfico entrante desde *Internet con destino Cliente 1* debe usar el enlace a través de **risp1** y para el *Cliente 2* el de **rsip2**.
- En caso de caída de uno de los enlaces, el tráfico deberá enrutarse por el otro *router*.

Entregable 5.1:

a) Analice su solución considerando el tráfico entrante y saliente para ambos clientes.
b) Indique las modificaciones que deben realizarse en el RIP del ISP, para que utilice la información de BGP.
c) Implemente un plan de pruebas para el caso de caída de un enlace entrante al ISP, verificando que se cumpla el segundo requerimiento.

Control Intermedio

El control intermedio se realizará en el monitoreo de la semana del 30/10 y en él se deberá mostrar su resolución de la Parte 1 y de la Parte 2. Además deberán comentar su idea para los experimentos de la Parte 3. Por detalles, consulte con su tutor.

Anexo 1

Para configurar NAT en un sistema operativo Linux se debe usar la utilidad `iptables` [14] la cual permite configurar reglas de filtrado IP.

Se sugiere considerar la siguiente configuración:

```
iptables -t nat -A POSTROUTING -s <red interna> -o <interfaz
salida> -j SNAT --to <ip publica>
```

Anexo 2

Para instalar y configurar el servicio DHCP en la máquina de Kathará deseada, se debe primero descargar un servidor DHCP en la máquina y configurarlo adecuadamente. De forma de facilitar el trabajo y que la instalación se mantenga a pesar de cerrar Kathará, recomendamos hacer lo siguiente para obtener y ejecutar una imagen con DHCP ya instalado:

1. Permitir al usuario redes-ob3 de la VM, correr comandos docker. Para ello es necesario ejecutar lo siguiente: '*sudo usermod -aG docker redes-ob3*'.
2. Obtener la imagen con DHCP. Para esto en la máquina donde está instalado Kathará se debe ejecutar: '*sudo docker pull mrichart/kathara:latest*'. Esto descarga de un repositorio una imagen de Linux con el DHCP ya instalado.
3. Configurar la máquina de Kathará que utilizará esta nueva imagen. Para esto en el archivo `lab.conf`, se debe agregar la siguiente línea: *dev[image]="mrichart/kathara"*, donde *dev* es el nombre del router o pc que correrá el DHCP server (por ejemplo, **rcl11**).

Luego, para ejecutar DHCP en el dispositivo debe:

1. Configurar interfaces donde se ofrece DHCP en `/etc/default/isc-dhcp-server`
2. Configurar DHCP en `/etc/dhcp/dhcpd.conf`
3. Iniciar servidor DHCP: `/etc/init.d/isc-dhcp-server start`

Además de configurar el servidor DHCP es necesario configurar las máquinas que oficiarán de clientes y se configurarán automáticamente utilizando el servidor.
Para esto se recomienda:

1. Configurar interfaz donde se usa DHCP en /etc/network/interfaces:
   * `auto eth0`
   * `iface eth0 inet dhcp`

2. Reiniciar servicio de red:
   * `/etc/init.d/networking restart`

Referencias y Bibliografía Recomendada

[1] Kathará Framework - https://www.kathara.org/
[2] Kathará: A Lightweight Network Emulation System - https://www.youtube.com/watch?v=ionEpKjv3Vk
[3] Kathará Wiki - https://github.com/KatharaFramework/Kathara/wiki
[4] Guías de instalación - https://github.com/KatharaFramework/Kathara/wiki/Installation-Guides
[5] Kathará over Kubernetes - https://github.com/KatharaFramework/Kathara/wiki/Megalos-(Kathara-over-Kubernetes)
[6] Kathará Introduction - https://github.com/KatharaFramework/Kathara-Labs/blob/main/tutorials/introduction/001-kathara-introduction.pdf
[7] Kathará Lab ARP - https://github.com/KatharaFramework/Kathara-Labs/blob/main/main-labs/basic-topics/arp/005-kathara-lab_arp.pdf
[8] Kathará Lab Static Routing - https://github.com/KatharaFramework/Kathara-Labs/blob/main/main-labs/basic-topics/static-routing/004-kathara-lab_static-routing.pdf
[9] Kathará Lab Two Hosts - *https://github.com/KatharaFramework/Kathara-Labs/blob/main/main-labs/basic-topics/two-hosts/003-kathara-lab_two-hosts.pdf*
[10] Kathará Lab Quagga - https://github.com/KatharaFramework/Kathara-Labs/blob/main/main-labs/intradomain-routing/quagga/quagga-introduction/002-kathara-lab_quagga.pdf
[11] Kathará Lab RIP - https://github.com/KatharaFramework/Kathara-Labs/blob/main/main-labs/intradomain-routing/quagga/rip/007-kathara-lab_rip.pdf
[12] RFC 2453 – RIP v2 - http://www.ietf.org/rfc/rfc2453.txt
[13] netkit-lab_two-switches.pdf - *https://eva.fing.edu.uy/mod/resource/view.php?id=197887*
[14] Linux iptables - https://linux.die.net/man/8/iptables
[15] Wikipedia – DMZ - https://es.wikipedia.org/wiki/Zona_desmilitarizada_(informatica)
[16] VM para realizar el Obligatorio 3 - http://espejito.fder.edu.uy/redes/redes2023_ob3_v2.ova
[17] Ubuntu – VLAN - https://wiki.ubuntu.com/vlan