Universidad ORT Uruguay

Facultad de Ingeniería

Redes

Obligatorio

Marzo de 2022

Índice

1. Finalidad del obligatorio

El objetivo de este obligatorio es poder poner en práctica y reafirmar los conocimientos aprendidos en el curso. Para organizar el trabajo, se estructurará en las siguientes 7 partes:

1. **Aplicaciones**: Familiarizarse con algunos de los protocolos de capa de aplicación (Telnet, SMTP, POP3, HTTP, FTP, SSH).

2. **DNS**: Analizar el tráfico DNS. Distinguir entre los servidores autoritativos y no autoritativos. Comprender la secuencia de mensajes y acciones que ocurren.

3. **TCP/HTTP**: Identificar el comienzo y fin de una conexión TCP, banderas y secuencia de los segmentos intercambiados en una conexión TCP. Familiarizarse con los estados ESTABLISHED y LISTENING.

4. **Asignación de direccionamiento, configuración del router e interfaces**: Familiarizarse con el funcionamiento del ambiente de laboratorio que se utilizará. Realizar la asignación de direcciones IP de acuerdo a los requerimientos y a la topología de la práctica. Configurar las interfaces de los routers en base a la asignación realizada.

5. **Ruteo estático**: Configurar en los 3 routers rutas estáticas para que todas las subredes tengan conectividad entre sí. Comprender los parámetros y el funcionamiento de las mismas.

6. **Ruteo dinámico**: Configurar en los 3 routers ruteo dinámico para que todas las subredes tengan conectividad entre sí. Comprender cómo funciona el ruteo dinámico.

7. **Protocolo ARP**: Familiarizarse con el rol de este protocolo y su alcance.

2. Metodología y detalle de la topología

Los docentes proporcionarán un archivo .ova para que los alumnos puedan levantar en su propia PC o notebook una máquina virtual (VM) que funcionará como servidor. Para poder importar el archivo .ova, será necesario descargar e instalar la aplicación Virtual Box. Junto con el .ova se proporcionará también un video explicativo detallando los pasos a seguir para poder levantar la VM.

Luego de instalar Virtual Box, en su PC estará disponible un nuevo adaptador de red, el cual servirá únicamente para la comunicación entre la PC y la VM. Las direcciones IP para dichos efectos son:

PC: `192.168.56.1/24`
VM (servidor): `192.168.56.2/24`

Cuando en el obligatorio necesite acceder al servidor lo podrá hacer a través de esta conexión. La VM cuenta también con otra interfaz de red a través de la cual se conecta a Internet. Se realiza NAT y se utiliza la misma interfaz que la PC para conectarse a Internet.

Para la segunda mitad del obligatorio se trabajará con la aplicación GNS3. La misma es un simulador de equipamiento de redes, que permite crear topologías virtuales, acceder a las consolas de los equipos y configurar los mismos.

Utilizando la mencionada aplicación se deberá crear un "anillo" de routers, cada uno de los cuales contará además con una subred. Se deberá lograr que todas subredes se comuniquen entre sí, utilizando diferentes métodos de enrutamiento.

Deberán seguirse los pasos que aparecen en el documento, contestando las preguntas y detallando las tareas realizadas en otro documento que será el que se entregue a los docentes. Se define una **entrega intermedia** con el trabajo de las primeras 3 partes del obligatorio (aplicaciones, DNS y TCP/HTTP) a través de Aulas y una **entrega final** a través de Gestión con todo el trabajo realizado.

3. Aplicaciones

Ejecute Virtual Box e inicie la VM proporcionada para este obligatorio. Inicie Wireshark, configúrelo para capturar el tráfico entre su PC y la VM ("Virtual Box host-only network").

3.1. Telnet

Conéctese al servidor usando el protocolo Telnet, con el usuario y contraseña "ort-grupo1".

1. Escriba el comando utilizado.
2. ¿Qué tipo de tareas puede realizar en el host de destino?
3. ¿Qué es necesario para que pueda acceder desde un equipo a otro remoto por Telnet?
4. ¿Hasta qué capa deben de entenderse los nodos entre sí para que el acceso por Telnet sea exitoso?
5. Si analiza el tráfico capturado con Wireshark:

   ¿Cuál es el número de puerto de origen y de destino con los que se está accediendo?

   Identifique los paquetes Telnet de intercambio entre el cliente y el servidor. ¿Qué información contienen esos paquetes?

3.2. SMTP: Simple Mail Transport Protocol - RFC 821

1. ¿Qué comando debe ejecutar para conectarse, mediante Telnet, al puerto 25 (SMTP) del servidor?
2. Mediante el empleo del nombre asignado a su usuario (ort-grupo1) realice un diálogo SMTP a su propio usuario y al usuario ort-grupo2. Detalle cuáles fueron los comandos utilizados en cada caso.
3. Identifique: el sobre, el encabezado y el cuerpo del mensaje. ¿Cuáles son las diferencias entre el sobre y el encabezado?

3.3. POP3: Post Office Protocol version 3 - RFC 1939

1. Utilizando el protocolo Telnet, establezca una conexión al puerto estándar del protocolo. Liste el comando utilizado.

2. Establezca un diálogo POP3, ingresando con el usuario asignado a su grupo (ort-grupo1), liste sus mensajes y recupere los mismos. ¿Qué comandos utilizó?

3. Verifique la correcta recepción de los mensajes que envió a su propio usuario en la parte de SMTP. Borre el último mensaje de la casilla. ¿Mediante qué comando lo hace?

3.4. HTTP: Hypertext Transfer Protocol - RFC 1945

1. Establezca una conexión al servidor a través del puerto habitual del protocolo HTTP, utilizando la aplicación Telnet. ¿Qué comando utilizó?

2. Recupere la página de prueba usada para el laboratorio, utilizando como URL la dirección IP del servidor. Indique el comando utilizado (cuando ejecute el comando, presione dos veces la tecla "enter"). Indique también la salida obtenida.

3. Indique el lenguaje en el cual está escrita la página.

4. ¿Con qué comando traería únicamente el encabezado de la página? Indique la salida obtenida y compárela con la obtenida en el punto anterior.

5. Acceda mediante un navegador web a la página y compare los resultados obtenidos.

3.5. FTP: File Transfer Protocol - RFC 959

1. ¿Cuál es el objetivo del protocolo FTP?

2. Conéctese mediante el cliente FTP de Windows al servidor cuya IP es `192.168.56.2`. Utilice el usuario ort-grupo1. ¿Qué comando utilizó?

3. Posiciónese en el directorio **/home/publico** y liste el contenido del mismo. ¿Qué archivos se observa?

4. Copie en su PC el archivo correspondiente al cliente SSH (archivo **putty.exe**). Indique la secuencia de comandos usada, teniendo en cuenta de que se trata de un ejecutable.

5. ¿Qué secuencia de comandos utilizaría si deseara copiar a su equipo todo el contenido del directorio actual indicando que no se desea recibir confirmación para cada archivo a transferir?

3.6. SSH: Security Shell

1. Usando el cliente SSH obtenido en el ejercicio anterior, establezca una conexión con el servidor al puerto estándar del servidor SSH. Indique cuál fue la configuración empleada.

2. ¿Qué diferencias existen entre usar SSH y Telnet?

4. DNS

Previo a comenzar esta parte, se debe verificar que la VM se encuentre funcionando tal cual se explicó anteriormente. En esta sección del obligatorio se trabajará con la funcionalidad **nslookup**, que permite realizar consultas DNS a pedido del usuario. Para ello se debe, en primer lugar, ejecutar los siguientes comandos desde la línea de comandos de su PC:

C:\Users\Usuario> nslookup
Servidor predeterminado: `8.8.8.8`
Address: `8.8.8.8`

> server `192.168.56.2`
Servidor predeterminado: [`192.168.56.2`]
Address: `192.168.56.2`

Luego de esto, las consultas DNS que se realicen con esta instancia de nslookup, se ejecutarán contra el servidor instalado en la VM.

A continuación, inicie Wireshark. Para esta parte de la práctica se debe capturar el tráfico de 2 interfaces al mismo tiempo: “Virtual Box host-only network” y la interfaz que esté usando la PC para salir a Internet. La forma de

hacerlo es presionar CTRL y seleccionar ambas interfaces antes de comenzar la captura.

1. Realice una consulta DNS por un registro A usando el comando nslookup. Elija un sitio que no haya sido utilizado recientemente. Indique el sitio, el comando utilizado y la respuesta.

2. Detalle el intercambio observado en Wireshark por el servidor para resolver la consulta, poniendo énfasis en quién origina la consulta, quién responde y los posibles pasos intermedios. Puede ser necesario aplicar filtros en Wireshark para lograr reducir la cantidad de paquetes visualizados (protocolo DNS por ejemplo). Tener en cuenta que existe una gran cantidad de tráfico que se cursa habitualmente por la conexión utilizada por el PC para acceder a Internet.

3. Reinicie la captura de Wireshark (puede guardar la anterior si así lo desea). Realice la misma consulta DNS y analice nuevamente el intercambio en Wireshark. ¿El servidor contesta de caché? ¿Cómo distingue si la respuesta es de caché o no? Detalle las diferencias con el caso anterior.

4. Obtenga la dirección IP asociada al nombre `www.lab.ort.edu.uy`. Detalle el comando y la salida obtenida.

5. Obtenga todos los dominios asociados a la dirección IP `192.168.56.2`. Indique el comando y la respuesta obtenida.

6. ¿Cuál es el registro por el que se debe preguntar para conocer el servidor al cual podemos entregar correos para el dominio `lab.ort.edu.uy`? Realice la consulta y detalle los comandos utilizados.

7. ¿Cuál es el comando para encontrar los servidores autoritativos del dominio `com.uy`? Indique el comando y detalle los resultados obtenidos.

8. Realice una consulta no recursiva, usando el registro A, correspondiente a un dominio por el cual no haya consultado anteriormente. Indique el comando utilizado y la salida obtenida. ¿Puede obtener la respuesta? ¿Por qué?

9. Vuelva a realizar la consulta pero en modo recursivo. Indique el comando utilizado y la salida obtenida. ¿Puede obtener la respuesta ahora? ¿Por qué?

10. Haga una consulta correspondiente a `www.yahoo.com` y repita inmediatamente la misma consulta. Detalle las consultas y las salidas obtenidas. Compare las respuestas y explique las diferencias.

5. TCP/HTTP

Ejecute Virtual Box e inicie la VM. Inicie Wireshark. Ingrese al menú "Edit", luego a "Preferences", "Protocols", "TCP":

- Quite "Relative Secuence numbers and Windows scaling".
- Elija "Analyze TCP sequence number".

Aplique las modificaciones, sálvelas y salga del menú "Preference". Inicie la captura de tráfico, entre su PC y la VM ("Virtual Box host-only network").

5.1. Análisis de mensajes y secuencia TCP

1. Acceda mediante el navegador a la página del servidor (`http://192.168.56.2`). Luego de obtenida la página, detenga la captura.

2. Identifique el establecimiento de conexión. Describa de la misma, los números de secuencia (SEQ) inicial de ambas partes, los números de reconocimiento (ACK), el largo del segmento, como así también qué banderas van activas durante la secuencia de segmentos intercambiados.

3. Identifique la finalización de la conexión, describa la secuencia de segmentos intercambiados indicando: los números de SEQ y ACK, como así también banderas activas y largo de segmentos.

4. Identifique en el request HTTP, aquel encabezado de solicitud y su valor, que le brinda información al servidor acerca del navegador web cliente. Justifique su uso.

5. Identifique en el response HTTP, aquel encabezado de respuesta y su valor, que le brinda información al cliente acerca del servidor web.

6. Analizando la captura realizada. ¿En qué momento se incrementan los números de secuencia y en qué valor lo hacen? Identifique todos los casos posibles.

7. Analizando los números de secuencia. ¿Puede deducir cuántos bytes fueron enviados en cada sentido? Justifique su respuesta.

8. ¿Puede observar en algún momento la bandera PSH en TCP? ¿Para qué se utiliza?

9. Si una parte de la comunicación desea enviar solamente un reconocimiento y no datos. ¿Cuál número de secuencia debe enviar?

10. Capture nuevamente e intente acceder ahora a la dirección del servidor pero en el puerto 8080. (`http://192.168.56.2:8080`). ¿Logró conectarse? ¿Por qué sucede esto? ¿Qué bandera se utiliza para señalizar esto?

    Antes de continuar:

    - Utilice Google Chrome, en caso de que no lo estuviera haciendo.
    - Quite el uso del proxy, si lo tiene.
    - Borre el caché de su navegador web.
    - Implemente un filtro en Wireshark para ver solo el tráfico HTTP.

11. Descargue la página del laboratorio (`http://192.168.56.2`). Indique cuál es la fecha de última modificación de la misma y cuál es el código de la respuesta HTTP.

12. Vuelva a descargar la página e indique ahora cuál es el código de respuesta HTTP. Además, justifique el porqué de esta situación e indique cómo es el procedimiento de solicitud/respuesta HTTP con los datos de la captura.

5.2. Análisis de las conexiones

1. Ejecute el comando **netstat –na** desde una consola de Windows. Detalle brevemente la salida observada.

2. ¿Qué significan los estados "ESTABLISHED" y "LISTENING" que observa?

3. Establezca una conexión Telnet al servidor en otra consola y ejecute nuevamente **netstat –na**. Describa qué diferencia hay con la salida anterior.

5.3. Throughput de una conexión TCP

En esta sección se estudiará cómo la capacidad de transferir datos del protocolo TCP es afectada por las características del enlace utilizado.

Para ello se utilizará el programa de línea de comandos de Linux *tc*. Este programa permite degradar la comunicación entre la VM Linux (donde residen los servidores HTTP, FTP, DNS, Telnet, SSH) y el sistema operativo anfitrión Windows, de una forma conocida y controlada.

1. Se comenzará estudiando la transferencia sobre un enlace con las siguientes características:

   - Ancho de banda: 10 Mbps (Mega-bits por segundo)
   - Retardo: 50 ms (mili-segundos)

   Para obtener esto, ingrese a la VM, con el usuario y contraseña "redes", y ejecute la siguiente línea en la terminal de línea de comandos de la VM Linux:

   ```
   ./enlace1.sh
   ```

2. Descargue el archivo **archivogrande.zip** del servidor mediante HTTP, usando: `http://192.168.56.2/archivogrande.zip`

3. Inicie una nueva captura y comience a descargar el archivo. En la captura identifique el comienzo y el fin de conexión y el número de secuencia inicial y final. Indique:

   a) La cantidad de bytes enviados.

   b) El tiempo transcurrido.

   c) Con los datos anteriores, calcule el throughput en Mbps y compárelo con el configurado como límite, utilizando la aplicación *tc*.

4. Seleccione el flujo TCP relativo a la descarga. Usando la opción **Statistics/TCP Stream Graph/time-sequence graph (Stevens)** observe la evolución del número de secuencia en función del tiempo y verifique el cálculo anterior.

5. Identifique si TCP finaliza la conexión en forma simétrica o asimétrica. Justifique brevemente su respuesta.

6. Se pasará ahora a utilizar un enlace con las siguientes características:

   - Ancho de banda: 10 Mbps
   - Retardo: 50 ms
   - Tasa de pérdida de paquetes: 0.5 %

   Para obtener esto, ejecute la siguiente línea en la terminal de línea de comandos de la VM Linux[1]:

   ```
   ./enlace2.sh
   ```

   Repita ahora las pruebas de los puntos 2 y 3. ¿Qué cambios observa? ¿Por qué ocurren los mismos?

[1]Para retornar el enlace a la configuración por defecto, usted dispone de la opción ./liberar_enlace.sh

6. Asignación de direccionamiento, configuración del router e interfaces

6.1. Topología

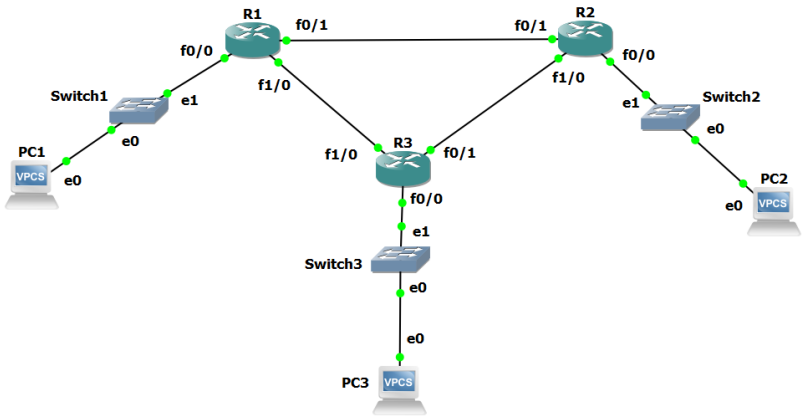

Figura 1: Topología a utilizar

6.2. Asignación de direcciones IP

Para realizar la asignación de direcciones IP se tomarán en cuenta las siguientes directivas:

- Se dispone del bloque `10.15.0.0/23`.
- Entre sí los routers se conectan con enlaces punto a punto.
- En el SW1 se deberán conectar 70 hosts.
- En el SW2 se deberán conectar 30 hosts.
- En el SW3 se deberán conectar 84 hosts.
- Los routers deberán utilizar la primera dirección del rango en las interfaces Ethernet.

1. En base a la topología y a las directivas, complete las siguientes tablas de asignación de direcciones.

Enlace	Subred (X.X.X.X/M)	IP Router	IP Router
R1 - R2			
R2 - R3			
R3 - R1			

Enlace	Subred (X.X.X.X/M)	IP Router
SW1		
SW2		
SW3		

2. En GNS3 importe el proyecto portable suministrado por el docente de Teórico, verá que la topología coincide con la Figura 1.

3. Comience la simulación y despliegue las consolas de los 3 routers.

6.3. Configuración de interfaces Ethernet

1. Basándose en la guía de comandos del Anexo, configure las interfaces hacia el switch y hacia los demás routers en cada router. Detalle los comandos utilizados.

2. Verifique el estado actual de las interfaces. Detalle los comandos utilizados y los resultados obtenidos. Si las interfaces no se encuentran operativas, detalle el porqué y las acciones que deber realizar para que queden operativas.

3. ¿Cómo vería todas las interfaces que tiene conectadas cada uno de los routers e información sobre cada una de ellas a modo de resumen? Detalle la salida obtenida.

6.4. Prueba de conectividad

1. Desde la consola de R1, pruebe la conectividad realizando ping a las 6 direcciones IP del resto de los routers. ¿Logra tener éxito en todos los casos? ¿Qué falta para que el router logre llegar a todas las direcciones IP? Detalle los comandos y el resultado obtenido.

2. Guarde la configuración de cada uno de los routers. Detalle el comando utilizado. *NOTA: Cada vez que lo considere necesario durante la práctica puede repetir esta acción para no perder los avances.*

7. Ruteo estático

En esta sección usted podrá configurar rutas de forma estática y verificar mediante línea de comando el estado de la tabla de ruteo. Una vez configurada dicha tabla, podrá probar mediante ping llegar a los distintos destinos del diagrama topológico total y evaluar los resultados.

1. Configure en cada router las rutas estáticas que le permitan llegar a todas las subredes, que hasta el momento no son alcanzables. Detalle los comandos utilizados.

2. Verifique el estado de la tabla de ruteo de los routers. Detalle los comandos utilizados y las salidas obtenidas.

3. Desde la consola de R1, pruebe la conectividad realizando ping a las 6 direcciones IP del resto de los routers. ¿Logra tener éxito en todos los casos?

8. Ruteo dinámico

8.1. Protocolo RIP

1. En esta tarea se configura el ruteo dinámico en cada router utilizando para ello el protocolo RIP. Utilice la guía de comandos del Anexo y detalle los comandos que ingresó.

2. ¿Puede ver las rutas configuradas vía RIP en la tabla de ruteo? ¿Y las rutas estáticas? ¿Por qué? Detalle el comando utilizado para visualizar las rutas y la salida obtenida en cada uno de los routers.

3. ¿Cómo haría para que se utilizaran únicamente las rutas dinámicas para encaminar los paquetes? Detalle los comandos utilizados.

4. ¿Cuál es la distancia administrativa y la métrica en cada ruta aprendida por RIP? ¿Dónde y con qué comando se puede observar esto?

5. Desde la consola de R1, pruebe la conectividad realizando ping a las 6 direcciones IP del resto de los routers. ¿Logra tener éxito en todos los casos?

6. Baje la interfaz entre R1 - R2, utilizando el comando `shutdown` dentro de la misma. ¿Qué comportamiento observa? ¿El protocolo reacciona al cambio? Describa los comandos que utilizó para responder y las salidas obtenidas. Vuelva a levantar la interfaz luego de realizado el ejercicio.

8.2. Protocolo OSPF

1. Configure OSPF en todos los routers. Asegúrese de que el protocolo quede activo en todas las interfaces. Detalle los comandos utilizados.

2. ¿Qué rutas aprendió el router? ¿Por qué visualiza estas rutas? ¿Qué ocurrió con las rutas aprendidas por RIP? ¿Por qué?

3. Desde la consola de R1, pruebe la conectividad realizando ping a las 6 direcciones IP del resto de los routers. ¿Logra tener éxito en todos los casos?

4. ¿Cuál es la distancia administrativa ahora? ¿Es la misma para todas las rutas?

5. ¿Y cuál es la métrica en cada ruta aprendida? Compare con la métrica que tenían las rutas aprendidas por RIP. ¿Hay diferencia? ¿Por qué? ¿Son comparables las métricas?

6. Pruebe cambiar ahora el parámetro `bandwidth` del enlace R1 - R2. ¿Qué ocurre con la métrica de las rutas? ¿Qué ruta siguen ahora los paquetes? ¿Por qué?

9. Protocolo ARP

1. En el escenario del punto anterior, configure en la PC1 alguna de las direcciones IP disponibles para su red de área local y el router R1 como gateway por defecto. Análogamente, configure en la PC2 alguna de las direcciones IP disponibles para su red de área local y el router R2 como gateway por defecto. Detalle los comandos utilizados en cada PC.

2. Realice una prueba de conectividad mediante ping desde la PC1 hacia su gateway por defecto, el router R1. Detalle la respuesta obtenida y el estado de la tabla ARP en el router R1.

3. Realice una prueba de conectividad mediante ping desde la PC1 hacia la PC2. Detalle la respuesta obtenida y el estado de la tabla ARP en el router R1.

4. ¿Encuentra una asociación MAC Address - IP para la PC2 en la tabla ARP del router R1? ¿Por qué?

10. Anexo

A continuación se presentan comandos que serán útiles para la realización de las tareas del obligatorio.

1. Configuración de dirección IP de las interfaces Ethernet:
   `RTR1#configure terminal`
   `RTR1(config)#interface` **nombre_interfaz** (ej: `FastEthernet 0/1`)
   `RTR1(config-if)#ip address` **dirección_IP máscara**
   `RTR1(config-if)#no shutdown`

2. Verificación del estado y parámetros de las interfaces:
   `RTR1#show interface` **nombre_interfaz**

3. Verificación de conectividad:
   `RTR1#ping` **IP_destino**

4. Verificación de conectividad forzando IP de origen:
   `RTR1#ping` **IP_destino** `source` **IP_origen**

5. Información de configuración y estado de interfaces:
   Todas las interfaces del router:
   `RTR1#show ip interface`
   Resumen de todas las interfaces del router:
   `RTR1#show ip interface brief`
   Una interfaz en particular:
   `RTR1#show ip interface` **nombre_interfaz**

6. Verificación del estado de tabla ARP:
   `RTR1#show ip arp`

7. Configuración de ancho de banda en una interfaz:
   `RTR1(config-if)#bandwidth` **velocidad** (velocidad en bps)

8. Configuración de RIP:
   `RTR1(config)#router rip`
   `RTR1(config-router)#version 2` (si fuera necesario)
   `RTR1(config-router)#network` **primera_IP_red_1**
   ⋮
   `RTR1(config-router)#network` **primera_IP_red_n**

9. Configuración de OSPF:
   `RTR1(config)#router ospf` **id_proceso**
   `RTR1(config-router)#network` **IP wildcard id_área**
   (ingresar todas las redes en las que se desea habilitar OSPF)

10. Configuración de una ruta estática:
    `RTR1(config)#ip route` **IP máscara IP_próximo_salto**
    (la IP y máscara corresponden a las de la red de destino)

11. Remoción de una ruta estática:
    `RTR1(config)#no ip route` **IP máscara IP_próximo_salto**

12. Verificación del estado de la tabla de ruteo del router:
    `RTR1#show ip route`

13. Respaldo del archivo de configuración actual en el mismo router:
    `RTR1#copy running-config startup-config`
    otra manera de hacer lo mismo:
    `RTR1#write`

14. Visualización de la configuración actual:
    `RTR1#show running-config`

15. Visualización de la configuración guardada:
    `RTR1#show startup-config`