

Redes de Computadoras

Trabajo práctico N°3

Capa de Red: Redes, subredes y superredes. DHCP y NAT. RIP y OSPF

Objetivos

Repasar y ampliar los conocimientos adquiridos en clases sobre ruteo en la capa de red, enrutadores, direcciones IP, protocolos IP e ICMP, subredes, DHCP, NAT y algoritmos de enrutamiento RIP y OSPF.

Metodología

Trabajo individual o grupal. 2 estudiantes por grupo máximo.

Tiempo de realización: 3 clases.

Aprobación

- Mostrar en clase las simulaciones que se solicitan en las actividades 1 y 4 funcionando correctamente.
- Subir a la plataforma Moodle las simulaciones que se solicitan en las actividades 1 y 4 funcionando correctamente (archivos .pkt).
- Corregir los errores en la red de la actividad 3 y subir a la plataforma Moodle la simulación funcionando correctamente (archivo .pkt).
- Responder las preguntas planteadas en el cuestionario “Trabajo Práctico N°3: Cuestionario” a través de la plataforma Moodle. Las preguntas están relacionadas con las actividades del trabajo práctico, por lo que se sugiere realizar las actividades primero.
- Escribir un breve informe y subirlo a la plataforma Moodle. El informe debe incluir:
 - Capturas de pantalla de la simulación en ejecución. Incluya una captura para la actividad 1 y una captura para la actividad 4.
 - Indicar cuales eran los errores encontrados en la actividad 3.
 - Las rutas encontradas en la actividad 5. Por cada ruta incluya algunas de las ciudades o regiones visitadas por los paquetes. No es necesario incluir todas ciudades.

Materiales necesarios

- Computadoras con acceso a Internet (providas por la facultad de Ingeniería).
- Simulador de redes Cisco Packet Tracer. El mismo puede descargarse sin costo desde Internet, como se indica en la guía del trabajo práctico N°2.
- Aplicaciones:
 - ping (disponible en línea de comandos de Linux o Windows).
 - whois (disponible en línea de comandos de Linux u online).

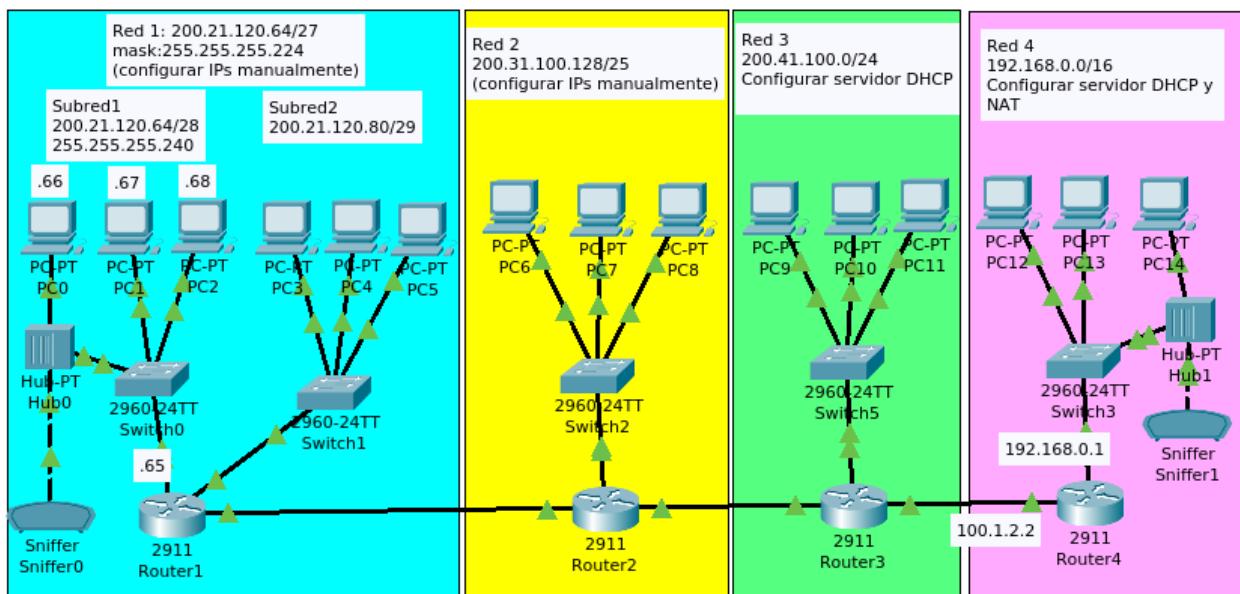
- traceroute (disponible a través de los repositorios de Linux) o tracert (instalada por defecto en Windows).

Actividad 1: Configuración de una internet. Servidores DHCP y NAT

Arme y ponga en funcionamiento la red que se muestra en la figura 1. Se sugiere utilizar los modelos de Routers y Switches que se muestran en la figura, u otros routers reales.

Sugerencias: Arme la red paso a paso. Comience con dos computadoras (las de la izquierda) y compruebe la conectividad en cada paso con el comando ping. Luego vaya paso a paso añadiendo un elemento por vez, verificando conectividad antes de seguir con el próximo elemento. Se sugiere agregar etiquetas que identifiquen a las redes (como en la figura), será mucho más fácil realizar la actividad.

Figura 1: Red de la actividad 1



La red está dividida en 4 redes del tipo sin clase:

- Red 1: 200.21.120.64/27, dividida en dos subredes, cuyas IPs deben configurarse manualmente:
 - Subred1: 200.21.120.64/28 (cuyas direcciones .65, .66, etc. y máscara de red se dan como ejemplo).
 - Subred2: 200.21.120.80/29 (cuyas direcciones y máscara de red deben ser configuradas).

- Red 2: 200.31.100.128/25, cuyas IPs deben configurarse manualmente (elija las que desee. Recuerde que la primera y la última IP del rango están reservadas y no pueden usarse).
- Red 3: 200.41.100.0/24, que debe incluir un servidor DHCP (ver en anexo 2 cómo configurar un servidor DHCP).
- Red 4: 100.1.2.0/24, que debe incluir un servidor NAT y un servidor DHCP. Note que al haber un servidor NAT, la red tiene una IP privada y una IP pública. (ver en anexo 2 cómo configurar un servidor DHCP y un servidor NAT).

Nota: La Red 4 es la más común hoy día. Probablemente tenga una como esta en su casa.

A continuación se dan una serie de sugerencias para armar la red:

Red 1: Las direcciones IP de los host de la Red 1 deben configurarse como estáticas (ver Anexo 1). Se dan como ejemplo las direcciones IP y máscaras de red de la Subred 1. Deberá asignar direcciones IP y máscaras de red adecuadas para la Subred 2.

Nota: La primera IP (host=0) identifica a la red, no puede usarse para identificar a ningún host. La siguiente IP (host=1) se asigna usualmente al router (no es obligatorio, pero por cuestiones de practicidad a la hora de trabajar con muchas IPs es recomendable hacerlo). La última IP (host=bx111....11) se usa para broadcast.

Configure las interfaces del Router1 (ver Anexo 1) que conecta con cada sub red y verifique conectividad. No necesita configurar entradas para las tablas de ruteo entre estas subredes, porque un router sabe como llegar a las redes que tiene conectadas directamente.

Verifique conectividad entre las máquinas de las dos subredes (deberían verse).

Red 2: Las direcciones IP de los host de la Red 2 deben configurarse como estáticas.

Se sugieren los siguientes pasos:

1. Agregue y conecte el Router2, el switch y las computadoras.
2. Configure las dos interfaces del Router2 (ver Anexo 1) y verifique conectividad (empleando el comando ping) con el Router1 (deberá configurar la interfaz del Router1 que conecta con el Router2). No continúe hasta que el Router2 tenga conectividad con el Router1.
3. Configure estáticamente las direcciones IP de las computadoras de la Red 2. Verifique conectividad entre las computadoras y entre las mismas y el Router2.
4. Si intenta verificar la conectividad entre una computadora de la Red 1 (por ejemplo, la PC0) y una computadora de la Red 2 (por ejemplo, la PC6), verá que no pueden comunicarse, debido a que los routers aún no tienen configuradas sus tablas de ruteo. Deberá agregar:
 - a. Una entrada a la tabla de ruteo del Router2 para que sepa como llegar a la Red 1 (ver Anexo 1).

- b. Una entrada a la tabla de ruteo del Router1 para que sepa como llegar a la Red 2 (ver Anexo 1).
5. Una vez agregadas las entradas respectivas a las tablas de ruteo de los Routers 1 y 2, verifique nuevamente la conectividad entre las computadoras de ambas redes. Deberá haber conectividad.

Red 3: Las direcciones IP de los host de la Red 3 deben configurarse dinámicamente mediante un servidor DHCP. Se sugieren los siguientes pasos:

1. Agregue y conecte el Router3, el switch y las computadoras de la Red 3.
2. Configure las dos interfaces del Router3 y verifique conectividad (empleando el comando ping) con el Router2 (deberá configurar la interfaz del router2 que conecta con el router3). No continúe hasta que el Router3 tenga conectividad con el Router2.
3. Configure las computadoras de la Red 3 de modo que las direcciones IP y la IP del gateway sean dinámicas asignadas por DHCP (ver Anexo 1).
4. Configure el servidor DHCP del Router 3, de modo que de direcciones IP a las computadoras de la Red 3 (ver Anexo 2).
5. Espere unos segundos y verifique las IP que el servidor DHCP dió a cada computadora de la Red 2 (utilice el comando ipconfig, que es el comando de Windows que muestra información sobre las interfaces).
6. Deberá agregar una entrada a las tablas de ruteo en cada router para que las redes ya configuradas sepan como llegar a la nueva red, y la nueva red sepa como llegar a las anteriores.
7. Verifique conectividad con todas las máquinas de la red.

Red 4: El Router 4 deberá implementar un servidor NAT, de modo de compartir la dirección IP pública 100.1.2.2 entre todas las computadoras que se conecten al mismo. Las direcciones IP privadas deberán estar en la red privada 192.168.0.0/16. Además, las IP privadas deberán ser asignadas por un servidor DHCP corriendo en el mismo router. Se sugieren los siguientes pasos:

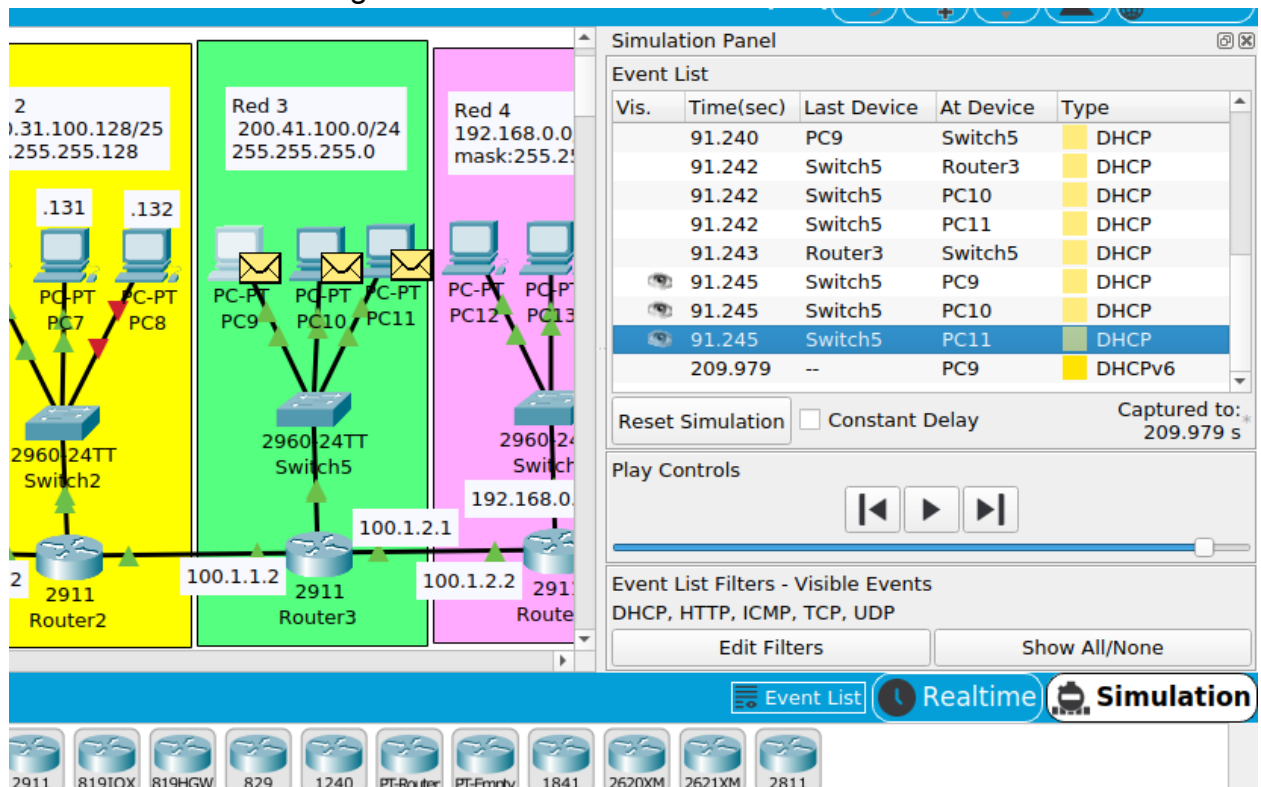
1. Agregue y conecte el Router 4, el switch y las computadoras de la Red 4.
2. Configure las dos interfaces del router. La interfaz que se conecta hacia el exterior de la red debe ser configurada con la IP pública, mientras que la interfaz que se conecta hacia el interior de la Red 4 debe poseer una IP dentro del rango de las IPs de la red privada. Luego de configurar las direcciones IPs del router, verifique conectividad (empleando el comando ping) con el router adyacente (deberá configurar también la interfaz del Router 3 que conecta con el Router 4).
3. Configure las computadoras de la red 4 de modo que las direcciones IP y la IP del gateway sean dinámicas por DHCP (ver Anexo 1).
4. Configure el servidor DHCP del Router 4, de modo que asigne direcciones IPs dentro del rango de la red privada indicada para las computadoras de la Red 4 (ver Anexo 2).

5. Espere unos segundos y verifique que la IP que el servidor DHCP asignó a cada computadora de la red 4 está dentro del rango esperado. Verifique que las computadoras de la Red 4 ven la IP pública del servidor NAT.
6. Configure el servidor NAT en el Router 4 (ver Anexo 2).
7. Agregar una entrada a las tablas de ruteo de los routers 1, 2 y 3 para que sepan como llegar a la Red 4 (**Importante: Deben saber llegar a la red que contiene la IP pública, no a la red privada**). Agregar todas las entradas necesarias a la tabla de ruteo del Router 4 para que él mismo sepa como llegar al resto de las redes. Verifique que la IP pública se ve desde cualquier computadora de la red.
8. Verifique conectividad con todas las máquinas de la red. Importante: desde cualquier computadora dentro de la red privada deben verse las computadoras de las redes públicas, pero **desde las computadoras en las redes públicas NO deben verse las computadoras de la red privada**.

Actividad 2: Análisis de paquetes

Para esta actividad utilizará la herramienta “Simulación” (o “Simulation”) de Packet Tracer, que encontrará en la esquina inferior derecha de la ventana. Al pulsar el botón “Simulation”, deberá ver una pantalla como la que se muestra en la figura 2:

Figura 2: Herramienta simulador de PacketTracer



The screenshot shows the Packet Tracer interface during a simulation. On the left, a network diagram is visible with three subnets: Red 2 (yellow), Red 3 (green), and Red 4 (pink). Red 2 contains PC7 and PC8 connected to Switch2, which is connected to Router2. Red 3 contains PC9, PC10, and PC11 connected to Switch5, which is connected to Router3. Red 4 contains PC12 and PC13 connected to Switch4, which is connected to Router4. Routers 2, 3, and 4 are interconnected. The Simulation Panel on the right shows an Event List with the following data:

Vis.	Time(sec)	Last Device	At Device	Type
	91.240	PC9	Switch5	DHCP
	91.242	Switch5	Router3	DHCP
	91.242	Switch5	PC10	DHCP
	91.242	Switch5	PC11	DHCP
	91.243	Router3	Switch5	DHCP
	91.245	Switch5	PC9	DHCP
	91.245	Switch5	PC10	DHCP
	91.245	Switch5	PC11	DHCP
	209.979	--	PC9	DHCPv6

At the bottom of the interface, there are buttons for 'Event List', 'Realtime', and 'Simulation', along with a toolbar containing various network device icons.

Antes de comenzar:

- Haga clic en “Edit Filters”, y quite todos los protocolos IPv4, IPv6 y Misc, dejando solamente marcados los protocolos ICMP, DHCP, UDP y TCP.
- Vaya a “**Options -> Preferences -> Miscellaneous**”, luego en “**Simulation - Buffer full Action**” seleccione “**Auto Clean Event List**”, y en “**Simulation - Buffer Behavior**”, seleccione “**Buffer Filtered Events Only**”. Esto es para que el simulador no guarde un registro de todos los paquetes generados, y limpie automáticamente el registro de paquetes generados (no utilizaremos dicho registro).
- Antes de cada acción, haga clic en “**Reset Simulation**” para borrar los paquetes mostrados en ese momento (para evitar confusiones).
- Para cada acción deberá hacer clic en el botón **Play** para ver el efecto.

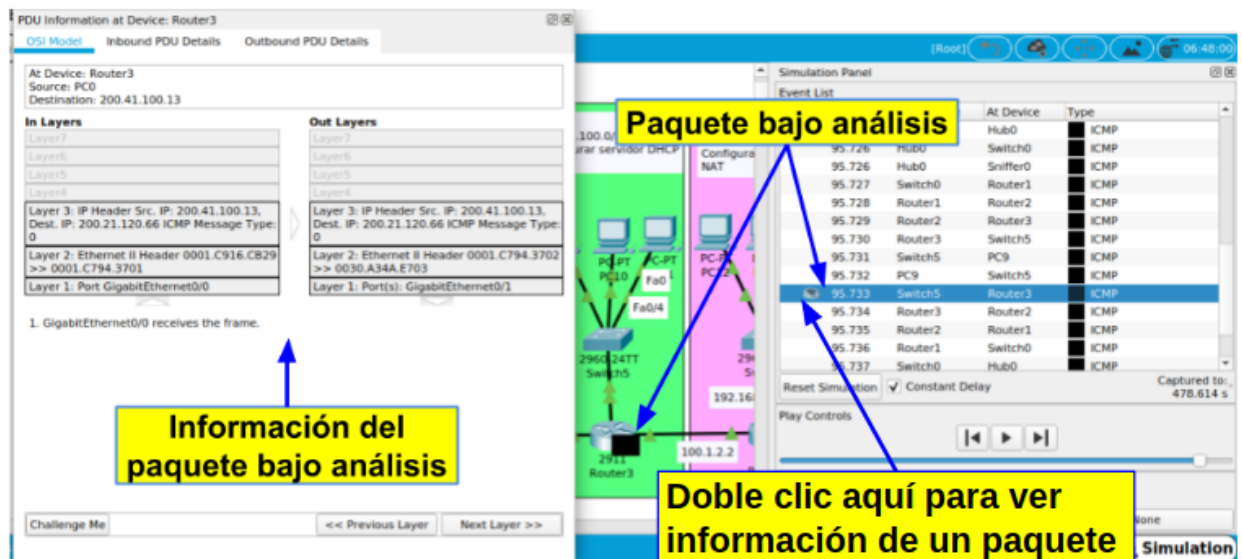
2.1 Diferencias entre paquetes IP y tramas Ethernet

Envíe un comando Ping de una PC en una red a una PC en otra red, pero que no incluya la red dentro del servidor NAT. Recuerde antes de enviar el comando, hacer clic en “Reset Simulation”, y luego de enviar el comando desde la terminal, hacer clic en Play. Espere a que termine el ciclo completo y detenga la simulación (haciendo clic en Play)

En el panel “Simulation Panel” haga clic en un paquete. En el diagrama de la red verá el paquete seleccionado, y se abrirá un nuevo panel que mostrará el contenido del paquete. Verá 2 o 3 pestañas, que son (como se muestra en la figura 3):

- OSI Model: muestra un resumen del contenido del paquete entrante y el paquete saliente del componente de red (en caso de que el componente sea el origen de un paquete, solo verá información del paquete saliente).
- Inbound PDU Details: Verá información detallada del contenido del paquete entrante.
- Outbound PDU Details: Verá información detallada del contenido del paquete saliente.

Figura 3: Paquete pasando por un componente de la red



Paquete bajo análisis

Información del paquete bajo análisis

Doble clic aquí para ver información de un paquete

At Device	Type
Hub0	ICMP
Switch0	ICMP
Sniffer0	ICMP
Router1	ICMP
Router2	ICMP
Router3	ICMP
Switch5	ICMP
PC9	ICMP
Switch5	ICMP
Router3	ICMP
Router2	ICMP
Router1	ICMP
Switch0	ICMP
Hub0	ICMP

Analice un paquete pasando por un router. Deberá contestar las siguientes preguntas a través de la plataforma Moodle:

- ¿La dirección IP origen de un paquete que entra a un router cambia al salir el paquete del router? ¿La dirección Ethernet origen de un paquete que entra a un router cambia al salir el paquete del router?

Analice un paquete pasando por un switch. Deberá contestar las siguientes preguntas a través de la plataforma Moodle:

- ¿La dirección IP de un paquete que entra a un switch cambia al salir el paquete del switch? ¿La dirección Ethernet de un paquete que entra a un switch cambia al salir el paquete del switch?

2.2 Configuración de red de cada computadora

Envíe varios comandos ping desde una computadora en una red a otra computadora en la misma red. Analice los caminos seguidos por el paquete. Conteste a través de la plataforma Moodle:

- Si un paquete se envía de una computadora en una red a otra computadora en la misma red, ¿Pasa el paquete por el router?

Envíe un comando ping desde una computadora en una red a otra computadora en otra red. Analice el camino seguido por el paquete. Conteste a través de la plataforma Moodle:

- Si un paquete se envía de una computadora en una red a otra computadora en otra red ¿Pasa el paquete por el router?

Envíe un paquete ping desde la máquina 200.21.120.66 a la máquina 200.21.120.68, analice si el paquete pasa por el router (no debería pasar por el router). Ahora cambie

la máscara de red de la computadora 200.21.120.66 por 255.255.255.252 (el valor anterior es 255.255.255.240), envíe nuevamente un ping desde la máquina 200.21.120.66 a la máquina 200.21.120.68 y verifique si pasa por el router (Si debería pasar por el router). Conteste a través de la plataforma Moodle:

- ¿Qué información indica a la computadora origen si la IP destino está en la misma red (y puede enviarle paquetes directamente) o en una red diferente (y debe enviar el paquete al router)?

Nota:

$200.21.120.66 \text{ AND } 255.255.255.240 = 200.21.120.64$

$200.21.120.68 \text{ AND } 255.255.255.240 = 200.21.120.64$

$200.21.120.66 \text{ AND } 255.255.255.252 = 200.21.120.64$

$200.21.120.68 \text{ AND } 255.255.255.252 = 200.21.120.68$

2.3 Servidor DHCP

En una computadora que sea parte de la red conectada al servidor DHCP, ejecute el comando "ipconfig /renew" (ver apéndice 2). Una vez que el servidor DHCP responde (verá la respuesta en la consola de comandos) analice el paquete inicial de la petición DHCP (DHCP request) y la secuencia de paquetes generados (podrá verlos utilizando la opción Simulador). Conteste a través de la plataforma Moodle:

- ¿Cuales son las direcciones IP y MAC origen y destino del paquete DHCP request?.

2.4 Paquetes desde una computadora NAT

Envíe un comando ping desde una computadora dentro de la red detrás detrás del servidor NAT hacia una computadora fuera de la red. Analice el paquete cuando se encuentra sobre el router que contiene el servidor NAT. Conteste a través de la plataforma Moodle:

- Al pasar un paquete por un servidor NAT: ¿Cambia la dirección Ethernet?, ¿Cambia la dirección IP?

Actividad 3: Descubriendo errores de redes

Descargue el archivo "Actividad3_red_con_errores.pkt" del aula virtual. El mismo es una simulación de una red. Todas las computadoras de la misma deben poder comunicarse con el servidor. Pero 4 de esas computadoras (PC1, PC2, PC3 y PC7) poseen errores que no permiten la comunicación.

Nota: En la red no hay ningún servidor de DHCP ni de NAT. Los router funcionan todos correctamente.

Detecte los errores. Indique el error respondiendo las preguntas respectivas en el cuestionario de Moodle.

Corrija los errores (debe mostrar y subir a través de la plataforma Moodle el archivo .ptk con la simulación funcionando sin errores).

Actividad 4: RIP y OSPF

Introducción

Descargue del aula virtual las redes denominadas actividad4_RIP.pkt y actividad4_OSPF.pkt. Ambos archivos contienen la simulación de la misma internet, pero configurada con diferentes protocolos de enrutamiento. En el primero, los routers han sido configurados mediante el algoritmo de enrutamiento RIP, y el segundo mediante el algoritmo de enrutamiento OSPF.

Ambas simulaciones poseen 10 routers conectados mediante enlaces de diferentes velocidades. Los enlaces de la fila superior son de 10 Mbps, los enlaces de la fila central son de 100 Mbps, y los enlaces de la fila inferior son de 1000 Mbps.

En ambas simulaciones, hay dos redes no conectadas a la internet: 201.38.14.0/26 y 202.39.44.0/26. Ambas redes poseen solo una computadora, pero podrían tener más.

Realizar las siguientes actividades sobre la red actividad4_RIP.pkt y sobre la red actividad4_OSPF.pkt. Se sugiere comenzar por la primera (es más simple).

4.1. Conecte la red 201.38.14.0/26 al router 0 y la red 202.39.44.0/26 al router 2. Deberá seleccionar y configurar adecuadamente la interfaz a utilizar en el router y configurar las interfaces de las PC. Configure las interfaces como 100Mbps full-duplex. (Sugerencia: antes de continuar, verifique el correcto funcionamiento del enlace entre las computadoras y los routers a través de los cuales se unen a la internet).

4.2. Configurar los enrutadores 0 y 2 para que anuncien a la internet las nuevas redes que se agregaron en 4.1, empleando el protocolo RIP en la red mostrada en el archivo actividad4_RIP.pkt y el protocolo OSPF en la red mostrada en el archivo actividad4_OSPF.pkt.

Para configurar RIP, deberá, como mínimo (ver Anexo 3 para conocer los comandos necesarios):

- Entrar a la configuración del protocolo RIP.
- Indicar las nuevas redes a anunciar.
- Elegir la versión correcta de RIP (utilice versión 2).

Para configurar OSPF, deberá, como mínimo:

- Entrar a la configuración del protocolo OSPF.
- Indicar las nuevas redes a anunciar (utilice una sola área, el área 1) e interfaces sobre las cuales trabajará OSPF.
- Configure los tiempos entre mensajes Hello y el tiempo a esperar para eliminar una ruta si no se reporta (sugerencia, utilice 3 y 60 segundos respectivamente).

Espere un minuto (aproximadamente) y verifique si puede ver las nuevas redes desde cualquier router de la red (en el Anexo 3 se indican los comandos para ver las rutas aprendidas tanto por RIP como por OSPF).

No olvide guardar las configuraciones realizadas en los enrutadores (ver Anexo 1 para conocer comandos para guardar información en los routers).

4.3. Para cada simulación, verifique el camino que siguen los paquetes para llegar desde las PC0 a la PC1. Puede utilizar la herramienta simulación de Packet Tracer (figura 2) eliminando todos los filtros, dejando solo ICMP.

4.4. Para cada simulación, apague uno de los routers que forma parte de la ruta por donde pasan los paquetes (no apague los routers a los cuales están conectadas las PCs). Espere unos 30 segundos. Verifique cual es el nuevo camino por el cual pasan los paquetes.

A continuación, apague uno de los routers que forma parte de la nueva ruta por donde pasan los paquetes (no apague los routers a los cuales están conectadas las PCs). Espere unos 30 segundos. Verifique cual es el nuevo camino por el cual pasan los paquetes (debería quedar un único camino posible).

Encienda los routers apagados y verifique las nuevas rutas (Deberá esperar a que los routers se activen).

Responda a través de Moodle: Para los protocolos RIP y OSPF, responda: ¿En que se basan estos protocolos para decidir una ruta?.

Actividad 5: Enrutamiento de paquetes en Internet

Para esta actividad, utilice una computadora con conexión a Internet.

Indique los países y ciudades por los que pasan los paquetes para llegar a los destinos indicados abajo, indicando las IPs de un router de cada ciudad (no es necesario indicar todos).

4.1 Aplicación traceroute

Para esta actividad puede utilizar la herramienta traceroute (puede descargarse de los repositorios de Linux. En Windows se llama tracert y suele estar instalada por defecto). Traceroute devolverá una lista de IPs de los routers por los cuales pasan los paquetes.

Algunas opciones útiles de traceroute:

--icmp: utilizar sondas ICMP (ping).

--tcp: utilizar sondas TCP. Útil si las sondas ICMP no llegan a destino.

--udp: utilizar sondas UDP. Útil si las sondas ICMP no llegan a destino.

-m: número máximo de saltos.

4.2 Ubicación geográfica de las IP mediante whois

Luego, para cada IP, puede consultar la ubicación del router, su propietario y otra información con la aplicación **whois** (del inglés who is? o ¿quién es?). El mismo se encuentra integrado en todas las distribuciones actuales de Linux o en muchas páginas web (por ejemplo). Puede accederlo a través de una terminal, por ejemplo:

whois 8.8.8.8

Dicho comando brindará gran cantidad de información, entre la cual se puede encontrarse el dueño de la dirección IP y su información. La información brindada por whois no está estandarizada, por lo que cada consulta puede brindar diferente información. Para conocer el dueño o dueños del router, busque campos tales como **OrgName**, **org-name**, **owner** o **descr**. Para conocer la ubicación del router, puede buscar campos como **address**, **city**, **country**.

4.3 Páginas web para obtener la ubicación geográfica de las IP

Varias páginas web brindan información obtenida con el servicio whois de manera gráfica, incluyendo mapas, como <https://iplocation.com/> (esta última es probablemente más simple de utilizar que whois, aunque brinda menos información)

Un ejemplo de la lista que deberá obtener es:

Ruta para alcanzar la IP 193.137.200.184 (Universidad de Coimbra, Portugal)

salto 3: 200.51.241.1 - Buenos Aires

salto 4: 81.173.106.61 - Madrid

salto 10: 154.54.47.229 - Wichita (Estados Unidos)

salto 14: 66.28.4.198 - Washington (Estados Unidos)

Salto 15: 154.54.58.233 - Wichita (Estados Unidos)

Salto 16: 130.117.0.2 - Schweiz (Suiza)

Salto 17: 149.29.9.10 - Wichita (Estados Unidos)

Salto 21: 62.40.98.106 - Lisboa (Portugal)

Salto 22: 83.97.88.210 - Londres

Salto 23: 194.210.6.202 - Portugal

Salto 27: 193.137.200.184 - Portugal, Universidad de Coimbra (Destino final)

No es necesario indicar todos los saltos. Por ejemplo, los saltos 1 y 2 no se incluyen por ser saltos en routers privados.

Los saltos 5, 6, 7 y 8 no se incluyen por estar todos en Madrid. Los saltos 9, 18, 19 y 20 no se incluyen porque dichos routers no responden (pueden tener desactivadas la posibilidad de responder consultas como las de whois). Los saltos 24, 25 y 26 no se incluyen por estar todos dentro de Portugal.

Los destinos cuya ruta se pide buscar son:

a) www.google.com

b) 175.45.176.73 (o 175.45.176.76 si la primera no funciona)

c) 101.251.6.246

d) 127.0.0.1

Nota 1: En Linux se sugiere utilizar la búsqueda mediante mensajes ICMP con un máximo de 60 saltos. Si la búsqueda no llega a destino, se sugiere utilizar mensajes TCP. En Windows no puede seleccionarse el mecanismo de búsqueda.

Nota 2: La búsqueda podría finalizar con indicadores como:

- !X o !Z: Indican que algún router no permite mensajes ICMP. Probablemente porque el acceso a dicha red está bloqueado. En ese caso indique donde se bloquea el paquete y que destino debería alcanzar (con whois IP).
- !N: Red inalcanzable.

Anexo 1: Configuración básica de computadoras y routers

Configuración básica de una computadora en Cisco Packettracer:

Hacer click sobre la computadora (o laptop). En la pantalla configuración (o config) debe configurar, como mínimo, la dirección IPv4, la máscara de red y el Gateway:

- Para la interfaz que utilizará (por ejemplo, FastEthernet0) debe configurar la dirección IPv4 y la máscara de red.
 - Para configurar una dirección IP estática, seleccione “static” e ingrese una dirección IP y una máscara de red.
 - Para configuración de IP dinámica, debe seleccionar DHCP y no escribir ninguna dirección (la asignará el servidor DHCP).
- En Global/settings, debe configurar el Gateway (router por defecto al cual se envía el paquete IP cuando el destino no pertenece a la red local).
 - Si configura una dirección IP estática, deberá proveer una dirección IP de gateway.
 - Si configura una dirección IP dinámica, debe seleccionar DHCP para el gateway y no escribir ninguna dirección IP.

Configuración básica de un Router Cisco mediante interfaz gráfica:

Podrá configurar a través de la interfaz gráfica (pestaña config) o a través de consola de comandos (pestaña CLI) las siguientes características de los routers:

- Direcciones IP de sus interfaces.
- Agregar o borrar entradas de las tablas de ruteo estáticas.
- Configurar el algoritmo de ruteo RIP.

Para ello, utilice la pestaña config. Luego de cada cambio realizado, debe ir a la consola de comandos (pestaña CLI) y ejecutar “no shutdown”, para que los cambios realizados tengan efecto sin necesidad de reiniciar el router.

No podrá configurar a través de la interfaz gráfica las siguientes características:

- Servidores DHCP y NAT.
- Algoritmo de ruteo OSPF.

Para estas características, deberá emplear la consola de comandos.

Configuración básica de un Router Cisco mediante consola de comandos:

Para configurar un router mediante consola de comandos, debe emplear la pestaña CLI. El router puede estar en cuatro estados:

- Modo normal
- Modo administrador
- Modo configuración
- Configurando una funcionalidad específica.

Se accede secuencialmente a cada uno de ellos en el orden mencionado (se pasa de modo normal a administrador, de administrador a configuración, y de configuración a configurando una funcionalidad específica).

- Modo normal: verá el símbolo **Router>**. Permite ejecutar comandos como ping.
- Modo administrador: verá el símbolo **Router#**. Permite ver tablas de ruteo y configuración de interfaces.
- Modo configuración: verá el símbolo **Router(config)#**. Permite configurar parámetros como rutas, un servidor DHCP, etc.
- Configurando una funcionalidad específica: verá diferentes símbolos según la funcionalidad que esté configurando. Por ejemplo, si está configurando una interfaz, verá el símbolo **Router(config-if)#**, si está configurando un servidor DHCP, verá el símbolo **Router(dhcp-config)#**, si está configurando un protocolo de enrutamiento, verá **Router(config-router)#**.

Para cada comando que se menciona abajo, el router debe estar en el estado correspondiente (el mismo se indicará en cada caso).

Comandos para pasar de un estado a otro:

- **Router> enable**: Pasa de modo normal a modo administrador.
- **Router# config**: Para de modo administrador a modo configuración.
- (cualquier estado) **exit**: Sale de los modos de configuración (pasa de modo “Configurando una funcionalidad específica” a “modo configuración”, de “modo configuración” a “modo administrador”, o de “modo administrador” a “modo normal”).

Los siguientes comandos configuran una interfaz, por ejemplo, la GigabitEthernet0/0 (por cada router deberá configurar al menos dos interfaces):

- **Router(config)# interface GigabitEthernet 0/0** (Selecciona la interfaz a configurar).
- **Router(config-if)# ip address 10.10.10.1 255.255.255.0** (Configura la IP y la máscara de red de la interfaz)
- **Router(config-if)# no shutdown**: Activa los cambios sin reiniciar el equipo.

Los siguientes comandos muestran información de las tablas de ruteo:

- **Router# show ip route** (muestra el contenido de las tablas de ruteo).
- **Router# show ip interface brief** (muestra la configuración dada a las interfaces del router).

El siguiente comando añade manualmente una entrada a las tablas de ruteo del router (si se agrega “no” adelante, borra la ruta):

```
Router(config)# ip route ip_destino_final mask_destino_final ip_proximo_salto
```

Router(config)#end (luego de configurar todas las rutas)

Donde:

ip_destino_final: es la dirección de red de destino final (la red que se desea alcanzar).

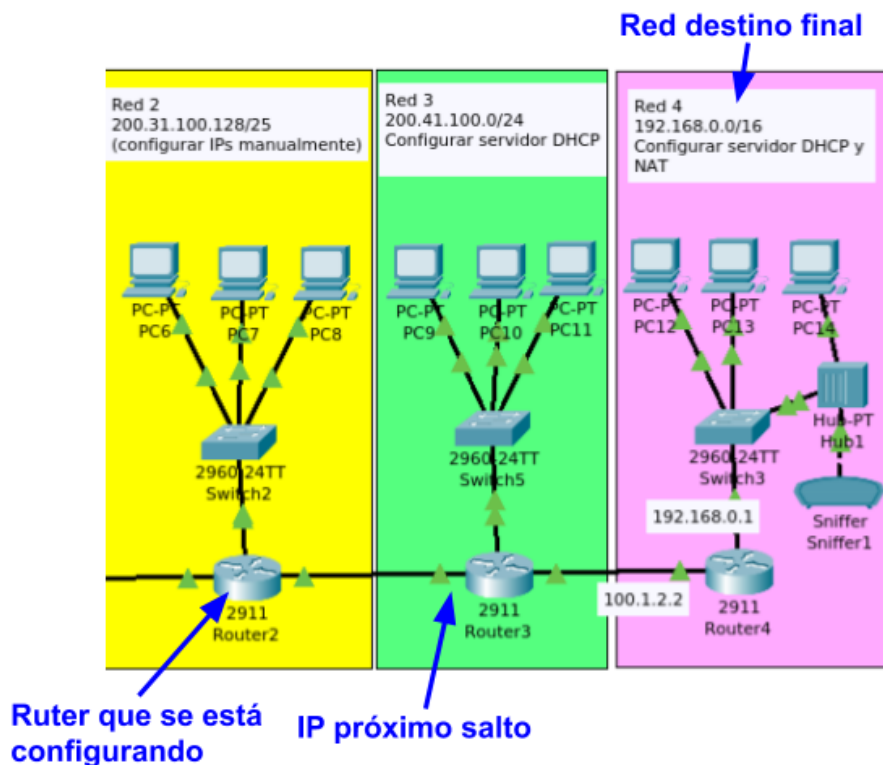
mask_destino_final: es la máscara de red de la red de destino final.

Ip_proximo_salto: es la dirección IP de la interfaz del próximo salto.

Como se muestra en la figura .

Configurar una entrada de la tabla de ruteo

Figura 4: Configuración de una ruta



Router#copy running-config startup-config (almacena la información en la memoria no volátil del router).

Anexo 2: Configuración de servidores DHCP y NAT

Configuración de un servidor DHCP en un router:

Se sugiere leer primero la sección “Configuración básica de un Router Cisco mediante consola de comandos” del Anexo 1.

Para configurar un servidor DHCP, ejecute los siguientes comandos:

Router(config)# ip dhcp excluded-address IP1 IP2 (Excluye el rango comprendido entre IP1 e IP2 del pool de direcciones a asignar dinámicamente por el DHCP).

Router(config)# ip dhcp pool RED_1 (Asigna un nombre al rango de direcciones IP que serán asignadas dinámicamente. Ejemplo: RED_1. Puede ser cualquier otro nombre)

Router(dhcp-config)# network IP_red Mascada_red (define una red o conjunto de direcciones IP desde el cual se extraerán direcciones IP para asignarlas dinámicamente mediante DHCP. Esta configuración debe coincidir con la configuración de la interfaz a emplear).

Router(dhcp-config)# default-router IP_Gateway (gateway por defecto. El DHCP informará la IP del gateway a las computadoras que envíen peticiones DHCP. También es la interfaz en la cual se escucharán peticiones DHCP).

Router# show ip dhcp pool: Muestra las asignaciones de DHCP realizadas.

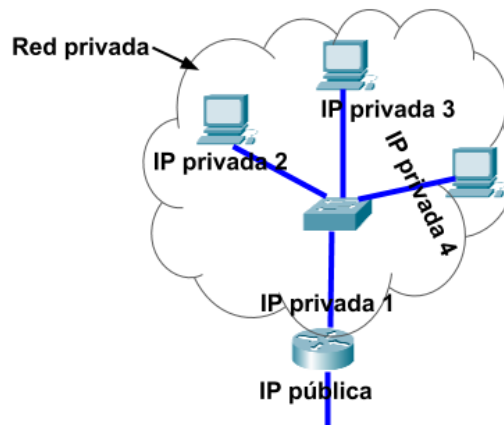
Comandos útiles en una PC para obtener o liberar direcciones IP desde un servidor de DHCP:

ipconfig /release: Libera una dirección IP. La PC queda sin dirección IP, y el servidor DHCP la puede asignar a otra computadora.

ipconfig /renew: Solicita una nueva dirección IP al servidor DHCP.

Configuración de un servidor NAT en un router:

La siguiente figura muestra como debe ser configurado un router para ser utilizado como servidor NAT. El router debe poseer al menos dos interfaces, una se configurará como IP pública, y la otra será parte de la red privada.



Los siguientes comandos configuran una interfaz del router como “interna” o entrada NAT (su IP debe ser una de las IP privadas)

```
Router(config)# interface GigabitEthernet0/0  
Router(config-if)# ip nat inside
```

Los siguientes comandos configuran una interfaz del router como “externa” o salida NAT (IP pública)

```
Router(config)# interface GigabitEthernet1/0  
Router(config-if)# ip nat outside
```

Las siguientes tres instrucciones configuran el servidor NAT. La siguiente instrucción configura una lista de direcciones que será referida como un número (en el ejemplo 100) para ser utilizadas por el servidor NAT:

```
Router(config)# access-list 100 remark == [Control NAT Service]==
```

La siguiente instrucción indica cuáles serán las direcciones que pueden utilizarse como IP privadas para NAT (note que se utiliza una notación similar a una máscara de red, pero a la inversa).

```
Router(config)# access-list 100 permit ip 192.168.0.0 0.0.255.255 any
```

La tercera y última instrucción indica que las direcciones incluidas en el listado 100 utilizarán la misma interfaz de salida (que debe tener asignada la IP pública):

```
Router(config)# ip nat inside source list 100 interface fastethernet1/0 overload
```

Comandos para verificar funcionamiento de NAT:

```
Router# show ip nat statistics
```

```
Router# show ip nat translation
```

```
Router# show access-lists
```

```
Router# show running-config
```

Para borrar cualquiera de las configuraciones anteriores, ejecutar la misma instrucción con “no” adelante. Ejemplo:

```
Router(config)# no access-list 100 remark == [Control NAT Service]==  
Router(config)# no access-list 100 permit ip 192.168.0.0 0.0.0.255 any  
Router(config)# no ip nat inside source list 100 interface fastethernet1/0 overload
```

Anexo 3: Configuración Protocolos RIP y OSPF

Configuración de RIP en un router mediante consola de comandos (también puede configurarse mediante interfaz gráfica):

Router(config)# router rip (entra a la configuración de RIP. Si RIP no está activado, lo activa)

Router# no router rip (desactiva RIP)

Router(config-router)# network 172.27.0.0 (Indica al router que debe anunciar la red 172.27.0.0 al resto de la internet)

Router(config-router)# no network 172.27.0.0 (Indica al router que no debe anunciar la red 172.27.0.0 al resto de la internet)

Router(config-router)# version 2 (Indica la versión de RIP a emplear, puede ser 1 o 2)

Router#show ip route rip (muestra rutas aprendidas con RIP. La información se muestra con el siguiente formato: "*destino_final [costo_administrativo/costo_ruta] via proximo_salto*").

Router#show ip rip database (muestra información sobre la configuración realizada).

Configuración básica de OSPF en un router mediante consola de comandos (solo puede configurarse mediante consola de comandos):

Router(config)#router ospf 1 (activa OSPF en un enrutador, indicando un número de proceso. Puede haber distintas instancias de OSPF corriendo en un router).

Router(config-router)#network 192.168.0.0 0.0.0.255 area 1 (Indica que la red 192.168.0.0 cuya máscara de red es 255.255.255.0 debe anunciarse al resto de la internet, indicando que estará en el área 1. Tenga en cuenta que la máscara de red se indica en forma inversa. La red debe estar conectada a una de las interfaces del router).

Router(config-router)#auto-cost reference-bandwidth 1000 (configura el valor por defecto del ancho de banda por referencia en Mbps. Este valor se utiliza para calcular el "costo" de cada enlace, como $\text{costo} = (\text{ancho de banda}) / (\text{ancho de banda por referencia})$)

Router(config-if)#ip ospf hello-interval 3 (indica a la interfaz previamente seleccionada mediante el comando "interface *interfaz*" que debe enviar mensajes hello cada 3 segundos anunciando la nueva red. Si los routers adyacentes no reciben estos mensajes hello, considerarán al router fuera de servicio)

Router(config-if)#ip ospf dead-interval 60 (indica a la interfaz previamente seleccionada mediante el comando "interface *interfaz*" que debe esperar hasta 60 segundos un mensaje hello de un router adyacente antes de considerar una red fuera de servicio).

Nota: Se sugiere no modificar los intervalos de tiempo de las interfaces que ya están conectadas.

Otros comandos útiles OSPF:

Router(config-if)# bandwidth 1000000 (configura el ancho de banda de la interfaz en kbps. Importante en OSPF, porque elige las rutas en función del ancho de banda de las mismas).

Router(config-if)# ip ospf cost 100 (asigna un valor de costo de ruteo a través de la interface, sobrescribiendo el valor que el router calcula por defecto. Si se agrega “no” adelante, borra la configuración previa y lo calcula por defecto desde el ancho de banda).

Router#show ip ospf interface (muestra información detallada de la configuración de OSPF para cada interfaz)

Router#show ip route ospf (muestra rutas aprendidas con OSPF. La información se muestra con el siguiente formato: *destino_final [costo_administrativo/costo_ruta] via proximo_salto*).

Router#show ip ospf (muestra información básica sobre OSPF).

Anexo 4: Método alternativo a traceroute

Este método alternativo a traceroute es el principio de funcionamiento del mismo. Para conocer las direcciones IPs de los routers por las que pasa un paquete para llegar a un destino final, puede utilizar el comando **ping -t X 8.8.8.8** (**ping -i X 8.8.8.8** en Windows), donde **X** es el tiempo de vida inicial del paquete. Cada router decrementa ese valor, hasta que llegue a 0. El router en el cual el tiempo de vida llega a 0, descarta el paquete, y envía un paquete ICMP indicando “**Time to live exceeded**” y la dirección IP del router que descarta el paquete. Al conocer las IP de los routers que descartan los paquetes, puede trazarse la ruta que seguirá el paquete cuando no se imponga un tiempo de vida. Repitiendo este procedimiento, incrementando **X** desde 1 en adelante hasta alcanzar el destino final, podrá saber las IPs de todos los routers por los que pasa el paquete hasta llegar al destino final.