UNIVERSIDAD DE TARAPACÁ

FACULTAD UNIVERSITARIA DE INGENIERÍA

Departamento de Ingeniería en Computación e Informática

Laboratorio 2: “Router estático”

Autor: Mino Brugos
Iván Cardemil
Gonzalo Vega
Curso: Laboratorio de redes
Profesor: Diego Aracena

Arica, 5 de octubre de 2019.

Tabla de contenidos

1. Introducción

Con el objetivo de poner en práctica nuestro conocimiento adquirido en el área de la comunicación de datos y redes es necesario experimentar el uso de dispositivos intermedios en ambientes reales, como lo puede ser una red doméstica. Pero antes de cometer la acción descrita, es de importancia estudiar cuales son los métodos y mecanismos utilizados para conectar dispositivos que se encuentren en distintas redes. Con el objetivo de comprender lo anterior, la experiencia del laboratorio fue divida en dos partes, donde la primera se puso énfasis en el ruteo estático y en los servicios que provee el mecanismo de IP Forward. Mientras que la segunda experiencia consistió en la asignación de direcciones IPv4 a dispositivos finales.

A diferencia del anterior laboratorio, el único requisito que deberá cumplir el dispositivo intermedio que hará de Router, es el de poseer un sistema operativo en específico y por lo menos dos interfaces ethernet. El equipo deberá realizar las configuraciones solicitadas en el laboratorio y utilizar diversas herramientas para comprobar el correcto flujo de datos entre las diferentes redes, y además, la obtención de mediciones que serán de ayuda a la hora de sacar conclusiones de las experiencias realizadas.

2. Objetivos

2.1 Propósito del documento

El siguiente documento busca exponer de forma clara y ordenada el resultado de la investigación realizada sobre la construcción de redes domésticas, y a partir de eso, describir de forma detallada las conclusiones obtenidas a partir de la experiencia de laboratorio.

2.2 Objetivo general

Investigar sobre el envío de paquetes entre distintas redes y la asignación dinámica de direcciones lógicas utilizando los dispositivos intermedios disponibles en el laboratorio, para entender de mejor forma su funcionamiento.

2.3 Objetivos específicos

- Estudiar los aspectos teóricos del envío de paquetes entre redes distintas.
- Diseñar la topología de la red a armar.
- Armar y configurar la red con los dispositivos del laboratorio.
- Asociar los resultados obtenidos con el contenido teórico.

3. Desarrollo

3.1 Marco teórico

3.1.1. ¿Qué es el enrutamiento?

Enrutamiento se refiere al proceso en el que los Router logran obtener y almacenar información sobre redes remotas, donde encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas. En otras palabras, los routers deciden después de examinar la dirección IP de destino dónde enviar los paquetes, para que este llegue a su red de destino, o simplemente descartan los paquetes si es que, por algún motivo, fallan todos los intentos de direccionarlo. Sin embargo, al principio un Router no conoce ninguna otra red que no sea la que está directamente conectada al enrutador mismo. Para que un Router pueda llevar a cabo el enrutamiento, primero debe saber de la existencia de redes remotas, por lo que el router tiene que estar configurado con enrutamiento dinámico y/o enrutamiento estático.

3.1.2 Tipos de enrutamiento

Como se mencionó en el punto anterior, existen dos tipos de configuración para el enrutamiento, que serán descritas a continuación.

3.1.2.1 Enrutamiento Estático

Con el enrutamiento estático el Router es configurado manualmente por el administrador de redes, por lo que es él, de acuerdo a las necesidades de la organización, quien decide cómo es que se comunica hacia las redes remotas. Algunas de las ventajas del enrutamiento estático son:

- **Control sobre la selección de la ruta:** Una ruta estática le indica al Router, exactamente dónde enviar los datos, por lo tanto, implementando enrutamiento estático también en los otros Router de la red, el administrador puede crear una ruta específica y controlada, por donde los paquetes pueden llegar a su destino final.
- **Disponibilidad:** A diferencia del enrutamiento dinámico, donde en caso de alguna falla en la ruta original, este genera una ruta alternativa. En el enrutamiento estático, siempre se utilizará la misma ruta, a excepción que falle algún medio físico.
- **Fácil de implementar en redes pequeñas**
- **Bajos gastos generales (Overhead):** Debido a que el Router ha sido configurado por donde enviar los datos, no va a necesitar realizar cálculos para encontrar el mejor camino.

3.1.2.2 Enrutamiento Dinámico

El enrutamiento dinámico le permite a los routers ajustar, los caminos utilizados para transmitir paquetes. Cada protocolo posee sus propios métodos para definir rutas (camino más corto, utilizar rutas publicadas por pares, etc.). Esto se logra mediante el uso de protocolos de enrutamiento, como los son RIP, IGRP, EIGRP u OSPF.

Un router configurado con un protocolo de enrutamiento dinámico puede:

- Recibir y procesar las actualizaciones enviadas por routers vecinos, que ejecutan el mismo protocolo de enrutamiento.
- Aprender sobre redes remotas por medio de las actualizaciones recibidas de routers vecinos.
- Si existiesen múltiples rutas a una misma red remota, aplicar un algoritmo para determinar la mejor ruta, la más rápida.
- Anunciar, a routers vecinos, sobre sus rutas a redes remotas.
- Actualizar sus rutas cuando, por algún motivo, ocurre algún cambio en la topología.

A diferencia del enrutamiento estático, este tipo se adapta de mejor forma a organizaciones que poseen redes más grandes.

3.2 Configuración de una red doméstica

3.2.1 Topología de la red

En el desarrollo de la actividad el equipo diseñó la red que se puede apreciar en la siguiente imagen (ilustración 1). La red está compuesta por dos switch y dos hosts cuyo sistema operativo fue Windows 10 y Ubuntu. Además, se utilizó un PC con Ubuntu como Router. Para conectar los dispositivos se utilizaron cables directos de par trenzado.

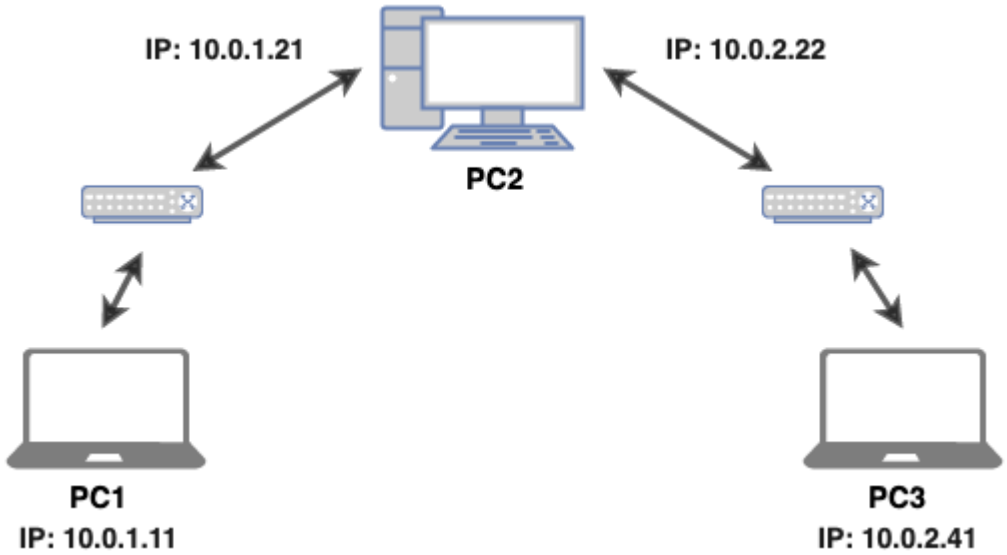

Ilustración 1Topología de la red

En la siguiente tabla (tabla 1) se puede muestra la dirección IPv4 asignada de forma estática a cada interfaz de los dispositivos.

Tabla 1 Dirección de cada dispositivo

Identificador	Interfaz Ethernet 1	Interfaz Ethernet 2
PC1	10.0.1.11	-
PC2	10.0.1.21	10.0.2.22
PC3	10.0.2.41	-

3.2.2 Configuración de la red

De acuerdo a la topología presentada en el punto anterior, se puede observar la siguiente imagen (ilustración 2) con la distribución de la red. Donde se puede observar que los dispositivos que se encuentran dentro de la circunferencia de color rojo, pertenecen a la **red 1**. Por su parte, los dispositivos que están en el área verde, son de la **red 2.**

Para identificar a qué red pertenece cada dispositivo, tan solo se debe fijar, en este caso, en el último byte de la porción de red en la dirección IP de cada dispositivo.

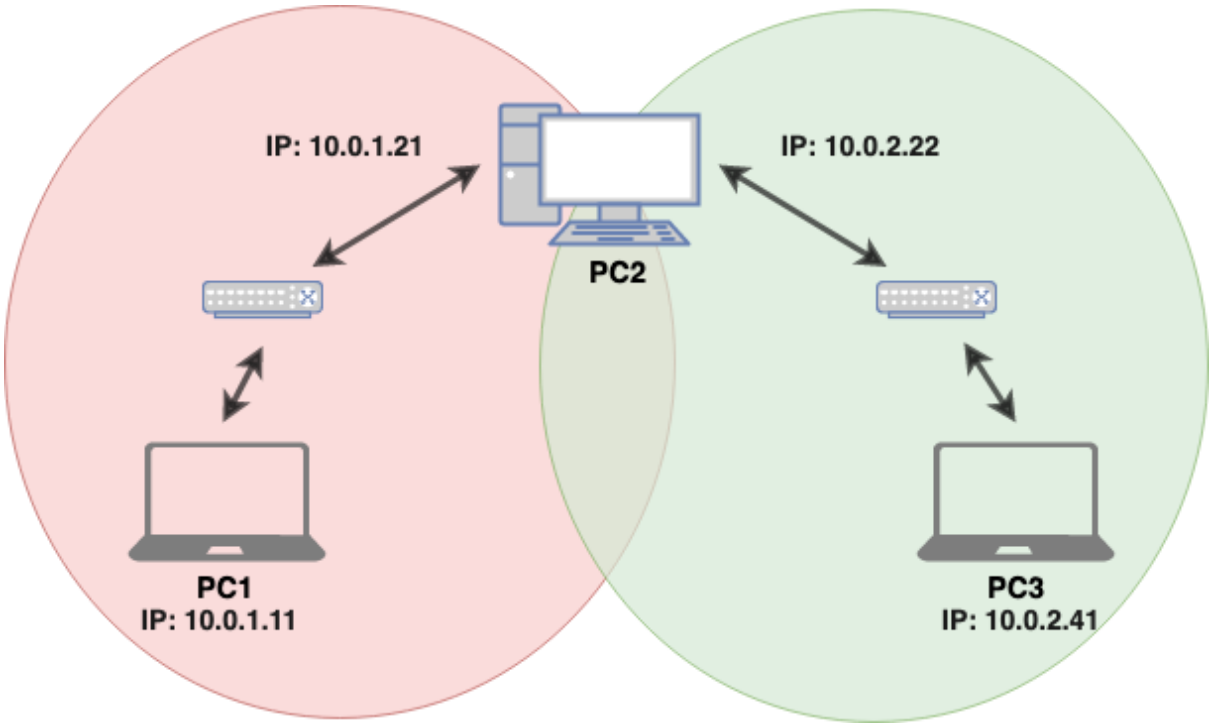

Ilustración 2 Diagrama por redes

Por lo tanto, se procederá a enseñar el cómo es que se configuró cada uno de los dispositivos de la red. Cabe destacar, que, en la red armada, los Switchs utilizados no fueron configurados.

3.2.2.1 Configuración de hosts

Antes de realizar las pruebas de conectividad fue necesario configurar las direcciones IPv4 en cada host. Debido a la naturaleza del ejercicio, esto se realizó de forma manual, por lo que, a continuación, se presentará cómo es que se logró configurar cada dispositivo de la red.

3.2.2.1.1 Host: PC1

Como se puede apreciar en la siguiente imagen (ilustración 3), el sistema operativo del PC1 utiliza Windows 10. En el campo de IP se rellena con la dirección asignada que se encuentra en la tabla asociada a la topología de red. Mientras que, en la puerta de enlace predeterminada, se debe utilizar la dirección de la interfaz Ethernet de la red 1 (**10.0.1.21**).

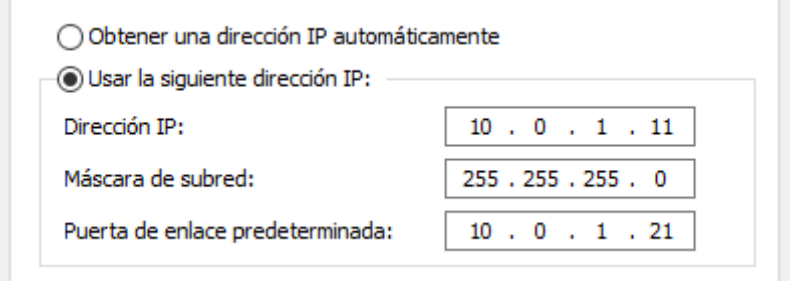

Ilustración 3 Configuración PC 1

3.2.2.1.2 Host: PC3

En la siguiente imagen (ilustración 4) se puede apreciar la configuración del PC3, donde se puede observar que este posee Ubuntu como sistema operativo. Para configurar su dirección IP y puerta de enlace se siguió la misma lógica que la configuración del PC1, donde se utilizó la IP que se encuentra en la tabla adjunta a la topología de red. Además, su puerta de enlace debió coincidir con la interfaz ethernet de la red 2 (**10.0.2.22**).

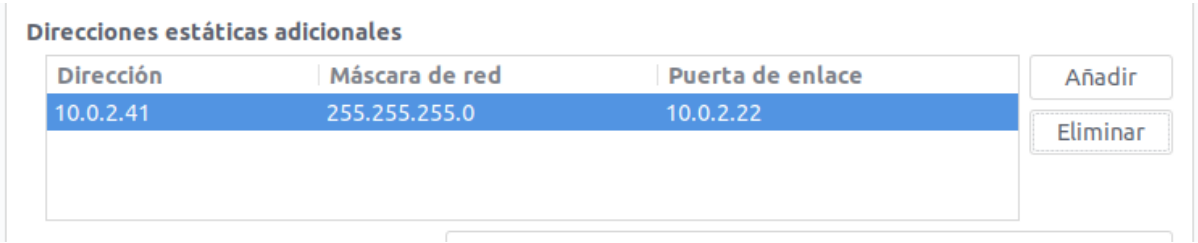

Ilustración 4 Configuración PC 3

3.2.2.2. Configuración de PC Router

En este caso particular, no solo se debió configurar las interfaces ethernet del dispositivo, además, se tuvo que configurar la tabla de ruteo. A continuación, se presenta el cómo es que se configuró cada uno de estos ítems.

3.2.2.2.1 Configuración de las interfaces

A diferencia de los hosts, el PC Router cuenta con cuatro interfaces ethernet, pero para efectos de este ejercicio, solo se utilizarán dos. Entonces en la siguiente tabla (tabla 2) se mostrará el resultado de la configuración de cada interfaz ethernet.

Tabla 2 Configuración de las interfaces del PC Router

Red 1: Interfaz ethernet 1	Red 2: Interfaz ethernet 2
IPv4 Dirección IP: 10.0.1.21 Dirección de difusión: 10.0.1.255 Máscara de subred: 255.255.255.0	**IPv4** Dirección IP: 10.0.2.22 Dirección de difusión: 10.0.2.255 Máscara de subred: 255.255.255.0

3.2.2.2.2 Configuración de la tabla de ruteo

La tabla de ruteo es aquella que almacena las rutas de los diferentes nodos de una red. Entonces para lograr el enrutamiento estático, se debió agregar las direcciones de los hosts descritos en el punto anterior. Para lograr esto es necesario utilizar el siguiente comando en PC con el sistema operativo Ubuntu en el modo super usuario.

route add -net ***dirección IP*** netmask ***máscara de red*** gw ***puerta de enlace***

La configuración realizada se puede apreciar en la siguiente imagen (ilustración 5).

```
root@redes-HP-Compaq-dc5800-Small-Form-Factor:/home/redes# route add -net 10.0.1.11 netma
sk 255.255.255.255 gw 10.0.1.21
SIOCADDRT: El archivo ya existe
root@redes-HP-Compaq-dc5800-Small-Form-Factor:/home/redes# route add -net 10.0.2.41 netma
sk 255.255.255.255 gw 10.0.2.22
root@redes-HP-Compaq-dc5800-Small-Form-Factor:/home/redes#
```

Ilustración 5 Configuración de tabla de ruteo

Por lo que los comandos introducidos fueron los siguientes:

1. # route add -net ***10.0.1.11*** netmask ***255.255.255.255*** gw ***10.0.1.21***
2. # route add -net ***10.0.2.41*** netmask ***255.255.255.255*** gw ***10.0.2.22***

3.3 Pruebas de conectividad

A continuación, se mostrarán los resultados de las pruebas de conexión entre los distintos dispositivos de la red.

3.3.1 Conectividad Host - PC Router

En primer lugar, se enseñarán los resultados de las pruebas entre los distintos hosts con el PC Router, donde se utilizarán diversas técnicas y herramientas para obtener y analizar los resultados obtenidos.

3.3.1.1 Pruebas PC1 - PC Router

Para hacer las pruebas de conectividad, se realizaron una serie de ping entre el PC host y el PC Router. Los resultados de esto se pueden apreciar en la siguiente serie de imágenes.

En la siguiente captura (ilustración 6) se puede apreciar un ping desde el PC Router hacia el PC host. Como se puede observar, existe conectividad entre ambos dispositivos.

```
64 bytes from 10.0.1.11: icmp_req=4 ttl=128 time=0.776 ms
64 bytes from 10.0.1.11: icmp_req=5 ttl=128 time=0.929 ms
64 bytes from 10.0.1.11: icmp_req=6 ttl=128 time=0.843 ms
64 bytes from 10.0.1.11: icmp_req=7 ttl=128 time=0.760 ms
64 bytes from 10.0.1.11: icmp_req=8 ttl=128 time=0.924 ms
64 bytes from 10.0.1.11: icmp_req=9 ttl=128 time=0.843 ms
64 bytes from 10.0.1.11: icmp_req=10 ttl=128 time=0.756 ms
64 bytes from 10.0.1.11: icmp_req=11 ttl=128 time=0.661 ms
```

Ilustración 6 Prueba de Ping de PC1 a PC Router

También se realizó el análisis utilizando la herramienta de wireshark, donde se puede observar de mejor forma el intercambio de paquetes entre los hosts. La siguiente imagen (ilustración 7) ayuda a comprobar el correcto funcionamiento de la red creada.

17 4.323275	10.0.1.21	10.0.1.11	ICMP	98 Echo (ping) request	id=0x0a96, seq=5/1280, ttl=64 (reply in 18)
18 4.323418	10.0.1.11	10.0.1.21	ICMP	98 Echo (ping) reply	id=0x0a96, seq=5/1280, ttl=128 (request in 17)
19 5.323304	10.0.1.21	10.0.1.11	ICMP	98 Echo (ping) request	id=0x0a96, seq=6/1536, ttl=64 (reply in 20)
20 5.323450	10.0.1.11	10.0.1.21	ICMP	98 Echo (ping) reply	id=0x0a96, seq=6/1536, ttl=128 (request in 19)
21 6.323313	10.0.1.21	10.0.1.11	ICMP	98 Echo (ping) request	id=0x0a96, seq=7/1792, ttl=64 (reply in 22)
22 6.323460	10.0.1.11	10.0.1.21	ICMP	98 Echo (ping) reply	id=0x0a96, seq=7/1792, ttl=128 (request in 21)
23 7.323377	10.0.1.21	10.0.1.11	ICMP	98 Echo (ping) request	id=0x0a96, seq=8/2048, ttl=64 (reply in 24)
24 7.323522	10.0.1.11	10.0.1.21	ICMP	98 Echo (ping) reply	id=0x0a96, seq=8/2048, ttl=128 (request in 23)

Ilustración 7 Captura de intercambio en Wireshark

Utilizando el comando netstat en el PC1 se puede apreciar que los paquetes con red destino **0.0.0.0** se enviaran por la red identificada en la puerta de enlace por defecto, identificada como **10.0.1.21**. Esto se puede apreciar en la siguiente imagen (ilustración 8).

```
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0        10.0.1.21       10.0.1.11    291
         10.0.1.0    255.255.255.0      En vínculo        10.0.1.11    291
        10.0.1.11  255.255.255.255      En vínculo        10.0.1.11    291
       10.0.1.255  255.255.255.255      En vínculo        10.0.1.11    291
        127.0.0.0        255.0.0.0      En vínculo        127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo        127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo        127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo        127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo        10.0.1.11    291
  255.255.255.255  255.255.255.255      En vínculo        127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo        10.0.1.11    291
```

Ilustración 8 Tabla de enrutamiento de PC1

3.3.1.2 Pruebas PC3 - PC Router

De forma análoga se realizó la comprobación de conectividad entre el PC3 y el PC Router, donde se pudo comprobar su perfecto funcionamiento.

3.3.2 Conectividad Host - Host

En los siguientes puntos se mostrarán los resultados de las pruebas de conectividad en dos escenarios distintos. El factor diferenciador entre estos, es la activación del mecanismo de reenvío de paquetes que se reciben por una interfaz física, llamado IP Forwarding.

3.3.2.1 Conectividad con IP Forward desactivado

En la siguiente imagen (ilustración 9) se puede apreciar del ping realizado desde el PC1 ubicado en la r**ed 1**, hacia el PC3 que se encuentra en la **red 2**.

```
C:\Users\AICI>ping 10.0.2.41

Haciendo ping a 10.0.2.41 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.0.2.41:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Ilustración 9 Ping desde PC1 a PC3

Como se puede apreciar en la imagen anterior (ilustración 9), al momento de realizar el envío de paquetes desde un dispositivo hacía red resulta en total fracaso, y esto se debe a que el dispositivo intermedio (Router), no es capaz de resolver esta petición. Por lo que se presenta la siguiente situación (ilustración 10).

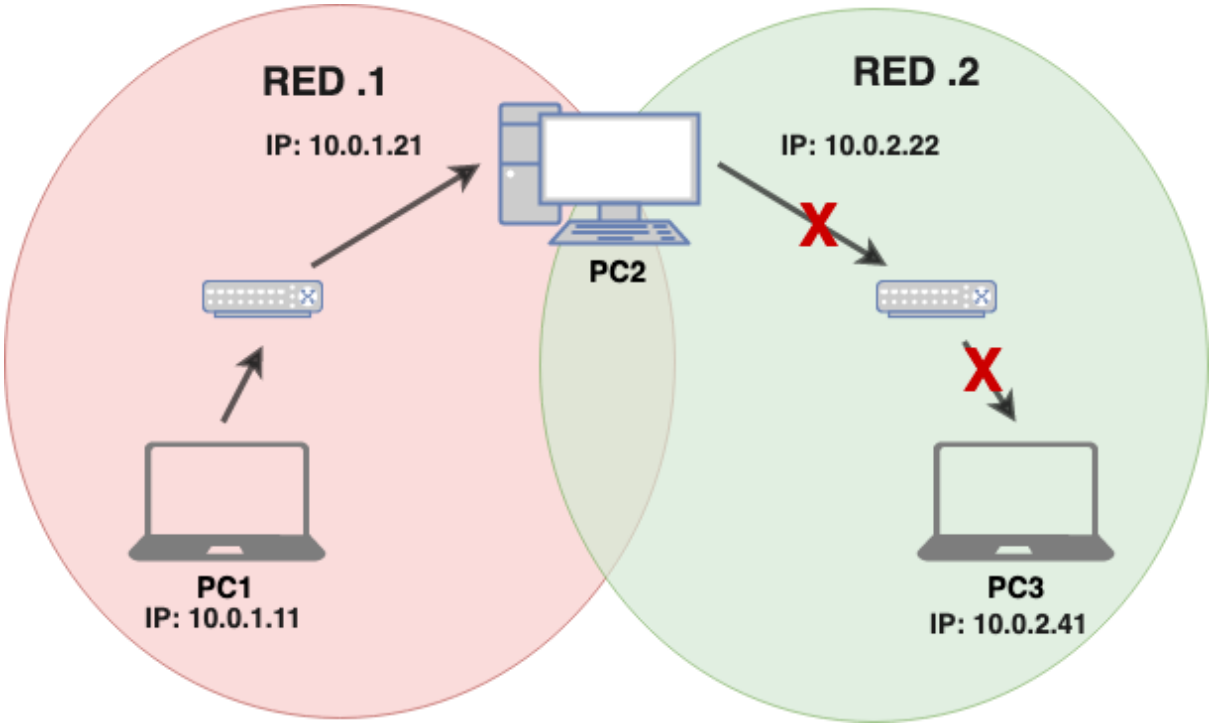

Ilustración 10 Diagrama de envío de paquetes sin IP Forward

Y es que, como se comprobó en la sección de pruebas de conectividad entre PC Host y PC Router, existe conectividad entre estos dispositivos, pero es justamente, el PC Router el que no es capaz de direccionar el mensaje hacía la otra red.

Realizando el análisis de wireshark, también se obtiene un mensaje de “no respuesta” al momento de enviar los paquetes al host destino.

2	3.599562	10.0.1.11	10.0.2.41	ICMP	74 Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (no response found!)
7	8.580867	10.0.1.11	10.0.2.41	ICMP	74 Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (no response found!)
11	13.580420	10.0.1.11	10.0.2.41	ICMP	74 Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (no response found!)
13	18.579959	10.0.1.11	10.0.2.41	ICMP	74 Echo (ping) request id=0x0001, seq=99/25344, ttl=128 (no response found!)

Ilustración 11 Captura de ping entre PC1 a PC3

3.3.2.2 Conectividad con IP Forward activado

Antes de mostrar los resultados del envío de paquetes entre PC Host, se enseñará cómo es que se activó el mecanismo de IP Forward.

3.3.2.2.1 Activación de IP Forward

Como se mencionó al inicio de la sección anterior, este mecanismo permite el reenvío de paquetes que se reciben por una interfaz física. Para activarlo en un PC con Ubuntu es necesario estar en modo de superusuario y luego introducir el siguiente comando.

echo **“1”** > /proc/sys/net/ipv4/ip_forward

Donde el número uno representa que el mecanismo está activado. Esto se puede observar abriendo el archivo de texto donde se encuentra el ip forward.

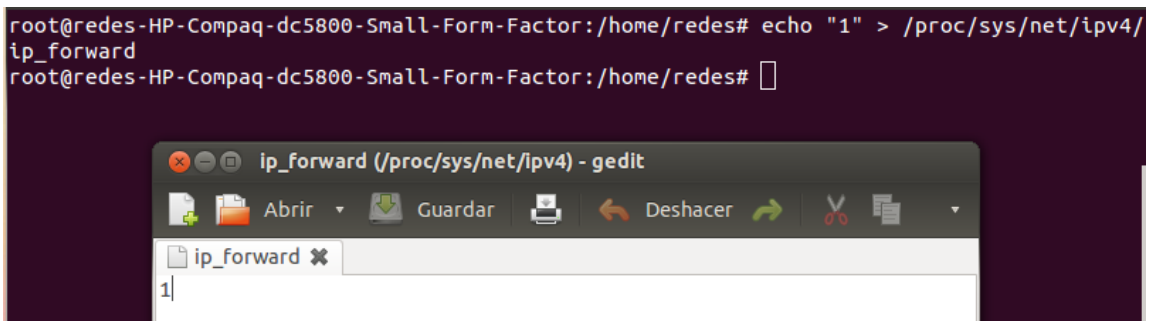

Ilustración 12 Configuración de IP Forward de PC Router

Cabe destacar que este comando se debe utilizar cada vez que se apague y encienda el equipo, a no ser que se introduzca un comando para que esta modificación persista.

3.3.2.2.2 Pruebas de conectividad

Una vez activado el mecanismo de IP forward, se realizaron las pruebas de conectividad entre host que se pueden apreciar en las siguientes imágenes (ilustración 13 y 14), donde se realizarán una serie de envíos desde el PC1 hacia el PC3.

```
C:\Users\AICI>ping 10.0.2.41

Haciendo ping a 10.0.2.41 con 32 bytes de datos:
Respuesta desde 10.0.2.41: bytes=32 tiempo=1ms TTL=63
Respuesta desde 10.0.2.41: bytes=32 tiempo=1ms TTL=63
Respuesta desde 10.0.2.41: bytes=32 tiempo=1ms TTL=63
Respuesta desde 10.0.2.41: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 10.0.2.41:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

Ilustración 13 Pruebas de conectividad de PC1 a PC3

En la imagen anterior (ilustración 13) se puede apreciar el envío de paquetes desde un dispositivo ubicado en la **red 1**, hacia un equipo en la **red 2**.

Para apreciar de mejor forma este intercambio de paquetes ICMP, se utilizará la herramienta de wireshark, pero en este caso, se capturará el envío de paquetes desde el PC3 (**red 2**) hacia el PC1 (**red 1**).

2	0.000149	10.0.1.11	10.0.2.41	ICMP	98	Echo (ping) reply id=0x1868, seq=1/256, ttl=128 (request in 1)
3	1.001211	10.0.2.41	10.0.1.11	ICMP	98	Echo (ping) request id=0x1868, seq=2/512, ttl=63 (reply in 4)
4	1.001385	10.0.1.11	10.0.2.41	ICMP	98	Echo (ping) reply id=0x1868, seq=2/512, ttl=128 (request in 3)
5	2.002635	10.0.2.41	10.0.1.11	ICMP	98	Echo (ping) request id=0x1868, seq=3/768, ttl=63 (reply in 6)
6	2.002779	10.0.1.11	10.0.2.41	ICMP	98	Echo (ping) reply id=0x1868, seq=3/768, ttl=128 (request in 5)
7	3.004087	10.0.2.41	10.0.1.11	ICMP	98	Echo (ping) request id=0x1868, seq=4/1024, ttl=63 (reply in 8)
8	3.004229	10.0.1.11	10.0.2.41	ICMP	98	Echo (ping) reply id=0x1868, seq=4/1024, ttl=128 (request in 7)
9	4.006032	10.0.2.41	10.0.1.11	ICMP	98	Echo (ping) request id=0x1868, seq=5/1280, ttl=63 (reply in 10)
10	4.006174	10.0.1.11	10.0.2.41	ICMP	98	Echo (ping) reply id=0x1868, seq=5/1280, ttl=128 (request in 9)

Ilustración 14 Captura del envío de paquetes entre PC1 a PC3

Otra prueba que se realizó, fue la de utilizar el comando **tracert** para obtener la ruta y los saltos que deben seguir los paquetes que son enviados desde una red a otra. A partir de esto se llegó al siguiente resultado que se puede apreciar en la imagen (ilustración 15).

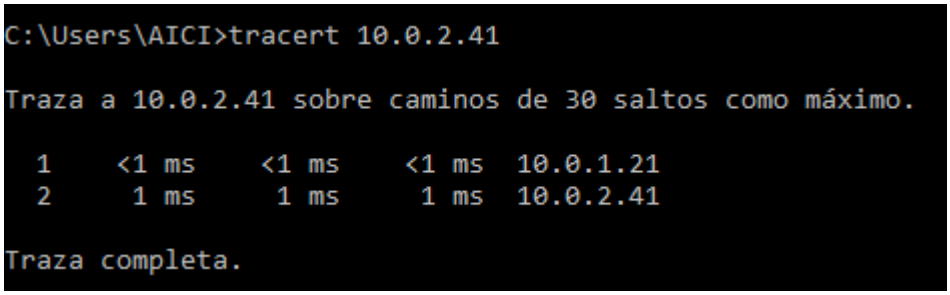

Ilustración 15 Traza que recorre el envío de paquetes desde el PC1 a PC3

Como se puede observar en la anterior imagen (ilustración 15), antes de que el paquete llegue al host de destino, tuvo que pasar por la interfaz del Router asociada al host. Una vez que el paquete haya llegado PC Router, este se encarga de dirigir el paquete a la dirección de destino en la otra red.

3.4 Configuración un PC como Router

Como parte fundamental al momento de configurar una red para cualquier entorno, es necesario considerar la posibilidad que más dispositivos de los que fueron considerados en una primera instancia requieran conectarse a la red una organización, lo que podría provocar un gran dolor de cabeza al administrador de red. Para abordar esto, es necesario utilizar protocolos como DHCP que permiten asignar una dirección lógica a cada dispositivo de forma automática.

3.4.1 Protocolo de configuración dinámica de host (DHCP)

3.4.1.1 ¿Qué es DHCP?

Dynamic Host Configuration Protocol (DHCP), o, mejor dicho, protocolo de configuración dinámica de host, es un protocolo de red de tipo cliente/servidor mediante el cual un servidor de DHCP asigna dinámicamente una dirección IP y también contiene otras funciones de utilidad como la configuración de la máscara de subred apropiada, la puerta de enlace predeterminada y la información del servidor DNS en un ordenador o cualquier otra forma de dispositivo.
Este servidor, mencionado anteriormente, posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

3.4.1.2 ¿Cómo funciona?

Todos aquellos dispositivos que estén configurados con DHCP mandan una petición al servidor DHCP solicitando información sobre las configuraciones de red. El servidor responde al dispositivo que realiza la solicitud proporcionando información de configuración sobre la dirección IP que ha sido especificada por el administrador de red. Luego, el servidor DHCP actualiza una asignación para que un dispositivo o cliente DHCP pueda solicitar los mismos parámetros, tras lo cual se puede volver a realizar el mismo proceso.

3.4.1.3 Operaciones DHCP

Las operaciones de DHCP se dividen en cuatro fases:

- **DHCP Discover**: Es una solicitud DHCP realizada por un cliente de este protocolo para que el servidor DHCP de dicha red de computadoras le asigne una dirección IP.
- **DHCP Offer**: Es el paquete de respuesta del Servidor DHCP a un cliente DHCP ante su petición.
- **DHCP Request**: El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.
- **DHCP Ackowledge**: El servidor reconoce la solicitud y la envía acuse de recibo al cliente del cliente, se inicia la fase final del proceso de configuración.

3.4.2 Configuración de servidor DHCP

Para el desarrollo de la actividad, el equipo armó la red que se puede apreciar en la siguiente imagen (ilustración 16). La red está compuesta por dos notebooks cuyo sistema operativa es Windows 10, un Switch y un PC con sistema operativo Ubuntu 12.04 que realizará las funciones de Router. Cabe destacar que el PC-Router debió tener al menos dos tarjetas Ethernet, donde una está conectada directo hacia Internet y la otra está conectada en el Switch. Se utilizaron cables directos como medio físico para realizar la conexión de los dispositivos.

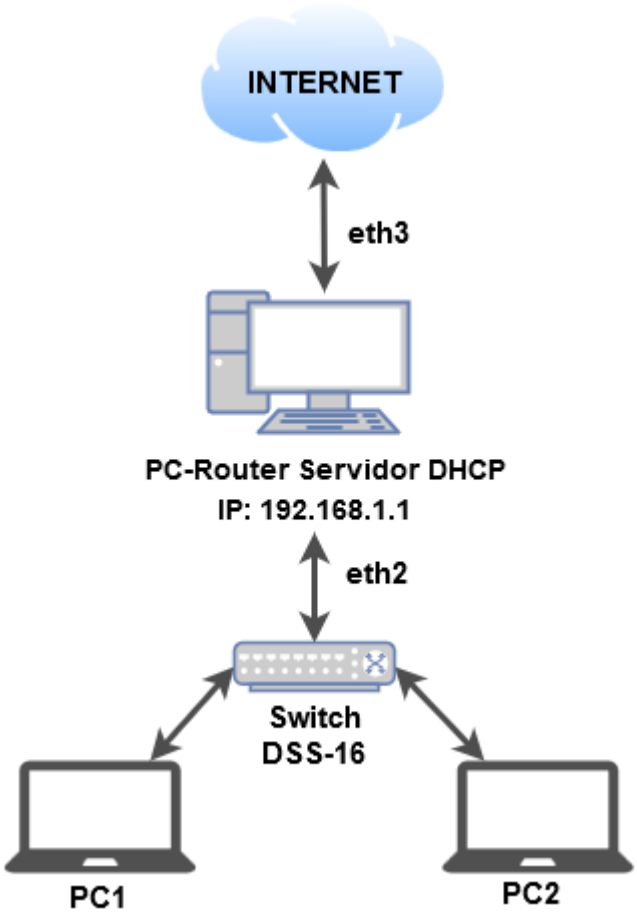

Ilustración 16 Arquitectura de la red DHCP

En la siguiente tabla (tabla 3) se puede observar como es se configuró cada interfaz ethernet de los dispositivos finales y el PC-Router, donde se podrá apreciar si está recibió una dirección Ipv4 de forma manual o automática.

Tabla 3 Configuración de dispositivos

Identificador	**Interfaz Ethernet 1**	**Interfaz Ethernet 2**
PC-Router	Automática	Manual
PC1	Automática	-
PC2	Automática	-

3.4.2.1 Configuración de interfaces en PC-Router y dispositivos finales

Como se puede apreciar en la tabla anterior (tabla 3), en la experiencia se utilizaron dos interfaces ethernet del PC-Router que fueron configuradas de la siguiente forma.

3.4.2.1.1 Configuración interfaz ethernet 1

Está interfaz se identifica en el sistema con el código de **eth3**, lo que quiere decir que se está utilizando la conexión cableada número cuatro. De acuerdo a la topología, está se conecta de forma directa a Internet, por lo que fue utilizada la configuración por defecto para la asignación de direcciones IP, por lo que es el Router de la Universidad el encargado de asignar direcciones públicas. Esto se puede apreciar en la porción de red de la dirección obtenida, donde inicia con la siguiente secuencia **"146.83."**. Se puede observar en la siguiente imagen el resultado de la configuración (ilustración 17).

Ilustración 17 Configuración eth3

3.4.2.1.2 Configuración interfaz ethernet 2

Como se puede apreciar en la arquitectura de la red (ilustración 16), se utilizó la interfaz ethernet que se identifica con el código **eth2**, está va a ser la encargada de suministrar direcciones Ipv4 privadas al resto de dispositivos que se conecten a la red. La configuración manual del PC-Router es un paso necesario antes de configurar e iniciar el servidor DHCP, es por eso que se realizó la configuración que se puede apreciar en la siguiente imagen (ilustración 18).

Ilustración 18 Configuración eth2

3.4.2.1.3 Configuración de dispositivos finales

Como se mencionó en la presentación de la arquitectura de la red, los dispositivos finales utilizan Windows 10 como sistema operativo Entonces, para habilitar la opción de recibir una dirección de forma automática se debió utilizar la siguiente configuración.

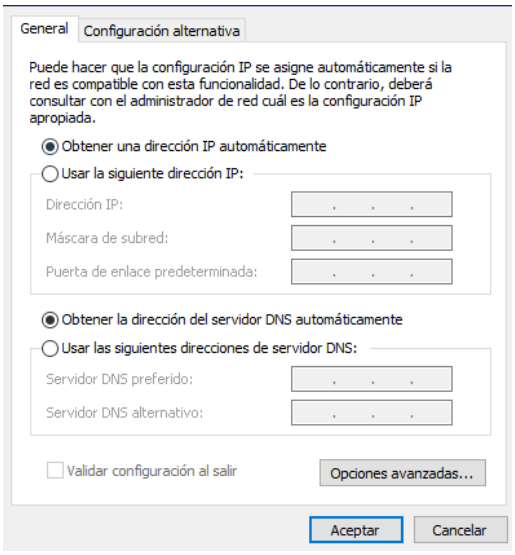

Ilustración 19 Configuración de host

3.4.2.2 Instalación de servidor DHCP en PC-Router

Para poder instalar el servidor en el dispositivo, es necesario entrar en modo administrador, ya que eso evitará que el sistema operativo solicité la contraseña del dispositivo en cada oportunidad que se quiera realizar un cambio, por lo que se deberá utilizar el siguiente comando en la terminal. Esto se puede apreciar la ilustración 20.

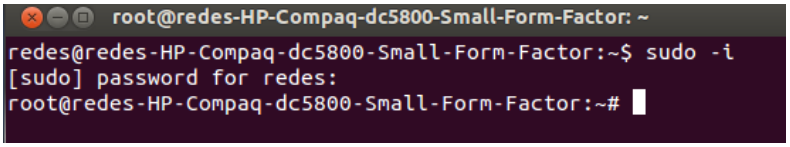

Ilustración 20 Ingresando a modo administrador

A continuación, se ingresó el siguiente comando para instalar el servidor DHCP. En la siguiente imagen (ilustración 21) se puede observar la instrucción y el mensaje retornado por el sistema operativo.

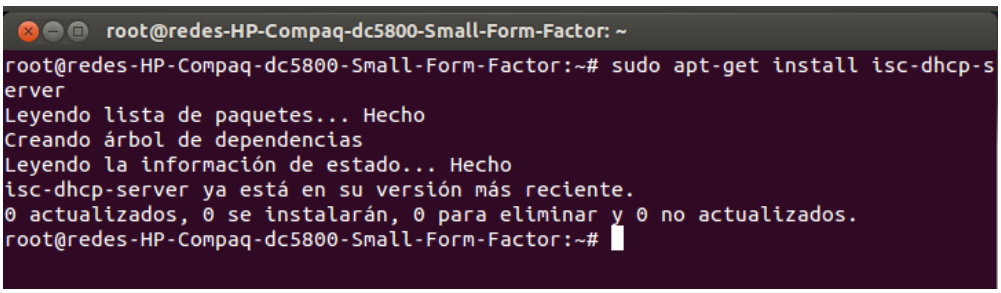

Ilustración 21 Instalación servidor DHCP

Por defecto el servidor DHCP realiza atiende a las peticiones por el puerto de conexión cableada número uno (eth0), pero en nuestro caso, el equipo de trabajo utilizó el puerto ethernet tres (eth2) por lo que debió realizar las siguientes modificaciones utilizando el comando que se puede apreciar en la ilustración 22.

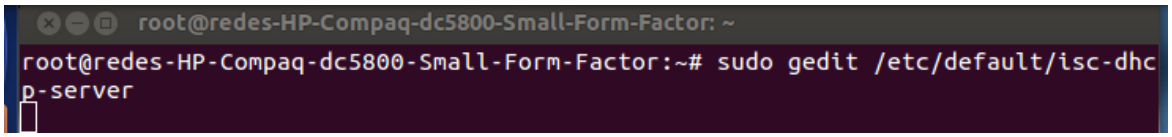

Ilustración 22 Edición de servidor DHCP

El comando anterior permitirá desplegar el editor de texto del sistema operativo, ahí se deberá cambiar el valor de la variable **INTERFACES** por el de la interfaz ethernet que va a ser utilizada. Esto se puede observar en la ilustración 23.

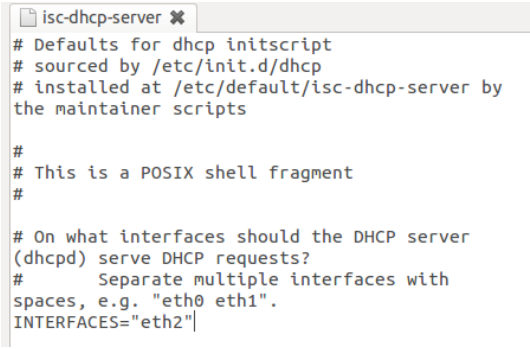

Ilustración 23 Modificación del archivo DHCP

Finalmente, para iniciar el servidor DHCP en el PC-Router, se deberá ingresar el siguiente comando en la terminal de Ubuntu.

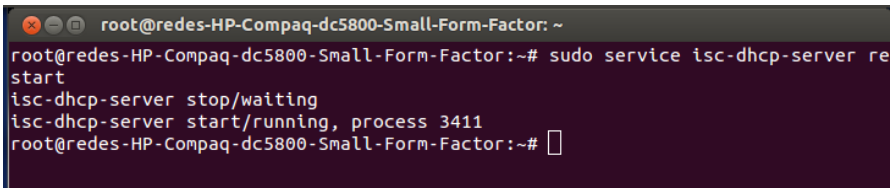

Ilustración 24 Inicio del servidor DHCP

3.4.3 Pruebas y mediciones

A continuación, se mostrarán los resultados de las pruebas de conectividad entre el PC-Router y el resto de dispositivos finales.

3.4.3.1 Asignación de direcciones Ipv4

El proceso de asignar IP de forma automática se puede observar utilizando la herramienta de Wireshark, donde se el software es capaz de capturar el intercambio de paquetes entre el servidor y el host. En el caso que se presentará a continuación, se muestra como es el proceso en el que un dispositivo solicita IP a un servidor DHCP. Esto se puede apreciar en la siguiente imagen (ilustración 25).

	Source	Destination	Protocol	Length	Info
1	192.168.1.5	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x258e1e3f
2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x62e02fd8
3	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0x62e02fd8
4	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0x62e02fd8
5	192.168.1.1	192.168.1.5	DHCP	342	DHCP ACK - Transaction ID 0x62e02fd8

Ilustración 25 Operaciones DHCP

A continuación, se describiría cada uno de los paquetes enviados entre los dispositivos.

1. El primer paquete el cliente solicita información al servidor DHCP. Además, el cliente libera su dirección IP.
2. El cliente, cuya IP es 0.0.0.0 envía un paquete con dirección de destino 255.255.255.255 lo quiere decir que es del tipo broadcast.
3. El servidor DHCP responde enviando un paquete DHCP OFFER.
4. El cliente responde al mensaje DHCP OFFER enviando un paquete DHCP REQUEST. La dirección de origen del cliente sigue siendo 0.0.0.0 y el destino para el paquete sigue siendo 255.255.255.255. El cliente conserva 0.0.0.0 porque el cliente no ha recibido la verificación desde el servidor que está bien comenzar a usar la dirección que ofrece. Tampoco cambia el destino (broadcast), porque más de un servidor DHCP puede que haya respondido a la solicitud y puede estar reteniendo una reserva para la solicitud del cliente. Esto permite a los otros servidores DHCP puedan liberar sus direcciones ofrecidas y devolverlos a sus grupos disponibles.
5. El servidor DHCP responde al mensaje DHCP REQUEST con un paquete DHCP ACK, completando así el ciclo de inicialización.

3.4.3.2 Pruebas de conectividad

Como prueba de conectividad se utilizó el comando tracert desde uno de los hosts hacia el servidor DHCP. Realizado esto, se obtuvo el siguiente resultado que se puede observar en la siguiente imagen (ilustración 26).

```
C:\Users\Usuario>tracert 192.168.1.1

Traza a 192.168.1.1 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  192.168.1.1

Traza completa.

C:\Users\Usuario>
```

Ilustración 26 TraceRoute desde host a servidor

De lo anterior, se obtuvo la siguiente captura de paquetes con la herramienta de Wireshark (ilustración 27).

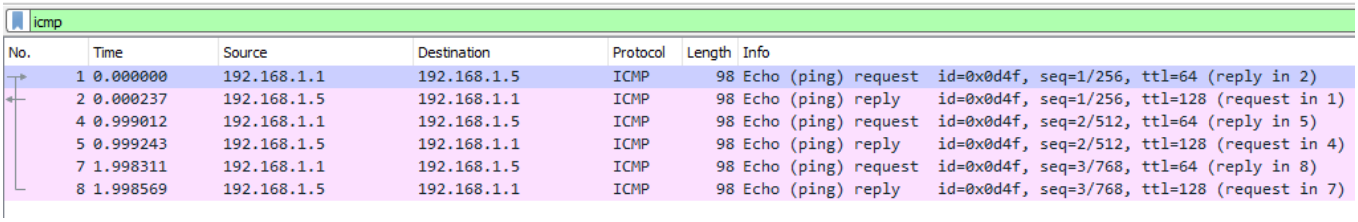

Ilustración 27 Captura con Wireshark

De acuerdo a las mediciones realizadas se pudo comprobar la correcta conectividad entre los hosts y el PC-Router. Además, se realizaron las pruebas de conectividad entre dispositivos finales, donde se realiza un ping desde un host con IP **192.168.1.3** hacia otro host en la misma red de IP **192.168.1.5**.

```
C:\Users\AICI>ping 192.168.1.5

Haciendo ping a 192.168.1.5 con 32 bytes de datos:
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ilustración 28 Pruebas de conectividad entre hosts

Finalmente, se utilizó el comando route -e desde el servidor DHCP con la finalidad de guardar el contenido de la tabla de ruteo del PC-Router.

```
root@redes-HP-Compaq-dc5800-Small-Form-Factor:~# route -e
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic   MSS Ventana irtt Interfaz
default         SalasPCs.broute 0.0.0.0         UG        0 0          0 eth3
146.83.102.0    *               255.255.255.128 U         0 0          0 eth3
link-local      *               255.255.0.0     U         0 0          0 eth2
192.168.1.0     *               255.255.255.0   U         0 0          0 eth2
root@redes-HP-Compaq-dc5800-Small-Form-Factor:~#
```

Ilustración 29 Tabla de ruteo de PC-Router

4. Conclusión

En conclusión, de acuerdo a las actividades de investigación y experimentación realizadas, se pudo determinar la importancia de realizar configuraciones de acuerdo a las necesidades de las organizaciones con la finalidad de conservar la integridad y seguridad del flujo de datos, por lo que el uso de técnicas como el ruteo estático son muy importantes de abordar. Otro punto clave, es la implementación de mecanismos que permitan compartir información entre dispositivos ubicados en distintas redes.

Además, partir de la segunda parte de la actividad se logró abordar la necesidad de diseñar e implementar redes que sean capaces de adaptarse a distintos escenarios, como lo son el cambio de los dispositivos finales que se serán parte de ella, es por eso que el estudio de protocolos como DHCP se vuelven muy necesario.

Abordando la experiencia práctica del laboratorio, se pudo comprobar los aspectos teóricos que se estudiaron en la primera parte de la actividad, por ejemplo, el intento de comunicación entre host que se encuentren en distintas redes sin activar el mecanismo de IP Forward, donde utilizó herramientas como Wireshark para realizar análisis sobre el no flujo de paquetes. También, se verifico el correcto funcionamiento del servidor DHCP al momento de conectar diversos dispositivos como lo son PC de escritorio o notebooks en la red.

Para finalizar, en el desarrollo del laboratorio logramos comprender el cómo es utilizar un dispositivo como los es un PC como un Router que sea capaz de comunicar otros equipos.

5. Referencias

- Facultad de informática de Barcelona. IP forwarding.
- System Admin. Rutas estáticas en Debian/Ubuntu.
- Debian handbook. Enrutamiento dinámico.
- Cisco. Enrutamiento: Conceptos fundamentales.
- Lazy Geek. How to Install the DHCP Server on Ubuntu 12.04LTS.
- Microsoft. Conceptos básicos DHCP (Protocolo de configuración dinámica de Host).