

PRÁCTICA 7 – ARP CON CISCO PACKET TRACERT

FECHA: 25/10/21

NOMBRE DEL EQUIPO: EL SIUUU TEAM

PARTICIPANTES: -FISCHER SALAZAR CÉSAR EDUARDO

-LÓPEZ GARCÍA JOSÉ EDUARDO

-MEZA VARGAS BRANDON DAVID

UNIDAD ACADÉMICA: REDES DE COMPUTADORAS

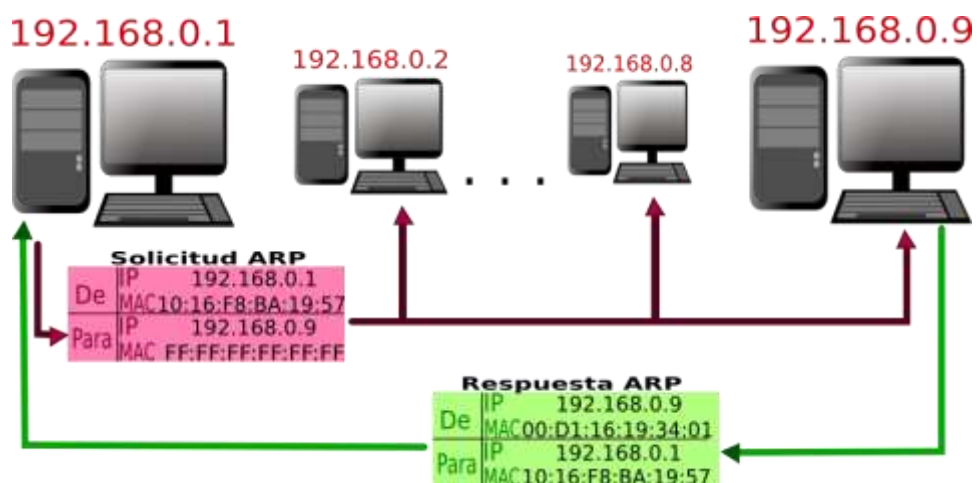
PANORÁMICA

INTRODUCCION

Ahora, retomaremos el entorno virtual práctico de Cisco Packet Tracer, donde tendremos un acercamiento hacia el protocolo ARP (Address Resolution Protocol), el cual es conocido como el primer protocolo a nivel de red.

ARP funciona de la siguiente manera: el protocolo se encarga de asignar direcciones; hay que distinguir si la dirección IP del host de destino se encuentra en la misma red local o en otra subred. En caso de asignar una dirección MAC a una determinada dirección IP, se lleva a cabo una revisión de la máscara de subred. Si la IP se encuentra en la red local, el primer paso es controlar si ya existe una entrada para ella en la caché del ARP.

De igual forma, el protocolo ARP utiliza un formato simple de mensaje para enviar solicitudes o responder a estas; se puede utilizar en cualquier plataforma y que, como tal, se ocupa de la asignación de direcciones MAC en un segundo plano independientemente del sistema, ya sea Linux, Windows o macOS. Asimismo, también existe una herramienta de línea de comandos homónima para los diferentes sistemas operativos con cuya ayuda se puede mostrar la caché de ARP y añadir o eliminar entradas manualmente (arp –man para Linux).



OBJETIVOS

OBJETIVO PRINCIPAL: ARMAR UNA RED EN CISCO PACKET TRACERT PARA ENTENDER EL FUNCIONAMIENTO DEL PROTOCOLO CISCO ARP

OBJETIVO SECUNDARIO. LEER LAS TRAMAS QUE SE PRESENTAN EN UNA SOLICITUD Y RESPUESTA ARP

RECURSOS NECESARIOS PARA REALIZAR LA PRÁCTICA

CISCO PACKET TRACERT

1 ROUTER 1841

2 SWITCH 2960-24TT

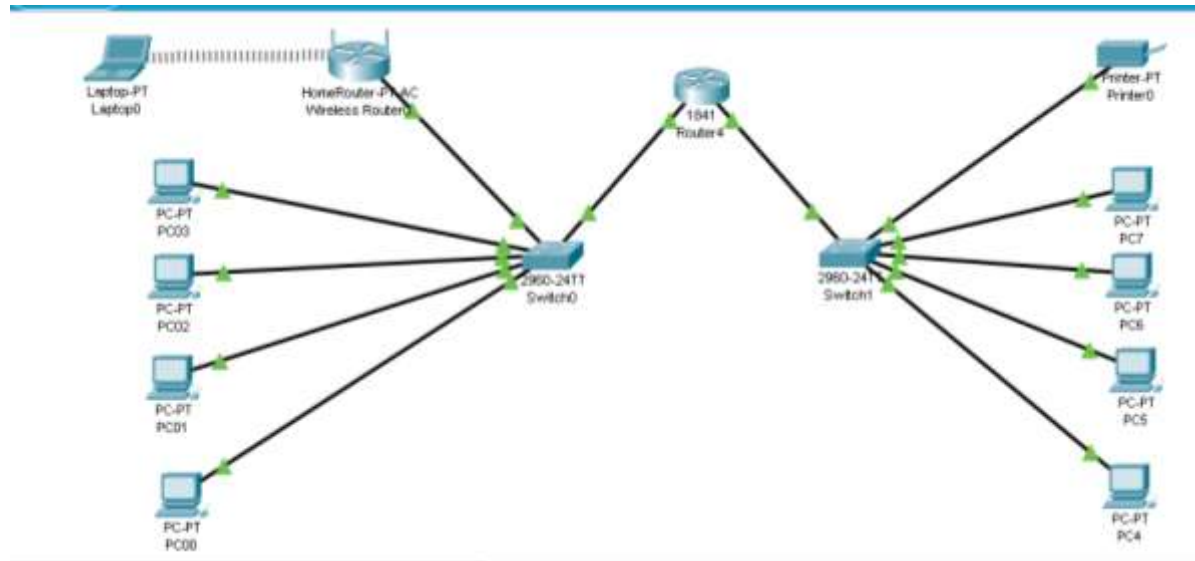
8 PC

1 ROUTER INALAMBIRICO PT-AC

1 LAPTOP INALAMBRICA

1 IMPRESORA

PARTE 1: ARMA ESTA RED EN CISCO PACKET TRACERT



PARTE 2:CONCLUSION DE RESULTADOS

2.1. LA DIRECCION IP DE LA RED DE LA IZQUIERDA ES LA 192.168.1.0, CONFIGURALA Y RECUERDA QUE TENEMOS UN ROUTER INALAMBRICO PARA PODER CONECTAR DISPOSITIVOS INALAMBRICOS, ASEGURARSE QUE HAY CONECTIVIDAD EN LA RED DE LA DERECHA. LA RED DE LA DERECHA TIENE IP 10.0.0.0.

La red armada con nuestra propia forma fue:

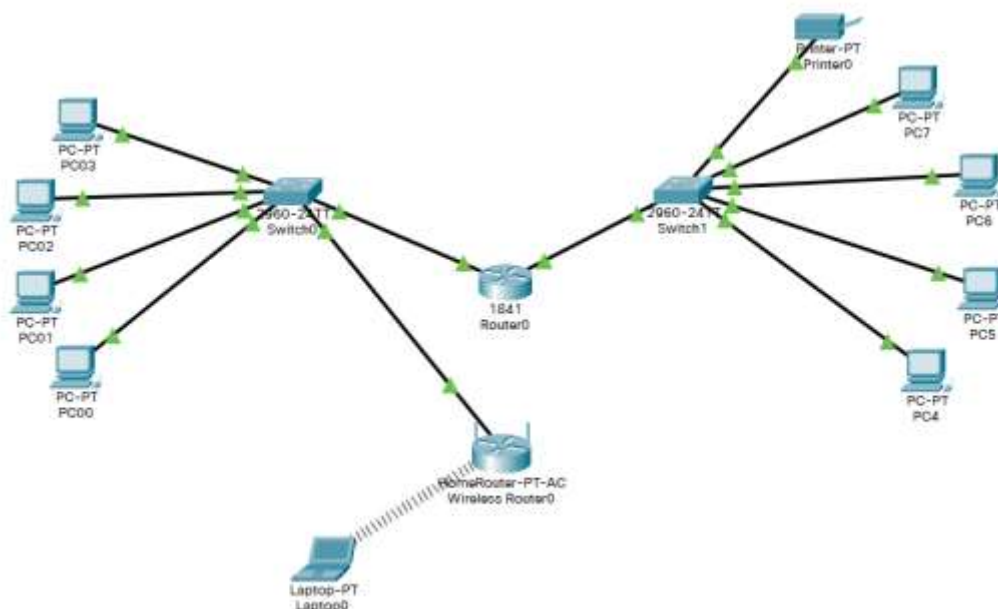


Imagen 1. Red de la práctica

Una vez armada nuestra red se verificó que tuviera conectividad la red de la derecha, así mismo la red de la izquierda.

Primeramente se establecieron comunicaciones entre los dispositivos de la red izquierda, habiendo correcta comunicación.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Di
	Successful	PC3	Laptop0	ICMP		0.000	N	0	(edit)	
	Successful	PC0	PC2	ICMP		0.000	N	1	(edit)	

Imagen 2. Correcta comunicación en red de la izquierda.

De igual forma se comprobó para la red de la derecha.

	Successful	Print...	PC6	ICMP		0.000	N	0	(edit)	
	Successful	PC7	Printer0	ICMP		0.000	N	1	(edit)	
	Successful	PC4	PC6	ICMP		0.000	N	2	(edit)	

Imagen 3. Correcta comunicación en la red de la derecha

2.2. TOMA CAPTURA DE PANTALLA EN DONDE LE PONGAS LAS DIRECCIONES IP EN EL MAPA A CADA DISPOSITIVO CON LA AYUDA DE LA HERRAMIENTA (PLACE NOTE) DE CISCO PACKET TRACERT.

A continuación, se muestra la red, con la diferencia de que ahora se muestra la ip de cada dispositivo gracias a la herramienta place note de cisco.

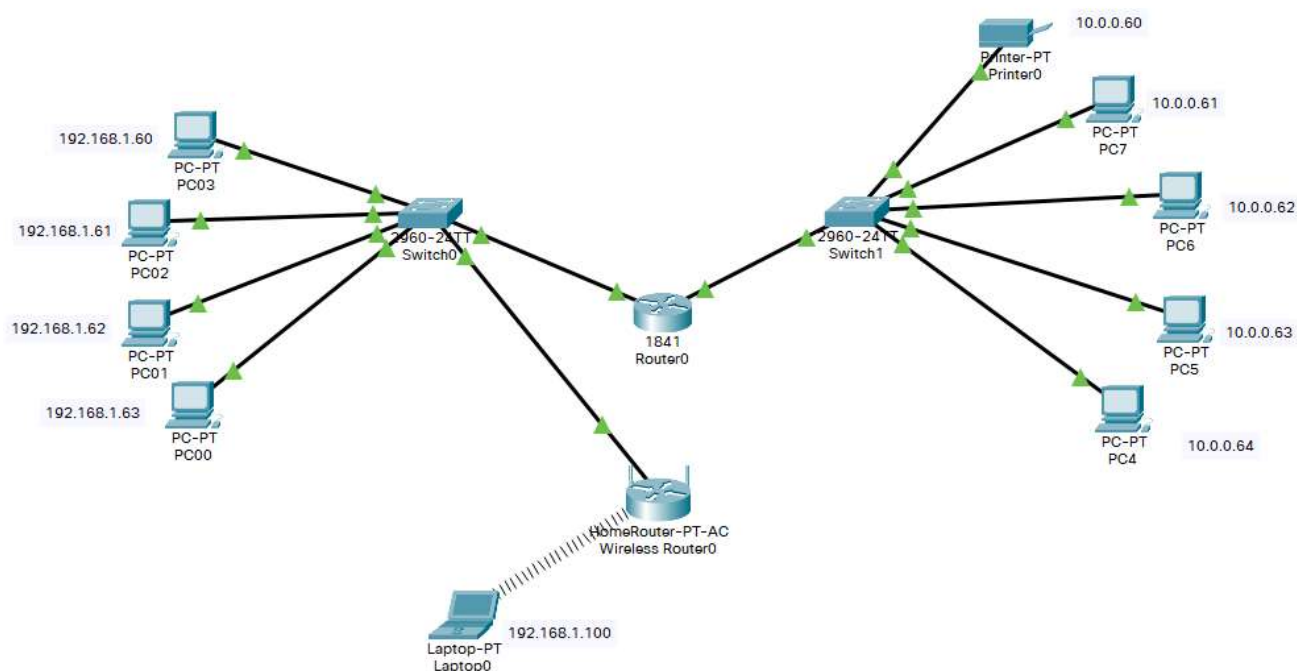


Imagen 4. Dispositivo con sus IP's

Como se ve, la repartición de ip's en la red de la derecha comenzó desde la 192.168.1.60, para el router inalámbrico comienza desde la 192.168.1.100 la cual esta asignada a la laptop. Para la red de la derecha se empezó a asignar desde la 10.0.0.60

2.3 CON LA AYUDA DEL COMANDO arp -a VERIFICAR LA TABLA DEL BUFFER DE ARP DE LA PC00, ESTO SE HACE CON LA AYUDA DE LA CONSOLA. TOMAR CAPTURA DE PANTALLA.

El comando arp nos permite crear, editar y mostrar las asignaciones de direcciones físicas a direcciones ip4v conocidas, en este caso arp-a, muestra todos los dispositivos que se encuentran actualmente en la cache arp del host, como se ve en la captura a continuación, se muestra la dirección ip, la mac y el tipo de direccionamiento.

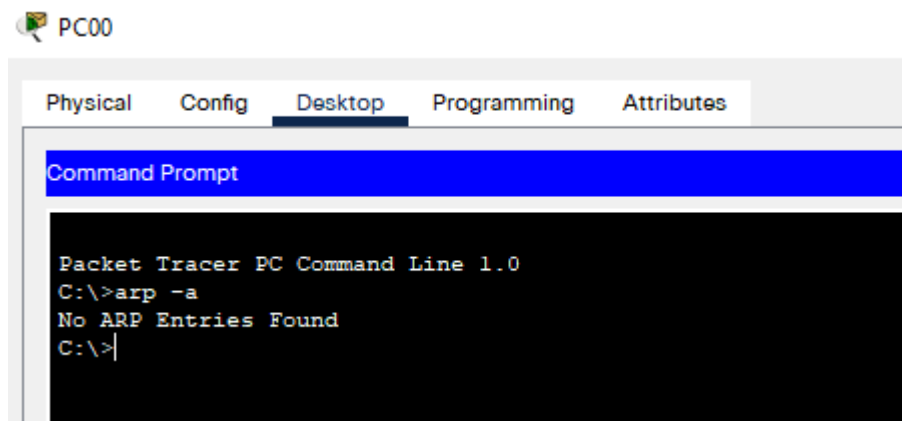


Imagen 5. Comando arp-a en PC00

Como vemos, esta computadora aún no tiene ninguna dirección.

2.4 DESDE LA PC00 HACER PING CON LA CONSOLA HACIA LA LAPTOP, TOMAR CAPTURA DE PANTALLA DEL RESULTADO.

En la siguiente imagen podemos ver el ping que se hace a la laptop desde la computadora pc00.

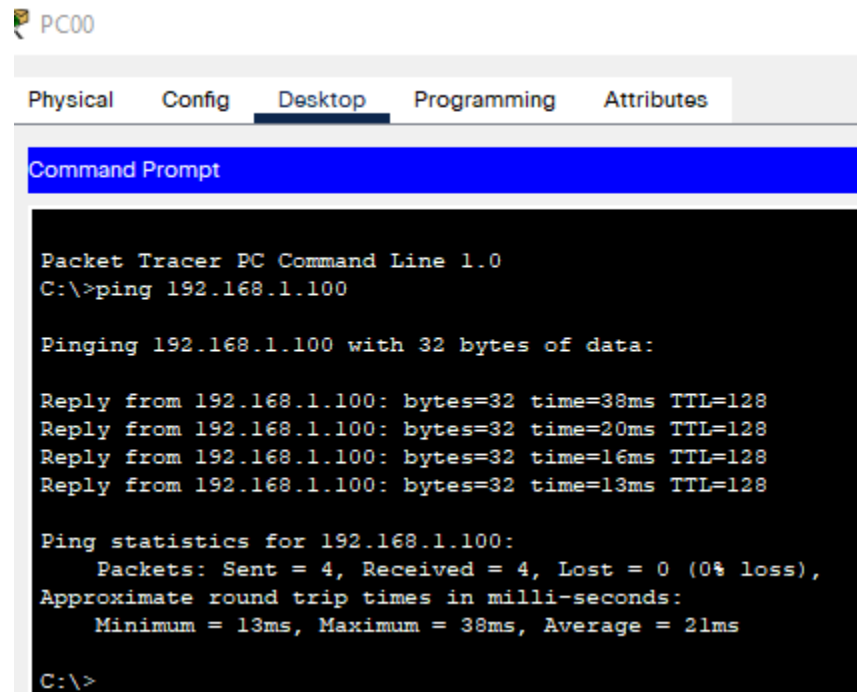


Imagen 6. Ping a la laptop

Como se ve en la imagen anterior la laptop recibe todos los paquetes sin error.

2.5 DESDE LA PC00 HACIA LA LAPTOP, CON LA AYUDA DE LA HERRAMIENTA ADD SIMPLE PDU, MANDAR UN PAQUETE DE PC00 A LA LAPTOP Y ABRIR EL MENU DE SIMULATION Y CONFIGURARLO DE ACUERDO CON EL VIDEO Y VERIFICAR CADA UNO DE LOS ENVIOS, VER LA TRAMA, TOMAR CAPTURA DE PANTALLA DE LAS TRAMAS TANTO DE LA SOLICITUD COMO DE LA RESPUESTA ARP.

en la imagen siguiente vemos a la configuración de los filtros del panel de simulación acorde al video.

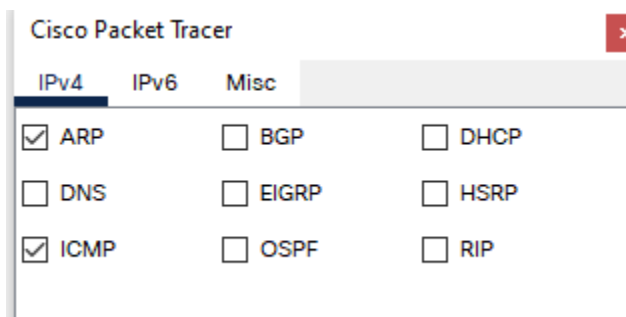


Imagen 7. Configuración filtros de simulación.

En la imagen siguiente imagen podemos ver que las únicas solicitudes y respuestas son ICMP, esto debido a que anteriormente hicimos un ping y la pc00 ya tiene en su buffer la dirección de la laptop.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC00	ICMP
	0.001	PC00	Switch0	ICMP
	0.002	Switch0	Wireless Ro...	ICMP
	0.003	Wireless Rout...	Laptop0	ICMP
	0.007	--	Laptop0	ICMP
	0.008	Laptop0	Wireless Ro...	ICMP
	0.009	Wireless Rout...	Switch0	ICMP
	0.009	--	Wireless Ro...	ICMP
	0.010	Wireless Rout...	Laptop0	ICMP
	0.010	Switch0	PC00	ICMP

Imagen 8. Panel de simulación

Ahora bien, analicemos esto mismo, pero sin que la dirección de la laptop este en la pc00, de esta forma se harán las solicitudes arp y sus correspondientes respuestas en cada paso de la simulación.

En la primera parte el mensaje se envía de la PC00 al switch, como podemos ver en la simulación se hace uso del protocolo ARP para traducir las direcciones IP a direcciones MAC, de esta forma se hace posible el envío de datos, pues este protocolo asigna su correspondiente dirección MAC a una dirección IP.

0.000	--	PC00	ICMP
0.000	--	PC00	ARP
0.001	PC00	Switch0	ARP

Imagen 9. Parte 1.

La trama capturada fue.

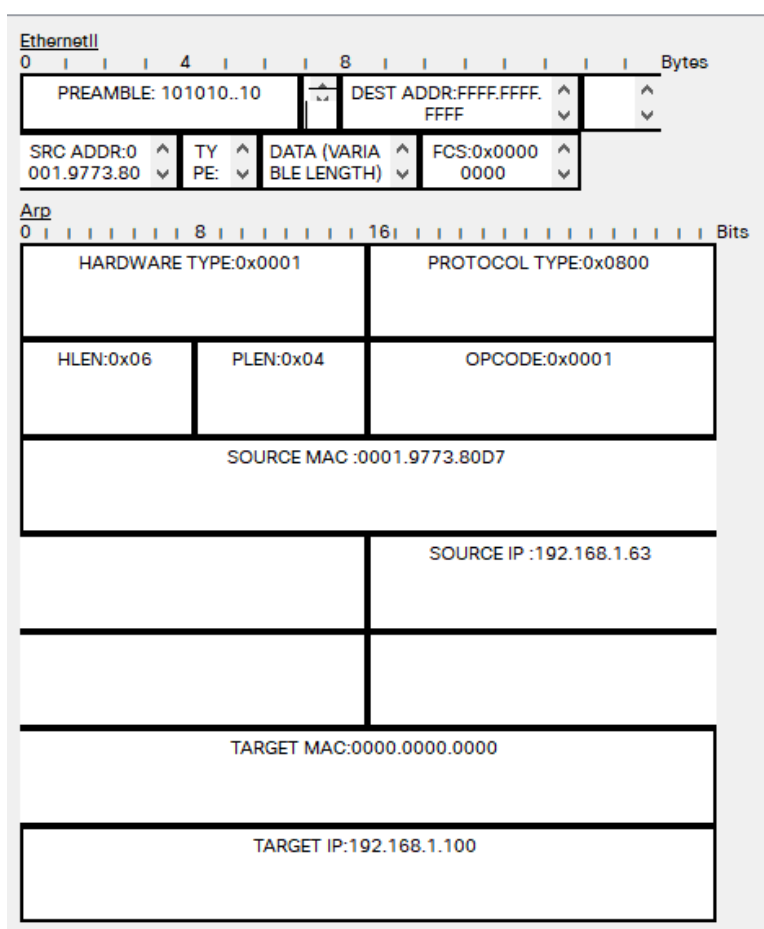


Imagen 10. Trama parte 1

Podemos ver que la dirección destino es una de broadcast, ya que el mensaje que se está enviando es de broadcast, de igual vemos la MAC origen que es la de la pc00. En el protocolo ARP podemos ver el que se tiene una IP objetivo, de la cual se obtendrá la mac más adelante.



	0.002	Switch0	PC03		ARP
	0.002	Switch0	PC02		ARP
	0.002	Switch0	PC01		ARP
	0.002	Switch0	Router0		ARP
	0.002	Switch0	Wireless Ro...		ARP

Imagen 11. Parte 2.

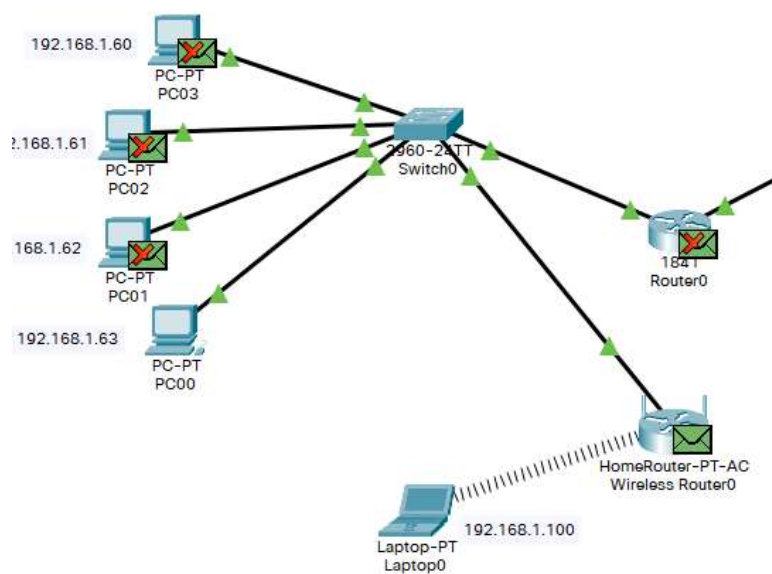


Imagen 12. Parte 2 de simulación.

En las dos imágenes anteriores vemos lo que sigue de la simulación, el switch se encarga de mandar el mensaje de la pc00 a los demás dispositivos de la red, pero al ser el mensaje de broadcast, los dispositivos a los que no va dirigido el mensaje lo ignoran, en esta parte nos interesa la trama capturada del switch al router inalámbrico, como vemos en la imagen 11, de igual forma hace uso del protocolo ARP.

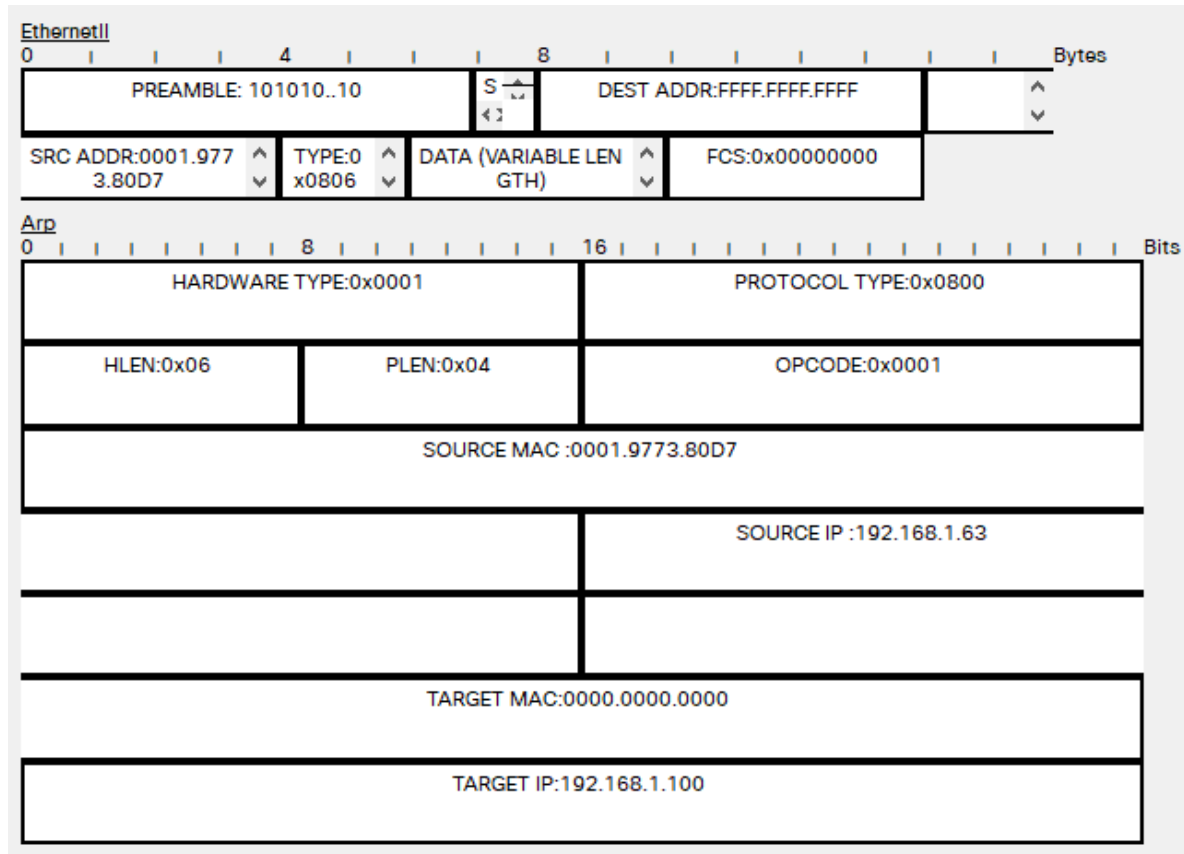


Imagen 13. Trama parte 2.

De igual forma a como sucedió en la parte 1, nos arroja la MAC destino que será de broadcast y el origen que es de la pc00, sin embargo aun no se sabe la dirección MAC de la IP objetivo. Para que no queden dudas se presenta a continuación la MAC de la pc00.

Device Name: PC00				
Device Model: PC-PT				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.1.63/24	<not set>	0001.9773.80D7
Bluetooth	Down	<not set>	<not set>	0001.64A4.79CA

Imagen 14. Mac pc00.

Posteriormente en la parte 3 del envío de datos se hace una solicitud del router inalámbrico a la laptop, hasta que la laptop da respuesta al protocolo.

0.003	Wireless Rout...	Laptop0	ARP
0.003	--	Wireless Ro...	ARP
0.004	--	Wireless Ro...	ARP
0.006	--	Wireless Ro...	ARP
0.007	--	Wireless Ro...	ARP
0.007	--	Wireless Ro...	ARP
0.011	--	Laptop0	ARP

Imagen 15. Parte 3.

De esta forma, revisaremos la trama arrojada por la última petición mostrada en la imagen 15, ya que esta es de la respuesta de la laptop.

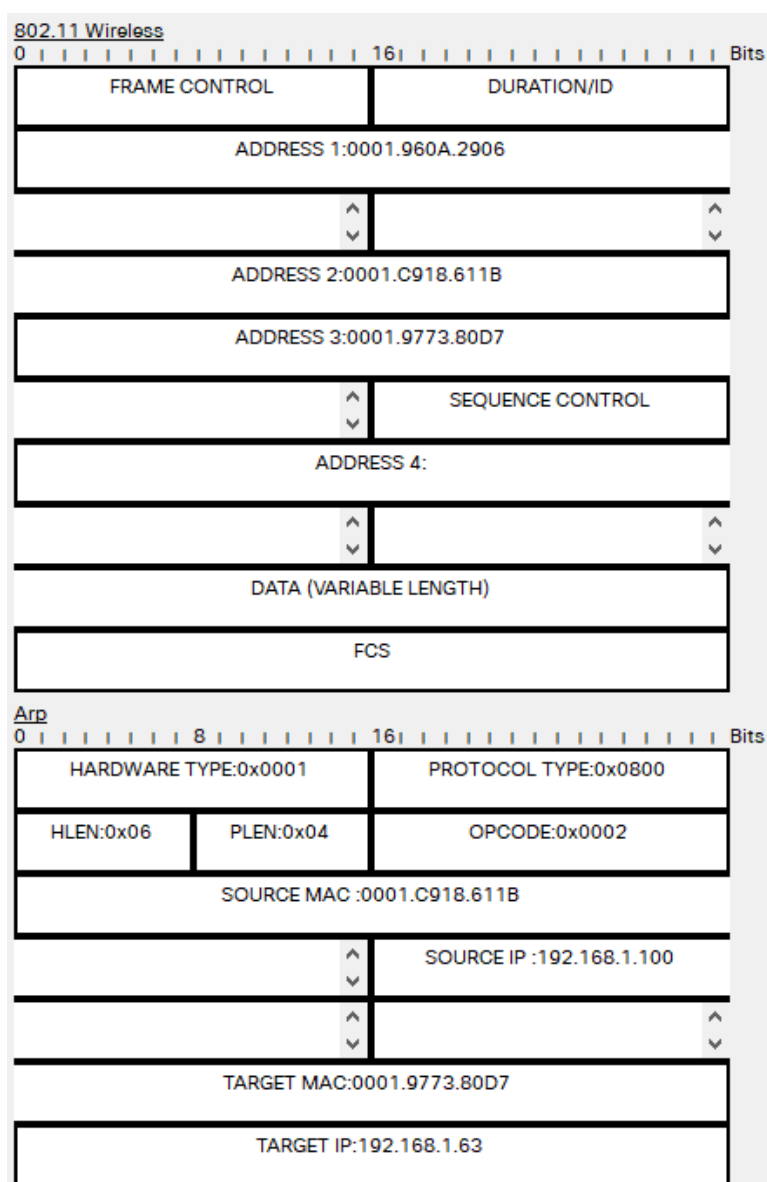


Imagen 16. Trama parte 3

En esta parte podemos ver en el apartado del protocolo ARP la respuesta que da la laptop, vemos que la laptop en este punto ya conoció la dirección MAC de la pc00, direcciones que se ven al final de la trama y que son las mismas de la imagen 14.

Posteriormente, esta respuesta de la laptop va hacia el router inalámbrico y hacia el switch, posteriormente del switch va a la pc00 usando el protocolo ICMP de esta forma se le indica a la pc00 el estado del mensaje y los nuevos detalles de este.

Laptop0	Wireless Ro...	ARP
Wireless Rout...	Switch0	ARP
Switch0	PC00	ARP
--	PC00	ICMP

Imagen 17. Parte 4

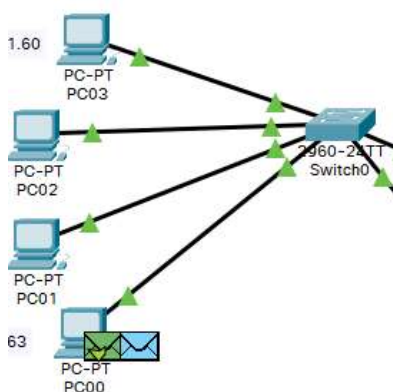


Imagen 18. Parte 4 del envío de datos.

La trama capturada que vamos a analizar es donde se hace uso del protocolo ICMP.

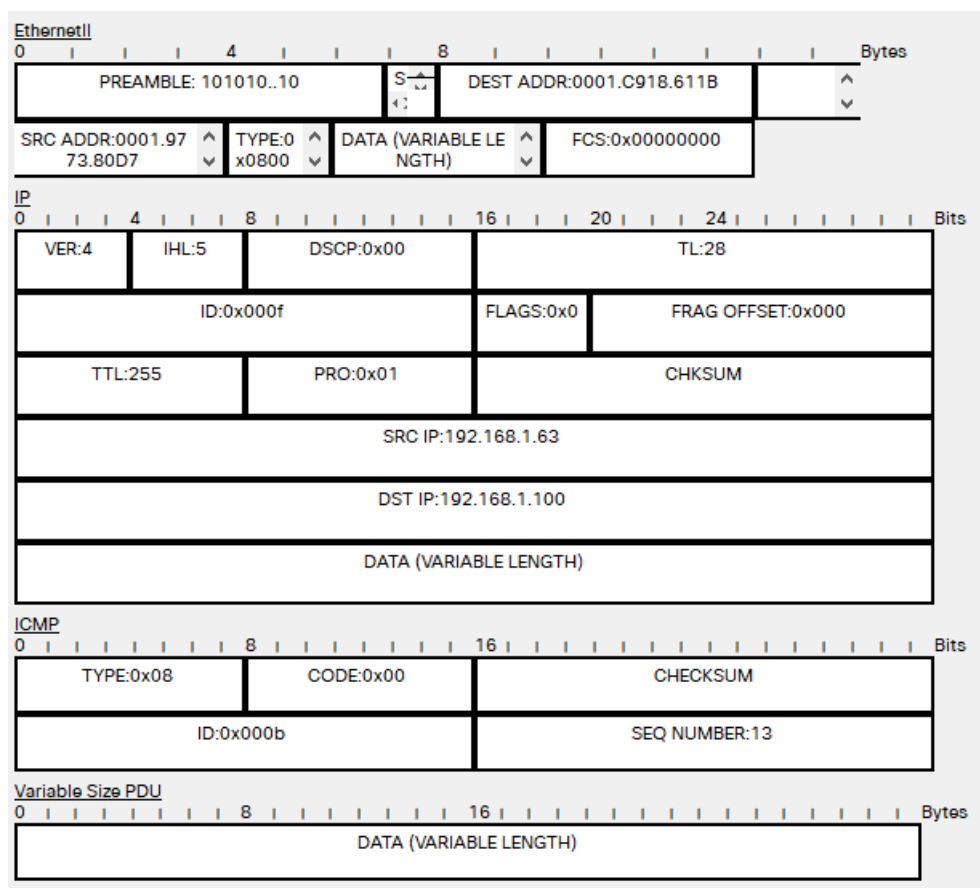


Imagen 19. Trama parte 4.

En esta trama podemos ver que la mac origen es la de la laptop y va dirigido a la pc00.

Finalmente una vez la laptop tiene en su cache la dirección de la pc00 y viceversa gracias al protocolo se hace el envío de datos correspondiente.

PC00	Switch0	ICMP
Switch0	Wireless Ro...	ICMP
--	Wireless Ro...	ARP
Wireless Rout...	Laptop0	ARP
--	Wireless Ro...	ICMP
Wireless Rout...	Laptop0	ICMP
--	Laptop0	ICMP
Laptop0	Wireless Ro...	ICMP
Wireless Rout...	Switch0	ICMP
Switch0	PC00	ICMP
--	Wireless Ro...	ICMP
Wireless Rout...	Laptop0	ICMP

Imagen 20. envío de datos exitoso.

Vemos que en la barra inferior nos muestra que el mensaje ha sido exitoso.


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC00	Laptop0	ICMP		0.000	N	0	(edit)	

Imagen 21. Envío exitoso

2.6 DE NUEVO EN LA CONSOLA DE LA PC00 EJECUTAR EL COMANDO arp -a TOMAR CAPTURA DE PANTALLA DEL BUFER ARP.

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.100         0001.c918.611b        dynamic
```

Imagen 22. arp -a en la pc00

Podemos ver en la imagen anterior que al hacer él envió la pc00 ya tiene en su cache de ARP la memoria MAC de la laptop, de esta forma le será posible enviar datos sin problemas. Como vimos en el punto anterior esto fue gracias al protocolo ARP.

En la imagen siguiente se corrobora la MAC de la laptop.

```
Device Name: Laptop0
Device Model: Laptop-PT

Port      Link   IP Address      IPv6 Address      MAC Address
Wireless0 Up      192.168.1.100/24 <not set>         0001.C918.611B
```

Imagen 23. MAC de la laptop

2.7 AHORA REPETIR EL PUNTO 2,4 PERO AHORA DESDE LA PC03 A LA PC4 Y EXPLIQUEN QUE PASA Y POR QUE, TOMAR CAPTURA DE PANTALLA.

En la imagen siguiente podemos ver el ping que hacemos desde la pc03 hacia la pc4.

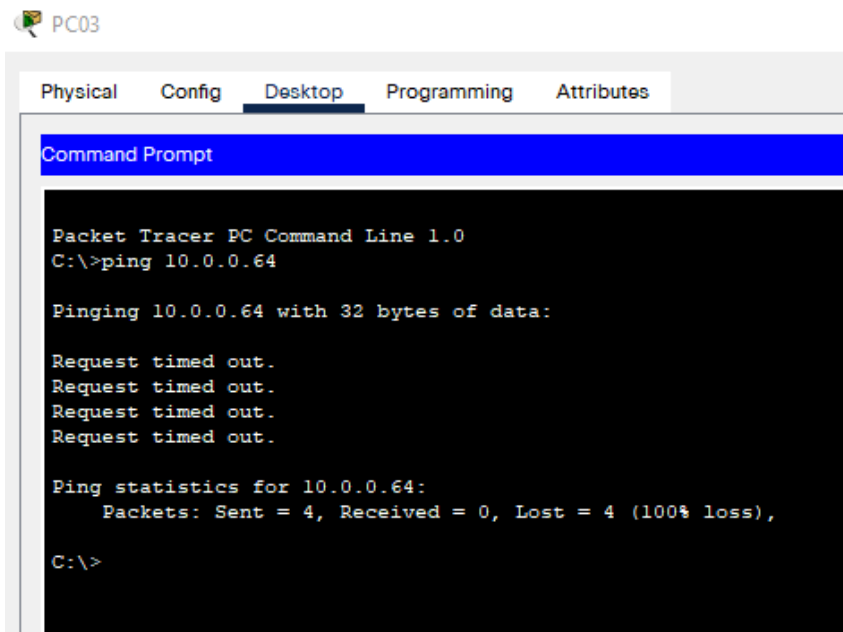


Imagen 24. Ping de pc03 a pc4.

Vemos que no podemos hacer ping a esa red, ya que no podemos mandar mensaje a equipos de otras redes, esto porque ARP solo nos sirve para mi segmento de red, es decir, mi dominio de broadcast y no otro, al ser la red de la derecha una red distinta, no es posible mandar datos.

2.8 BORRE EL BUFER DE CADA UNA DE LAS PCS QUE YA TENGAN GUARDADA LA TABLA DE ARP. TOMAR CAPTURA DE PANTALLA

PC00

En la imagen siguiente primer ejecutamos el comando arp -a para ver las direcciones que tiene en la tabla de arp para posteriormente borrarla.

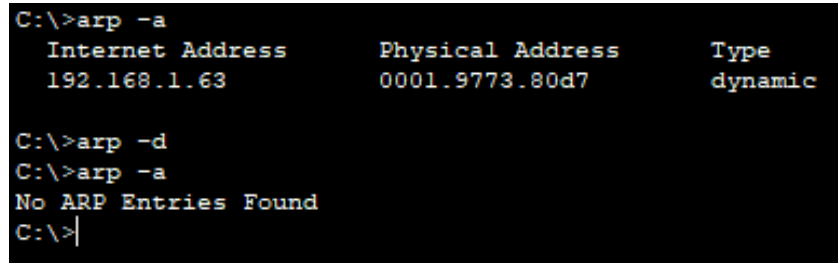
```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.100         0001.c918.611b        dynamic

C:\>arp -d
C:\>arp -a
No ARP Entries Found
```

Imagen 25. arp -d en pc00

LAPTOP

Ahora hacemos lo mismo con la laptop



```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.63          0001.9773.80d7        dynamic

C:\>arp -d
C:\>arp -a
No ARP Entries Found
C:\>|
```

Imagen 26. arp -d en laptop

2.6 EXPLIQUE LA UTILIDAD DEL PROTOCOLO ARP E ICMP EN LOS ENVIOS EN BASE A ESTAS CONSIDERACIONES TEORICAS

ARP

Se utiliza para supervisar y modificar la tabla de asignación de direcciones IP y MAC.

ARP utiliza un cache que consiste en una tabla que almacena las asignaciones entre la capa de enlace de datos y las direcciones IP en la capa de red

La capa de enlace de datos se encarga de gestionar las direcciones MAC

ARP asocia las direcciones IP a las direcciones MAC justo a la inversa del protocolo RARP,

el tiempo predeterminado de duración de la cache es de 60 segundos y después de ese tiempo se actualiza

RARP asocia las direcciones MAC a las direcciones IP

ICMP

los routers utilizan esta implementación del protocolo IP para devolver mensajes sobre problemas con datagramas al remitente del paquete.

para intercambiar datos de estado o mensajes de error

el protocolo ICMP es esencial para la comunicación en redes IP,

Gracias al protocolo arp podemos conocer la dirección mac de un dispositivo de nuestra red a partir de su ip, de esta forma podemos hacer envío de datos, es decir, establecer comunicación entre los dispositivos de la red.

El protocolo icmp también es fundamental para la comunicación en redes ip, con este protocolo podemos saber y comprobar la accesibilidad de un determinado host en la red, de esta forma sabemos si es posible entablar comunicación entre distintos equipos. De igual forma los routers usan este protocolo para informar a los equipos de la red la situación y datos de la red.

3. CONCLUSIONES INDIVIDUALES DE CADA PARTICIPANTE DEL EQUIPO

FISCHER SALAZAR CÉSAR EDUARDO

En esta práctica cambiamos la programación por la simulación de una red con una topología propuesta que nos permitiera conocer el funcionamiento del protocolo ARP y ICMP, en el que pudimos observar sus características de cada protocolo.

El ARP nos permitía realizar una petición a todas las máquinas buscando la dirección del dispositivo terminal destino pues al desconocerse la dirección IP este protocolo permite conocer esta información a través de su MAC asociada que nos establecerá una conexión estos dispositivos.

Por otra parte, observe que el protocolo ICMP solamente nos informaba sobre las incidencias que podrían presentarse en la entrega de paquetes o de errores en nuestra red.

Una práctica interesante que nos permite ver en acción más protocolos que nos proporcionan comunicación entre elementos terminales de una topología distinta.

LÓPEZ GARCÍA JOSÉ EDUARDO

Con ayuda de esta práctica y de la herramienta de simulación del Cisco Packet Tracer, se pudo tener una visualización en entorno virtual del funcionamiento del protocolo ARP a través de la topología propuesta.

Por medio de esta interacción se observó la funcionalidad completa de este protocolo en la topología, al ver que los paquetes se enviaron de forma correcta, haciendo comprender que la comunicación entre los dispositivos de la topología se encuentra en orden.

Así, con la asistencia de la información de red (IP, MAC de origen y destino, tipo de mensaje ARP) se vio el encapsulamiento de la trama para poder realizar el envío de mensajes ARP que solamente recibe el dispositivo que envíe esa solicitud ARP y lo irá añadiendo a una tabla ARP. Esto puede significar una pequeña desventaja de este protocolo, debido a que no es la ideal al querer buscar comunicación en otros dispositivos.

En general, fue de mucha ayuda observar en acción todos los elementos que dispone el uso de este protocolo dentro de la herramienta de Packet Tracer y cuándo emplearlo para futuras prácticas.

MEZA VARGAS BRANDON DAVID

Gracias a esta práctica comprendí de mejor manera la utilidad del protocolo ARP e ICMP aplicados a una red como se vio en este caso con la red construida en cisco packet tracer.

Concluyendo así que gracias al protocolo ARP e ICMP podemos hacer posible las comunicaciones entre los dispositivos de la red, el protocolo ARP por su parte se encarga de conocer la dirección MAC asociada a una dirección IP, colocando estos datos en una tabla cache de ARP, de esta forma para comunicaciones futuras ya sabrá la MAC e IP del dispositivo al que se quieren comunicar y viceversa.

Por su parte el protocolo ICMP brinda información de la red en cuestión y brinda el estado igual de la red a los dispositivos pertenecientes a la red.

Es de considerarse la situación que pasa con el protocolo ARP con otras redes, pues como vimos en la práctica, el protocolo ARP no es útil cuando queremos comunicar equipos de redes diferentes.

Sin duda una práctica de utilidad para saber el uso y funcionamiento del protocolo ARP e ICMP gracias a las herramientas que nos brinda packet tracer como lo es el apartado de simulación.