



Universidad Nacional
ARTURO JAURETCHE

Informe – Redes de Computadoras I

Primer Cuatrimestre del año 2020

Comisión: 2

Profesor: Román Bond

Alumno: Federico Almada

Contenido

1. Introducción.....	3
2. Objetivos específicos	3
3. Descripción de las redes.....	4
3.1 Descripción de la red A	4
3.2 Descripción de la red B	6
4. Tareas realizadas y resultados.....	7
4.1 Pruebas en la red A.....	7
4.2 Pruebas en la red B.....	9
5. Conclusiones.....	11
6. Anexo	12
6.1 Packet Tracer	12
7. Bibliografía.....	12

1. Introducción

El presente informe es un Trabajo Práctico Final de la materia Redes de Computadoras I, el objetivo del mismo es presentar el desarrollo e implementación de dos redes de computadoras, así como también, mostrar las tareas realizadas y resultados obtenidos con las mismas. Para ello, se mostrará una descripción de cada una de las redes con información detallada de la configuración realizada, luego, se mostrará la implementación de cada red en un software de diseño y simulación de redes, y además se expondrán los problemas que surgieron a lo largo de la implementación y como éstos fueron solucionaron.

2. Objetivos específicos

- Calcular direcciones IP de manera manual, realizando “subnetting”.
- Simular la red en Packet Tracer.
- Asignar direccionamiento IP estático a cada dispositivo.
- Analizar el funcionamiento de la capa de red.
- Analizar el funcionamiento de la capa de enlace.
- Profundizar los conceptos referidos a cada capa.
- Visualizar el comportamiento del protocolo ICMP y ARP.

3. Descripción de las redes

3.1 Descripción de la red A

La red A es una red compuesta por 8 subredes creadas a partir de la dirección 214.97.192.0/22. A continuación, se mostrarán las especificaciones:

Especificaciones

- Subred con capacidad para conectar 500 dispositivos.
- Subred con capacidad para conectar 120 dispositivos.
- Subred con capacidad para conectar 120 dispositivos.
- Subred con capacidad para conectar 60 dispositivos.
- Subred con capacidad para conectar 28 dispositivos.
- Subred con capacidad para conectar 28 dispositivos.
- Subred con capacidad para conectar 12 dispositivos.
- Subred con capacidad para conectar 12 dispositivos.

Para hacerla lo más optima posible, se calcularon las subredes de manera contiguas. En la Tabla 1 se muestra las configuraciones de cada dispositivo. En la Tabla 2 se observa cada una de las interfaces.

Dispositivo	Subred	IP	Máscara	Gateway	Broadcast
PC0	214.97.192.0/23	214.97.192.2	255.255.254.0	214.97.192.1	214.97.193.255
PC1	214.97.192.0/23	214.97.192.254	255.255.254.0	214.97.192.1	214.97.193.255
PC2	214.97.194.0/25	214.97.194.2	255.255.255.128	214.97.194.1	214.97.194.127
PC3	214.97.194.0/25	214.97.194.126	255.255.255.128	214.97.194.1	214.97.194.127
PC4	214.97.194.128/25	214.97.194.130	255.255.255.128	214.97.194.129	214.97.194.255
PC5	214.97.194.128/25	214.97.194.254	255.255.255.128	214.97.194.129	214.97.194.255
PC6	214.97.195.0/26	214.97.195.2	255.255.255.192	214.97.195.1	214.97.195.63
PC7	214.97.195.0/26	214.97.195.62	255.255.255.192	214.97.195.1	214.97.195.63
PC8	214.97.195.64/27	214.97.195.66	255.255.255.224	214.97.195.65	214.97.195.95
PC9	214.97.195.64/27	214.97.195.94	255.255.255.224	214.97.195.65	214.97.195.95
PC10	214.97.195.96/27	214.97.195.98	255.255.255.224	214.97.195.97	214.97.195.127
PC11	214.97.195.96/27	214.97.195.126	255.255.255.224	214.97.195.97	214.97.195.127
PC12	214.97.195.128/27	214.97.195.130	255.255.255.240	214.97.195.129	214.97.195.143
PC13	214.97.195.128/28	214.97.195.142	255.255.255.240	214.97.195.129	214.97.195.143
PC14	214.97.195.144/28	214.97.195.146	255.255.255.240	214.97.195.145	214.97.195.159
PC15	214.97.195.144/28	214.97.195.158	255.255.255.240	214.97.195.145	214.97.195.159

Tabla 1: Configuraciones de cada dispositivo en la red A

Dispositivo	Interfaz	Subred	IP	Máscara	Broadcast
Router1	Ethernet0	200.12.13.0/24	200.12.13.1	255.255.255.0	200.12.13.255
Router1	FastEthernet1	214.97.192.0/23	214.97.192.1	255.255.254.0	214.97.193.255
Router1	FastEthernet2	214.97.194.0/25	214.97.194.1	255.255.255.128	214.97.194.127
Router1	FastEthernet3	214.97.194.128/25	214.97.194.129	255.255.255.128	214.97.194.255
Router1	FastEthernet4	214.97.195.0/26	214.97.195.1	255.255.255.192	214.97.195.63
Router1	FastEthernet5	214.97.195.64/27	214.97.195.65	255.255.255.224	214.97.195.95
Router1	FastEthernet6	214.97.195.96/27	214.97.195.97	255.255.255.224	214.97.195.127
Router1	FastEthernet7	214.97.195.128/28	214.97.195.129	255.255.255.240	214.97.195.143
Router1	FastEthernet8	214.97.195.144/28	214.97.195.145	255.255.255.240	214.97.195.159

Tabla 2: Interfaces del router de frontera de la red A

Como se pudo apreciar en la tabla anterior, en la interfaz Ethernet0 del router de frontera se encuentra una red externa con la dirección 200.12.13.0/24. Esta red externa tiene un servidor web alojado en el que se harán distintas pruebas.

3.2 Descripción de la red B

La red B es una red de tipo LAN que en principio cuenta con 15 dispositivos, entre ellos dos servidores, pero a futuro la red tiene pensado extenderse un 50%.

$$\text{Hosts estimados} \rightarrow 15 \cdot 1.5 = 22,5 \text{ hosts}$$

En base al cálculo realizado, para optimizar la eficiencia de la red, se estimó que será necesario configurar la red con capacidad para 23 direcciones privadas para dispositivos. Con el siguiente calculo se obtendrá la cantidad de direcciones IP utilizables para dispositivos:

$$2^5 - 2 = 30 \text{ hosts para la red B}$$

“LAN (Local Area Networking): Una red LAN o de área local es una conexión de dispositivos dentro de un área específica. Cada dispositivo se denomina nodo de la red y está conectado al servidor. Aunque no hay un límite máximo claro para lo que se puede considerar una LAN, esta red cubre típicamente un área pequeña, como una sola oficina, un edificio, o unos pocos edificios en un área”.

En la Tabla 3 se muestra las configuraciones de cada dispositivo en la red B.

Dispositivo	Subred	IP	Máscara	Gateway	Broadcast
Server0	192.168.0.0/27	192.168.0.2	255.255.255.224	192.168.0.1	192.168.0.31
Server1	192.168.0.0/27	192.168.0.3	255.255.255.224	192.168.0.1	192.168.0.31
PC0	192.168.0.0/27	192.168.0.4	255.255.255.224	192.168.0.1	192.168.0.31
PC1	192.168.0.0/27	192.168.0.5	255.255.255.224	192.168.0.1	192.168.0.31
PC2	192.168.0.0/27	192.168.0.6	255.255.255.224	192.168.0.1	192.168.0.31
PC3	192.168.0.0/27	192.168.0.7	255.255.255.224	192.168.0.1	192.168.0.31
PC4	192.168.0.0/27	192.168.0.8	255.255.255.224	192.168.0.1	192.168.0.31
PC5	192.168.0.0/27	192.168.0.9	255.255.255.224	192.168.0.1	192.168.0.31
PC6	192.168.0.0/27	192.168.0.10	255.255.255.224	192.168.0.1	192.168.0.31
PC7	192.168.0.0/27	192.168.0.11	255.255.255.224	192.168.0.1	192.168.0.31
PC8	192.168.0.0/27	192.168.0.12	255.255.255.224	192.168.0.1	192.168.0.31
PC9	192.168.0.0/27	192.168.0.13	255.255.255.224	192.168.0.1	192.168.0.31
PC10	192.168.0.0/27	192.168.0.14	255.255.255.224	192.168.0.1	192.168.0.31
PC11	192.168.0.0/27	192.168.0.15	255.255.255.224	192.168.0.1	192.168.0.31
PC12	192.168.0.0/27	192.168.0.16	255.255.255.224	192.168.0.1	192.168.0.31

Tabla 3: Configuraciones de cada dispositivo en la red B

Además de la red LAN, también se encuentra conectado al router una red externa en una de sus interfaces, como se muestra en la Tabla 4.

Dispositivo	Interfaz	Subred	IP	Máscara	Broadcast
Router0	FastEthernet0	222.222.22.192/29	222.222.22.193	255.255.255.248	222.222.22.199
Router0	FastEthernet1	192.168.0.0/27	192.168.0.1	255.255.255.224	192.168.0.31

Tabla 4: Interfaces del router de frontera de la red B

4. Tareas realizadas y resultados

4.1 Pruebas en la red A

Una vez realizado el “subneteo” de todas las direcciones correspondientes a cada subred en la red A. Lo que se hizo fue diseñar toda la red en Cisco Packet Tracer (en el Anexo se tendrá información detallada sobre este software), para luego implementar las configuraciones técnicas de cada dispositivo. En la Figura 1 se puede observar como quedó el diseño de la red A. Luego de terminar la configuración de todos los dispositivos en la red, se hicieron algunas pruebas, a continuación, los resultados:

En la primera prueba, se hizo un Ping mediante consola desde el primer terminal disponible de la primera subred (PC0) hasta el último terminal de la misma subred, los resultados fueron los esperados, luego, para comprobar si existía conexión entre cada terminal de las distintas subredes, se realizó un Ping desde PC0 hasta el primer terminal de cada subred, el resultado fue el siguiente:

```
C:\>ping 214.97.194.2 -n 2

Pinging 214.97.194.2 with 32 bytes of data:

Reply from 214.97.194.2: bytes=32 time<1ms TTL=127
Reply from 214.97.194.2: bytes=32 time<1ms TTL=127

Ping statistics for 214.97.194.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 214.97.194.130 -n 2

Pinging 214.97.194.130 with 32 bytes of data:

Reply from 214.97.194.130: bytes=32 time<1ms TTL=127
Reply from 214.97.194.130: bytes=32 time<1ms TTL=127

Ping statistics for 214.97.194.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 214.97.195.2 -n 2

Pinging 214.97.195.2 with 32 bytes of data:

Reply from 214.97.195.2: bytes=32 time=15ms TTL=127
Reply from 214.97.195.2: bytes=32 time<1ms TTL=127

Ping statistics for 214.97.195.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 7ms
```

Captura 1

Como se puede ver en la Captura 1, cada nodo responde al Ping realizado desde el terminal PC0, eso demuestra que la primera prueba realizada salió exitosa.

En la siguiente prueba, se envió un mensaje desde PC0 a cualquier otro nodo. En esta prueba ocurrió el primer error, aunque en realidad no era un error de implementación, sino, de un protocolo.

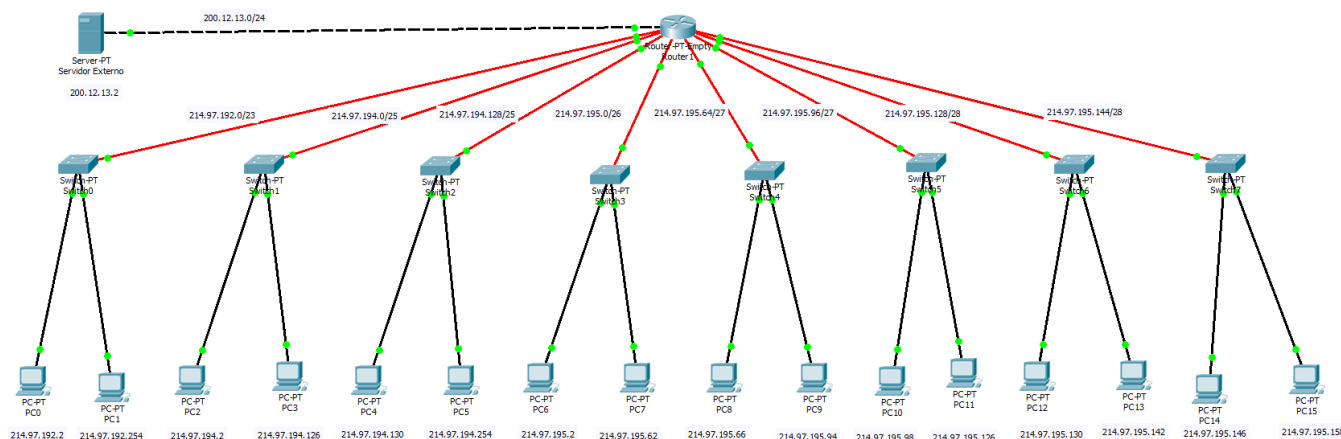


Figura 1: Diseño de la red A

El problema fue el siguiente, se intentó enviar un mensaje desde PC0 hasta PC2. Cuando parecía que todo iba saliendo bien, la comunicación no se pudo realizar. En la Captura 2 se muestra el falló que apareció.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC0	PC2	ICMP		0.000	N	50
	Successful	PC0	PC2	ICMP		0.000	N	51
	Successful	PC0	PC4	ICMP		0.000	N	52

Captura 2

Sin embargo, cuando se volvió a realizar la prueba, el mensaje llegaba correctamente desde PC0 hasta PC2. Entonces algo raro estaba pasando. El problema finalmente era debido a las tablas ARP, las cuales estaban vacías al principio, por lo tanto, la comunicación era rechazada. Cuando se realizó el segundo intento con los mismos terminales, la comunicación se concretó ya que las tablas ARP se habían mapeado, es decir, existía una entrada con las direcciones IP y MAC respectivas a cada dispositivo. El protocolo ARP se va a profundizar más en la red B.

Una vez hecha la prueba de simulación de mensajes desde cada nodo de la red. Lo último que se probó fue abrir la página del servidor web que se encuentra ubicado en una red externa con la dirección IP 200.12.13.2. El mismo, se encuentra conectado en la primera interface del router de frontera, por lo tanto, debe ser accesible desde los disantos nodos de la red A. En la Captura 3 se puede apreciar como desde un nodo de la red A se puede acceder a la página web del servidor externo.



Captura 3

Se probó acceder a la página web del servidor externo en cada nodo de la red A desde el navegador de cada terminal, y salió el “hello world”. Lo cual demuestra que se ha configurado bien el servidor.

4.2 Pruebas en la red B

Luego de la implementación (en la Figura 2 se muestra el diseño de la red B) y configuración de toda la red B se realizaron las siguientes pruebas:

En primer lugar, en el modo Simulación del Packet Tracer, se hizo un filtrado de protocolos para que se mostraran solamente los mensajes del protocolo ARP.

Protocolo ARP: “almacena en una tabla local las correspondencias entre las direcciones IP y las direcciones MAC. A esta tabla se le conoce con el nombre de “caché ARP” o tabla de resolución de direcciones. Esta tabla es temporal, es decir, se crea nueva cada vez que se activa el sistema, y se rellena dinámicamente con las asociaciones entre direcciones IP y MAC que se obtienen al aplicar el protocolo ARP”.

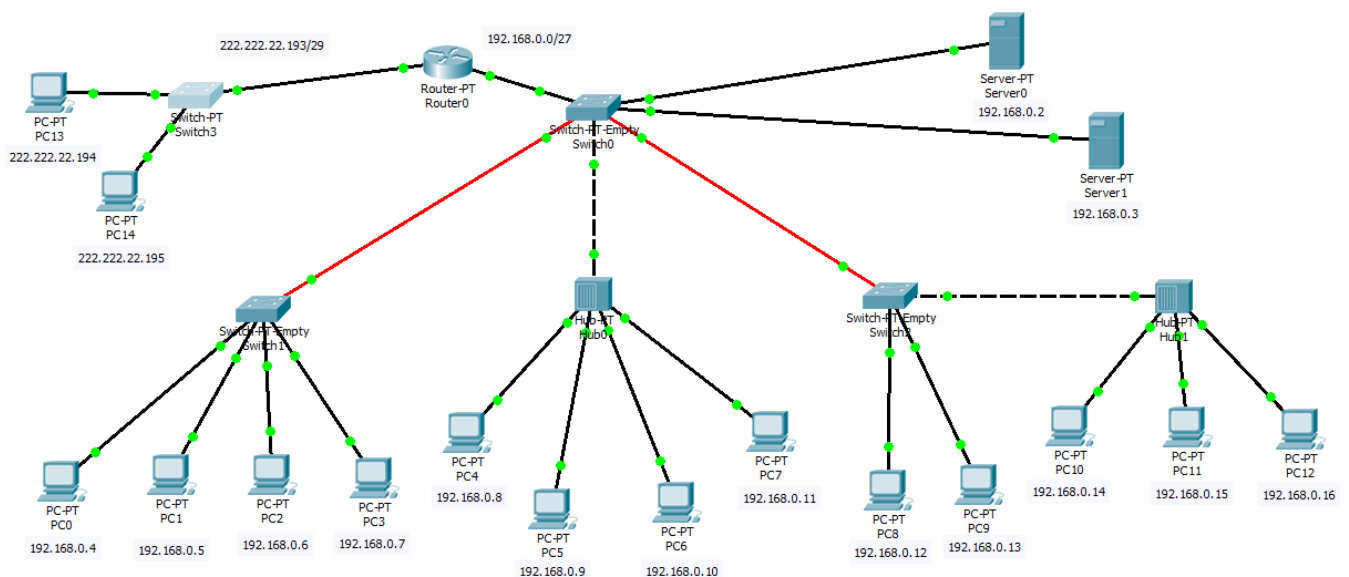


Figura 2: Diseño de la red B

Antes de empezar con la prueba, se explicará brevemente porqué se utiliza este protocolo. Básicamente las direcciones IP no conocen el hardware o la MAC del nodo destino al cual se quiere enviar un mensaje. ARP es la solución a este problema. Por eso es fundamental en la capa de enlace.

Ahora se pasará a explicar la primera prueba:

El primer paso fue enviar un mensaje desde PC0 a PC4 (en la Captura 4 se ve el estado inicial de la tabla ARP en PC0), desde PC0 el mensaje llegó al Switch1, el switch como todas las tablas ARP están vacías, Switch1 envió un mensaje a todos los enlaces conectados a él (PC1, PC2, PC3 y Switch0), como el mensaje no es para ninguno de los enlaces que recibieron el mensaje, entonces lo rechazan, excepto el Switch0, ya que como todo switch cuando tiene sus tablas ARP vacías, recibe el mensaje y lo envía a todos sus enlaces, excepto el enlace desde donde recibió el mensaje. Switch0 envía a todos sus enlaces, todos lo rechazan, excepto Hub0, como todo hub acepta el mensaje y lo amplifica a todos sus enlaces. Una vez que los nodos conectados al hub recibieron el mensaje, el único nodo que lo acepta es PC4, el nodo destino.

```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

Captura 4

Luego el proceso de que los switch llenaron sus tablas ARP, el proceso de vuelta fue más directo. PC4 devuelve el mensaje, pasando el mensaje primero por el Hub0, el hub lo amplifica nuevamente a todos los enlaces, el único que acepta es Switch0, el switch como ya tiene asignada sus tablas ARP, conoce donde se ubica el destino PC0, entonces Switch0 le envía el mensaje a Switch1 y este último le hace llegar el mensaje a PC0. (En la captura 5 se ve el estado de la tabla ARP de PC0 al recibir el mensaje de PC4).

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.0.8           00e0.f765.e2a4        dynamic
```

Captura 5

La siguiente prueba fue hacer un Ping desde cualquier nodo y ver como se completa las tablas ARP. Para esto se tuvo que filtrar el protocolo ICMP, el cual es utilizado generalmente para enviar mensajes y verificar si dos nodos tienen comunicación entre sí.





Después de filtrar para que se visualice solo el protocolo ICMP, se probó hacer un Ping desde PC4 a un nodo de la red externa 222.222.22.193/22. El router rechazó el envío y no llegó a destino. PC4 agregó a su tabla ARP la entrada de el Gateway como se puede apreciar en la Captura 6.

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.0.1           0001.97e4.0944       dynamic
192.168.0.4           0001.974b.d08c       dynamic
```

Captura 6

Luego se reintentó hacer el ping entre los mismos nodos y se concretó la conexión como se ve en la captura 7. Se llegó a la conclusión de que cuando se hace un Ping por primera vez a un nodo donde no se tenga agregado en la entrada de la tabla ARP, entonces se inunda la red con el fin de llenar las tablas y así cuando se vuelve a enviar otro ping ya se pueda establecer la conexión.

El Hub, sin embargo, al trabajar en capa física no tiene inteligencia como el switch para auto aprender y no volver a inundar sus enlaces.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	I
	Failed	PC4	PC13	ICMP		0.000	N	0	
	Successful	PC4	PC13	ICMP		0.000	N	1	

Captura 7

5. Conclusiones

En síntesis, se enfocó en el diseño de redes lo más contiguas posibles, de tal forma que sobren direcciones para futuras subredes y se estimó la cantidad de direcciones IP utilizables para dispositivos de acuerdo a las necesidades y especificaciones de cada red.

Durante la implementación en el software de simulación y diseño de redes Packet Tracer se pudo apreciar mejor el funcionamiento del protocolo ICMP y el protocolo ARP. También se pudo ver la diferencia entre un Hub y un Switch, el switch inunda la red cuando las tablas están vacías, en cambio, el hub amplifica la señal que recibe hacia todos sus enlaces.

Hoy en día es muy común utilizar switches en lugar de hubs, aunque en algunas empresas, aún se utilizan para enviar un mensaje a todos los nodos.

Por último y no menos importante, gracias a este trabajo práctico se lograron solidificar los conceptos adquiridos durante toda la cursada. En el desarrollo de la red A se profundizaron los conceptos a nivel capa de red y en cuanto a la red B se profundizaron los conceptos a nivel capa de enlace.

6. Anexo

6.1 Packet Tracer

Es una herramienta poderosa para realizar simulaciones de redes informáticas. Permite realizar prácticas simples y complejas en una variedad de dispositivos más allá de enrutadores y conmutadores. Permite también crear soluciones que estén interconectadas para ciudades inteligentes, hogares y empresas.

7. Bibliografía

- [1] – “Cisco Networking Academy – Packet Tracer” <https://www.netacad.com/courses/packet-tracer>
- [2] – “Speedcheck – LAN” <https://www.speedcheck.org/es/wiki/lan/>