UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

Laboratorio 1: Capa de enlace

Integrantes:	Alex Muñoz
	Alberto Rodríguez
Curso:	Sistemas de Comunicación
Sección	0-L-1
Profesor:	Carlos González
Ayudante:	Catalina Morales

5 de Junio de 2020

Tabla de contenidos

1. Introducción

Dentro de la informática y la telecomunicación, existen protocolos de comunicaciones, estas consisten como un conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre sistemas, en palabras más simples, se puede definir como el "idioma" en el se comunican computadores dentro de una misma red. Algunos de ellos son el modelo OSI y el modelo TCP/IP, los cuales están compuestos por capas, cada una con funcionalidades específicas. este laboratorio se centra en una, la capa de enlace.

La capa de enlace es la responsable de llevar la transferencia fiable de datos, libre de errores además del control del flujo de la información. El contexto de la capa de enlace nos dice que los frames o tramas viajan de un nodo de origen a un nodo destinos en el que ambos están conectados físicamente entre si.

El objetivo principal es poder aprender como funciona el envió de datos y el funcionamiento de distintos protocolos a través de la capa de enlace. Explicado esto mas detalladamente, es poder comprender quienes están conectados a una red local, cuales son sus direcciones, que tecnología y protocolos de capa física utilizan, la velocidad a la que realizan el envió de datos. Además de analizar con detalle el protocolo ARP y su funcionamiento dentro de la red local.

Para poder desarrollar todo lo anterior a cabo, se utilizan diversas herramientas de análisis de redes. Estas son:

- nmap: Se utiliza para averiguar la topología de la red (es decir, que computadores están activos en la red local, que puertos están abierto y que servicios hay disponibles)
- Iperf3: Para medir la velocidad de un enlace en internet.
- Wireshark: Un analizador de protocolos que permite realizar capturas del tráfico de red, en este caso se usará, para analizar el funcionamiento del protocolo ARP.

2. Marco teórico

2.1. Direcciones MAC (Media Access Control)

Corresponde a un numero binario de 6 bytes (48 bits) exclusivo de cada tarjeta de red. Para organizar esto, se utilizan los primeros 3 bytes (24 bits) de la dirección MAC para indicar la dirección del dispositivo y los últimos 3 bytes para identificar al fabricante.

Figura 1: Visualización campos dirección MAC (en hexadecimal)

Cabe destacar que la dirección MAC que consiste únicamente en bits 1 es utilizada para la difusión, es decir, se acepta en todas las direcciones de la red.

2.2. Protocolo ARP (Address Resolution Protocol)

ARP corresponde a un protocolo de la capa de enlace, cuyo objetivo es encontrar la dirección MAC correspondiente a una dirección IP para establecer comunicación con dicho dispositivo. Esta acción es realizada enviando un paquete ARP a la dirección de difusión (FF:FF:FF:FF:FF:FF) a la red, preguntando a cada dispositivo si posee la dirección MAC de la direción IP especificada, en el caso que la posea, la envía como respuesta al dispositivo que realizó la difusión para poder comenzar la comunicación. Un ejemplo simple de esto se encuentra en la figura 2.

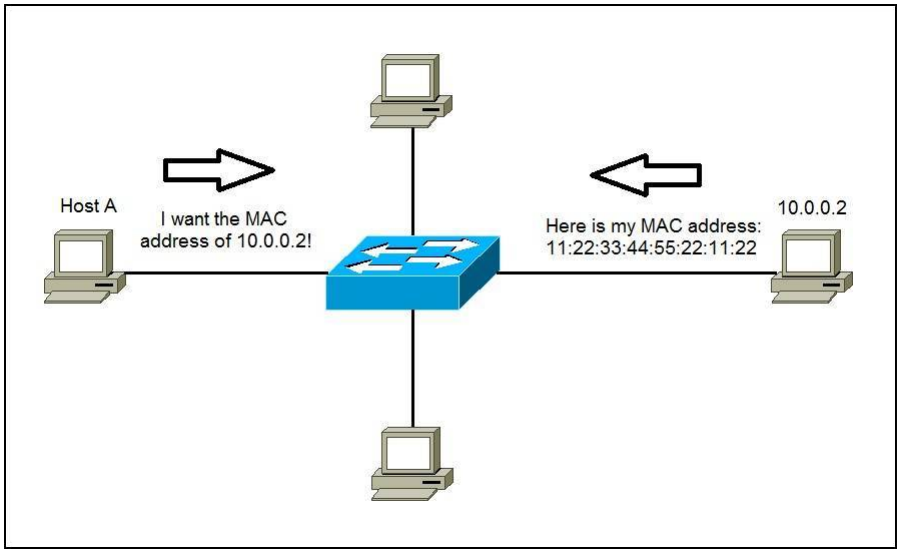

Figura 2: Funcionamiento protocolo ARP: Host A pregunta por 10.0.0.2, luego 10.0.0.2 responde con su dirección MAC.

3. Desarrollo y resultados

3.1. Parte 1: Capa física y enlace

Comenzando por conocer la dirección IP del computador utilizado junto a su rango de direcciones de la red local utilizando el comando *ifconfig* para ver la configuración de las interfaces de red dentro del terminal:

```
$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.101.11  netmask 255.255.255.0
broadcast 192.168.101.255
        inet6 fe80::1598:a85:4fe3:9690  prefixlen 64
scopeid 0x20<link>
        ether d8:cb:8a:9b:2a:a1  txqueuelen 1000  (Ethernet)
        RX packets 50797  bytes 52037437 (52.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36467  bytes 6020956 (6.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 5227  bytes 992662 (992.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5227  bytes 992662 (992.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

A partir de esto se obtiene que la IP del computador actual es *192.168.101.11* y, por lo tanto, el rango de direcciones IP de la red local es desde la dirección 192.168.101.1 hasta 192.168.101.255.

Conociendo esto, se utilizará *nmap* en conjunto con el rango IP para detectar todos los dispositivos conectados a la red local.

```
$ nmap -sn 192.168.101.0-255
Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-30 10:35 -04
Nmap scan report for _gateway (192.168.101.1)
Host is up (0.0020s latency).
Nmap scan report for 192.168.101.3
Host is up (0.016s latency).
Nmap scan report for 192.168.101.6
Host is up (0.093s latency).
Nmap scan report for alexmunozp-MS-7850 (192.168.101.11)
Host is up (0.00012s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.52 seconds
```

A partir de los datos obtenidos gracias a nmap, se puede realizar el Cuadro 1, el cual posee los dispositivos conectados a la red, la forma en la que se conectan, su dirección MAC e IP. Esta información se encuentra resumida en el diagrama de red de la figura 3.

Dispositivo	Capa física	Dirección MAC	Dirección IP
Router SOFTEL ONU-4FE	Cable 802.3ah 10Gbps Wifi 802.11.g 54Mbps	e0:67:b3:36:ea:af	192.168.101.1
Celular Motorola G5 Plus	Wifi 802.11.g 54Mbps	9a:da:c4:e2:ef:da	192.168.101.3
Celular Samsung Galaxy A70	Wifi 802.11g 54Mbps	7a:4d:4d:87:7c:e8	192.168.101.6
PC de escritorio (Red Realtek RTL8111G)	Cable 802.3ah 10Gbps	d8:cb:8a:9b:2a:a1	192.168.101.11

Cuadro 1: Dispositivos conectados a la red local.

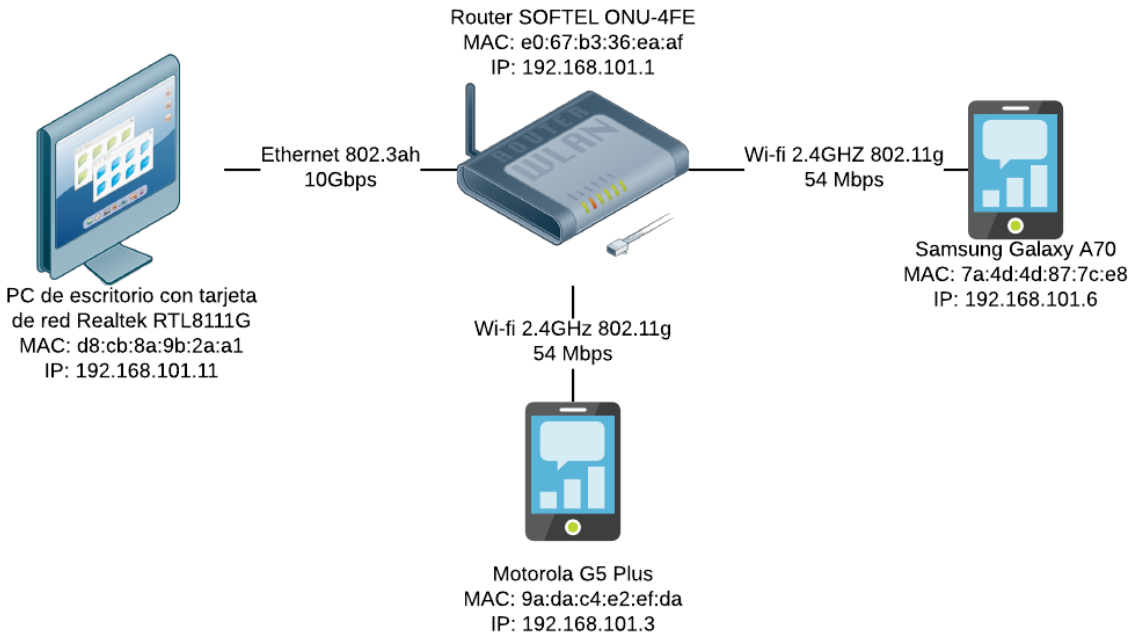

Figura 3: Diagrama de red del cuadro 1

Posteriormente se utiliza *iperf3* para realizar un test de velocidad entre el computador y un celular (el que usa la dirección 192.168.101.6), configurando el primero como servidor (*iperf3 -s*) y el último como cliente (*iperf3 -c 192.168.101.11 -u -b NM*, donde N toma los valores 1, 10, 100, 200, 300, 400, 500, 600, 700, 800, 900 y 1000, realizándose este test 6 veces para cada N), obteniéndose el gráfico de tasa de datos (N) contra porcentaje de fallos en la figura 4 con desviación estándar igual a 0.

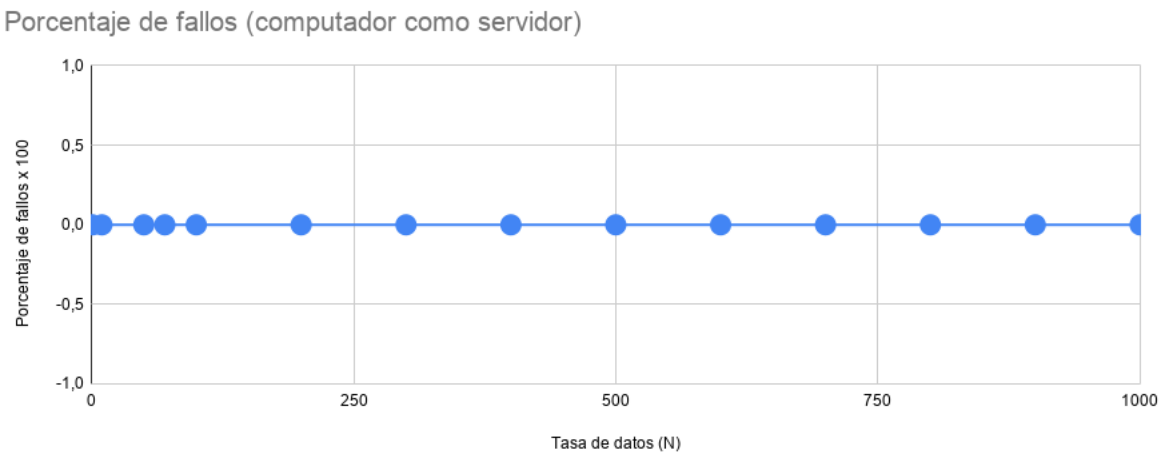

Figura 4: Gráfico tasa de datos vs porcentaje de fallos x 100. Donde el computador es el servidor

Luego, se hace el mismo proceso, pero en viceversa, colocando al celular como servidor y el computador como cliente, obteniendo el gráfico de la figura 5, donde el promedio de la desviación estándar de cada tasa de datos (N) es igual a 1,043873628.

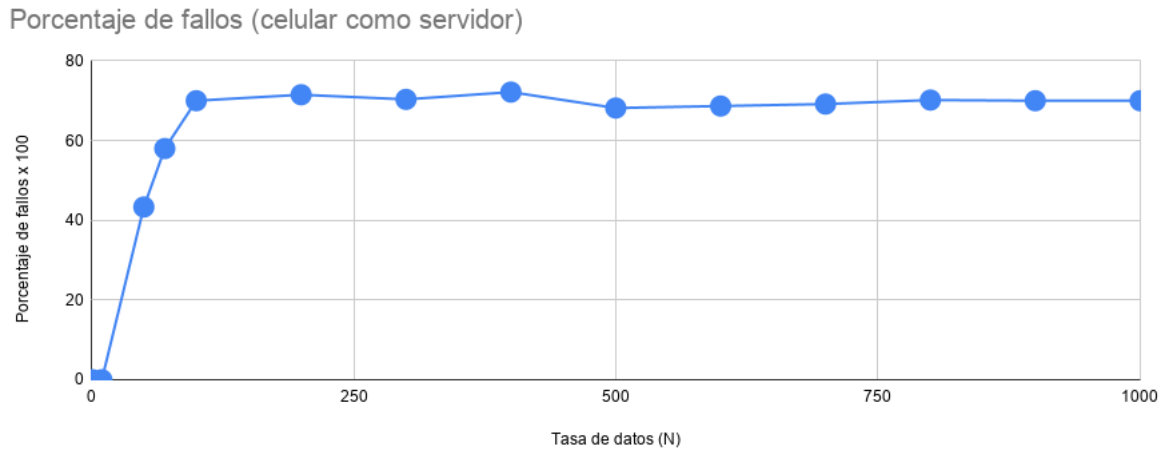

Figura 5: Gráfico tasa de datos vs porcentaje de fallos x 100. Donde el celular es el servidor

3.2. Parte 2: Protocolo ARP

Comenzando por eliminar la tabla ARP utilizando el comando: *sudo ip -s -s neigh flush all*, para posteriormente comprobar el estado de dicha tabla utilizando *arp -n*.

```
$ sudo ip -s -s neigh flush all
192.168.101.18 dev enp3s0 lladdr 34:f6:4b:28:e4:e8 used
58/58/30 probes 4 STALE
192.168.101.3 dev enp3s0 lladdr 9a:da:c4:e2:ef:da used
58/58/30 probes 4 STALE
192.168.101.4 dev enp3s0 lladdr 9a:da:c4:35:32:a1 used
56/56/28 probes 6 STALE
192.168.101.6 dev enp3s0 lladdr 7a:4d:4d:87:7c:e8 used
58/58/30 probes 4 STALE
192.168.101.15 dev enp3s0 lladdr f0:d7:aa:d8:97:45 used
56/56/28 probes 6 STALE
192.168.101.1 dev enp3s0 lladdr e0:67:b3:36:ea:af ref 1
used 1134/5/1133 probes 1 REACHABLE
*** Round 1, deleting 6 entries ***
*** Flush is complete after 1 round ***

$  arp -n
Direccion        TipoHW      DireccionHW          Indic     Mascara Interfaz
192.168.101.1    ether     e0:67:b3:36:ea:af       C            enp3s0
```

Después de eliminar la tabla ARP, es posible observar que se mantiene la dirección 192.168.101.1 que corresponde a la del router presente en la tabla 1.

Luego de esto, se inicia Wireshark para capturar los paquetes ARP que pasan por la tarjeta de red del computador y se utiliza el comando *ping 168.168.101.6* para comunicarse con la dirección especificada en dicho comando. Es posible percatar en la figura 6 se comienzan a captar inmediatamente varios paquetes ARP.

No.	Time	Source	Destination	Protocol	Length	Info
37	4.031907143	Micro-St_9b:2a:a1	Broadcast	ARP	42	Who has 192.168.101.6? Tell 192.168.101.11
38	4.108043583	7a:4d:4d:87:7c:e8	Micro-St_9b:2a:a1	ARP	60	192.168.101.6 is at 7a:4d:4d:87:7c:e8
58	9.230689572	7a:4d:4d:87:7c:e8	Micro-St_9b:2a:a1	ARP	60	Who has 192.168.101.11? Tell 192.168.101.6
59	9.230700682	Micro-St_9b:2a:a1	7a:4d:4d:87:7c:e8	ARP	42	192.168.101.11 is at d8:cb:8a:9b:2a:a1
69	9.861188325	9a:da:c4:21:9d:d7	Broadcast	ARP	60	Who has 192.168.101.11? Tell 192.168.101.5
70	9.861204669	Micro-St_9b:2a:a1	9a:da:c4:21:9d:d7	ARP	42	192.168.101.11 is at d8:cb:8a:9b:2a:a1
230	15.872012849	Micro-St_9b:2a:a1	9a:da:c4:21:9d:d7	ARP	42	Who has 192.168.101.5? Tell 192.168.101.11
231	15.875841643	9a:da:c4:21:9d:d7	Micro-St_9b:2a:a1	ARP	60	192.168.101.5 is at 9a:da:c4:21:9d:d7
278	25.087993340	Micro-St_9b:2a:a1	7a:4d:4d:87:7c:e8	ARP	42	Who has 192.168.101.6? Tell 192.168.101.11
280	25.112237071	7a:4d:4d:87:7c:e8	Micro-St_9b:2a:a1	ARP	60	192.168.101.6 is at 7a:4d:4d:87:7c:e8
302	31.133556656	7a:4d:4d:87:7c:e8	Micro-St_9b:2a:a1	ARP	60	Who has 192.168.101.11? Tell 192.168.101.6
303	31.133565798	Micro-St_9b:2a:a1	7a:4d:4d:87:7c:e8	ARP	42	192.168.101.11 is at d8:cb:8a:9b:2a:a1
307	33.320791287	Shenzhen_36:ea:af	Micro-St_9b:2a:a1	ARP	60	Who has 192.168.101.11? Tell 192.168.101.1
308	33.320809124	Micro-St_9b:2a:a1	Shenzhen_36:ea:af	ARP	42	192.168.101.11 is at d8:cb:8a:9b:2a:a1
340	41.215993920	Micro-St_9b:2a:a1	9a:da:c4:21:9d:d7	ARP	42	Who has 192.168.101.5? Tell 192.168.101.11

Figura 6: Paquetes ARP detectados por Wireshark al utilizar comando ping 168.168.101.6

Posteriormente se utiliza se verifica el estado de la tabla ARP (*arp -n*):

```
$ arp -n
Direccion        TipoHW  DireccionHW         Indic  Mascara  Interfaz
192.168.101.5    ether   9a:da:c4:21:9d:d7   C              enp3s0
192.168.101.6    ether   7a:4d:4d:87:7c:e8   C              enp3s0
192.168.101.1    ether   e0:67:b3:36:ea:af   C              enp3s0
```

Se puede apreciar en la última tabla ARP que aparecen los dispositivos que han realizado protocolos ARP (apreciable en la figura 6, donde se reciben paquetes ARP desde las direcciones 192.168.101.1, 192.168.101.5 y 192.168.101.6).

4. Análisis de resultados

4.1. Parte 1

Comparando el porcentaje de error por tasa de datos de las pruebas de velocidad realizadas con la herramienta *iperf3* de las figuras 4 y 5 con las velocidad del enlace del diagrama de la figura 3, se ve que hay una clara diferencia entre el computador de escritorio y el celular en cuanto a recibir una gran cantidad de datos por parte de un cliente. Esto es debido principalmente a la diferencia de velocidad del enlace y procesamiento entre los dispositivos, o sea, el PC de escritorio posee capacidad suficiente para procesar todo el espectro de tasa de datos permitido por iperf3 (N entre [1, 1000]), apoyado de suficiente velocidad de enlace para recibir los datagramas de manera correcta. Por otra parte, el dispositivo móvil está más restringido por la velocidad del enlace (54Mbps) y su propia velocidad para procesar los datos, lo cual puede ser observado claramente en la figura 5, donde el porcentaje de fallos incrementa de forma muy rápida hasta llegar a un estable 70 % de perdidas, mientras que el computador se queda establemente en 0 % de fallos (figura 4).

4.2. Parte 2

Al realizar el comando *sudo ip -s -s neigh flush all* y posteriormente *arp -n*, se puede observar que solo aparece el dispositivo con la IP 192.168.101.1, correspondiente al router de la red. Esto es debido a que tanto el router como el computador están en constante comunicación todo el tiempo, por ello, es bastante probable que al momento de vaciar la tabla ARP instantáneamente el computador haya lanzado algún paquete ARP a la red para intentar establecer comunicación.

Por otra parte, al momento de utilizar el comando *ping 192.168.101.6*, el computador va a necesitar la dirección MAC del dispositivo con dicha IP, pero como la tabla ARP se encuentra vacía, empieza a mandar paquetes ARP a la red preguntando por la dirección 192.168.101.6 (figura 6), respondiéndole el router y entregándole la dirección MAC de la IP buscada. También se puede ver en la figura 6, que se mandan paquetes ARP normalmente sin necesidad de "forzarloçon ping, como se puede ver en la línea 230 el computador pregunta

por la dirección MAC de la IP 192.168.101.5, sin utilizar la herramienta *ping*. Por ello, al realizar el comando *arp -n* ahora aparecen en la tabla las direcciones IP 192.168.101.5 y 192.168.101.6.

Después de realizar todo lo anterior, se puede comprobar que el tráfico de la red es normal, debido a que cada paquete ARP es respondido de manera correcta (o sea, cada pregunta por una dirección MAC es respondida) y no se pierden estos paquetes. Además, en conjunto con lo analizado en la parte 1, los porcentajes de perdida de datos tienen sentido para cada tipo de conexión, llevando a la conclusión de que efectivamente, el tráfico de esta red es normal.

5. Conclusiones

Luego de la experiencia realizada pudimos analizar y entender de mejor manera los conceptos y funcionamientos de protocolos a nivel de la capa de enlace, utilizando las herramientas mencionadas a lo largo del laboratorio.

Al obtener la información de los distintos dispositivos conectados a la red local, se crea una tabla con todos los dispositivos encontrados. Realizando la tabla pudimos observar como los dispositivos que tenemos en nuestras casas utilizan las redes vistas en clases, estas son la red Ethernet y la red inalámbrica Wifi 802.11, junto con el diagrama se red, se entiende como se forma una red de área local (LAN), que dispositivos de nosotros la componen, y como se comunican a través direcciones MAC e IP. Comprender como se realiza un test de velocidad, mediante la construcción de gráficos donde se puede ver el porcentaje de fallos obtenidos, respecto a distintas tasa de datos ingresadas, entre el computador y un celular.

Con Wireshark pudimos ver de forma "real" como es el tráfico de red de nuestra área local y al igual que las tablas interactivas realizadas en clases, como dispositivos realizan el protocolo ARP para preguntar por la dirección MAC, respecto a una dirección IP.

Finalmente, podemos decir que gracias al este primer laboratorio hemos reforzado nuestro conocimientos acerca de la capa de enlace y como esta funciona para poder comunicar los dispositivos que usamos día a día. Se espera en un próximo trabajo de laboratorio poder complementar lo aprendido hoy sobre capa de enlace, y como interacciona con la capas siguientes del modelo.

Bibliografía

Tanenbaum, A. S. (2012). *Redes de computadoras*, volume 5. Pearson.

Videos, P. A. (2018). Arp explained - address resolution protocol. [Online] `https://www.youtube.com/watch?v=cn8Zxh9bPio`.