Práctica 6

Capa de Transporte - Parte II

1. Utilizando la máquina virtual, use Wireshark para capturar paquetes enviados y recibidos en cada uno de los siguientes casos. Para ello, arranque la captura en la interfaz con IP 172.28.0.1 antes de realizar los incisos A, B, C y D.

    a. Abra un navegador e ingrese a la URL: www.redes.unlp.edu.ar. Analice la secuencia de segmentos TCP que permiten la apertura del canal de comunicación por el cual posteriormente viajarán los mensajes HTTP intercambiados. ¿Con qué nombre se conoce a dicha secuencia? ¿Qué flags se utilizan en cada uno de los segmentos intercambiados? ¿Qué indica cada uno de estos flags?

    b. Cierre el navegador. Analice la secuencia de segmentos TCP que ocurren al hacerlo ¿Cuál es el objetivo éstos? ¿Qué flags se utilizan en cada uno de dichos segmentos? ¿Qué indica cada uno de estos flags?

    c. Para este ejercicio debe usar tanto el navegador Chromium como Iceweasel. Utilice Chromium para ingresar a la URL: www.redes.unlp.edu.ar y seguidamente utilice Iceweasel para ingresar nuevamente a la URL: www.redes.unlp.edu.ar

        i. Observe la información de Puerto Origen y Puerto destino de cada una de las comunicaciones. En base a lo observado, responda ¿Es posible conectarse 2 veces en forma simultánea al mismo lugar? ¿Qué distingue una conexión de otra? Capture el tráfico de red si considera necesario para observar dicha información.

        ii. Identifique lo observado en el punto anterior utilizando el comando ss.

    d. Desde la consola use el servicio tftp.

        i. Primero cree un archivo llamado prueba.txt, por ejemplo:

        ```
        echo Prueba > prueba.txt
        ```

        ii. Ejecute tftp 172.28.0.29 y copie el archivo anterior desde su PC al servidor, a través de la opción put.

        ```
        put prueba.txt
        ```

        iii. Cierre la conexión, borre el archivo de su PC (rm prueba.txt) y obténgalo ahora del servidor a través de la opción get:

        ```
        get prueba.txt
        ```

    e. ¿Qué diferencias encuentra en cuánto a mensajes intercambiados entre los puntos A, B respecto del punto D?

f. ¿Qué diferencias encuentra en el punto D respecto a los anteriores respecto a utilización de puertos y protocolo de transporte utilizado?

2. Investigue los distintos tipos de estado que puede tener una conexión TCP.
   (Ver la página: https://thewalnut.io/app/release/73/#time=21)

3. Dada la siguiente salida del comando ss, responda:

```
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
tcp    LISTEN     0      128                *:22                    *:*      users:(("sshd",pid=468,fd=29))
tcp    LISTEN     0      128                *:80                    *:*      users:(("apache2",pid=991,fd=95))
udp    LISTEN     0      128       163.10.5.222:53                  *:*      users:(("named",pid=452,fd=10))
tcp    ESTAB      0      0         163.10.5.222:59736    64.233.163.120:443    users:(("x-www-browser",pid=1079,fd=51))
tcp    CLOSE-WAIT 0      0         163.10.5.222:41654     200.115.89.30:443    users:(("x-www-browser",pid=1079,fd=50))
tcp    ESTAB      0      0         163.10.5.222:59737    64.233.163.120:443    users:(("x-www-browser",pid=1079,fd=55))
tcp    ESTAB      0      0         163.10.5.222:33583     200.115.89.15:443    users:(("x-www-browser",pid=1079,fd=53))
tcp    ESTAB      0      0         163.10.5.222:45293     64.233.190.99:443    users:(("x-www-browser",pid=1079,fd=59))
tcp    LISTEN     0      128                *:25                    *:*      users:(("postfix",pid=627,fd=3))
tcp    ESTAB      0      0            127.0.0.1:22            127.0.0.1:41220  users:(("sshd",pid=1418,fd=3),
                                                                                       ("sshd",pid=1416,fd=3))
tcp    ESTAB      0      0         163.10.5.222:52952     64.233.190.94:443    users:(("x-www-browser",pid=1079,fd=29))
tcp    TIME-WAIT  0      0         163.10.5.222:36676     54.149.207.17:443    users:(("x-www-browser",pid=1079,fd=3))
tcp    ESTAB      0      0         163.10.5.222:52960     64.233.190.94:443    users:(("x-www-browser",pid=1079,fd=67))
tcp    ESTAB      0      0         163.10.5.222:50521     200.115.89.57:443    users:(("x-www-browser",pid=1079,fd=69))
tcp    SYN-SENT   0      0         163.10.5.222:52132        43.232.2.2:9500   users:(("x-www-browser",pid=1079,fd=70))
tcp    ESTAB      0      0            127.0.0.1:41220         127.0.0.1:22     users:(("ssh",pid=1415,fd=3))
udp    LISTEN     0      128          127.0.0.1:53                    *:*      users:(("named",pid=452,fd=9))
```

   a. ¿Cuántas conexiones hay establecidas?

   b. ¿Cuántos puertos hay abiertos a la espera de posibles nuevas conexiones?

   c. El cliente y el servidor de las comunicaciones HTTPS (puerto 443), ¿residen en la misma máquina?

   d. El cliente y el servidor de la comunicación SSH (puerto 22), ¿residen en la misma máquina?

   e. Liste los nombres de todos los procesos asociados con cada comunicación. Indique para cada uno si se trata de un proceso cliente o uno servidor.

   f. ¿Cuáles conexiones tuvieron el cierre iniciado por el host local y cuáles por el remoto?

   g. ¿Cuántas conexiones están aún pendientes por establecerse?

4. Dadas las salidas de los siguientes comandos ejecutados en el cliente y el servidor, responder:

```
servidor# ss -natu | grep 110
tcp    LISTEN     0     0             *:110              *:*
tcp    SYN-RECV   0     0     157.0.0.1:110     157.0.11.1:52843

cliente# ss -natu | grep 110
```

```
tcp     SYN-SENT   0     1     157.0.11.1:52843     157.0.0.1:110
```

a. ¿Qué segmentos llegaron y cuáles se están perdiendo en la red?

b. ¿A qué protocolo de capa de aplicación y de transporte se está intentando conectar el cliente?

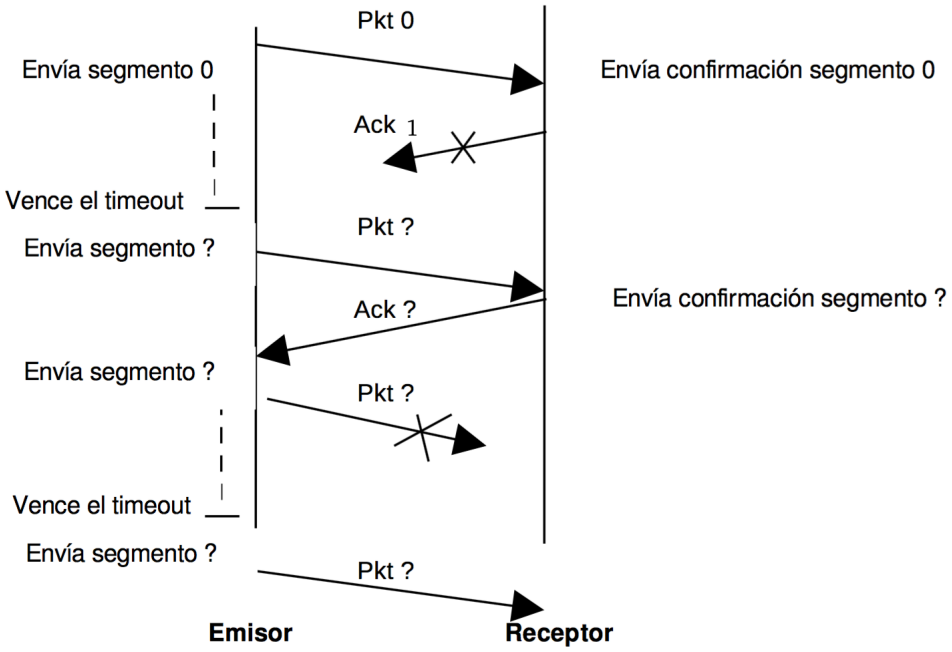
c. ¿Qué flags tendría seteado el segmento perdido?

5. ¿Cual es el puerto por defecto que se utiliza en los siguientes servicios?

   Web / SSH / DNS / Web Seguro / POP3 / IMAP / SMTP

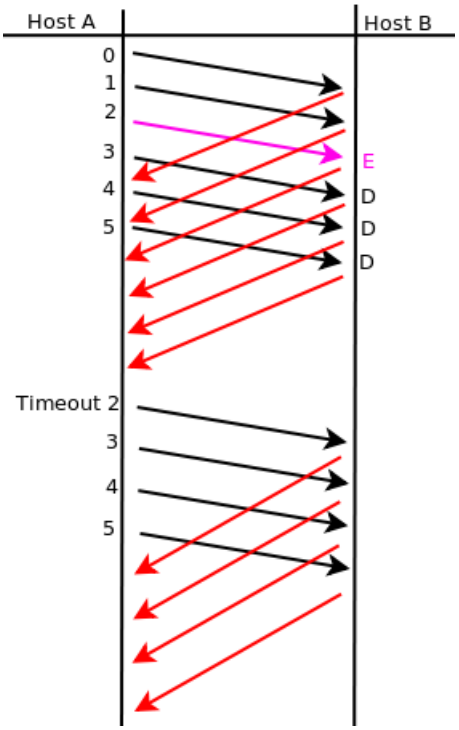
   Investigue en qué lugar en Linux y en Windows está descripta la asociación utilizada por defecto para cada servicio.

6. Complete los (?) de la siguiente secuencia Stop and Wait:

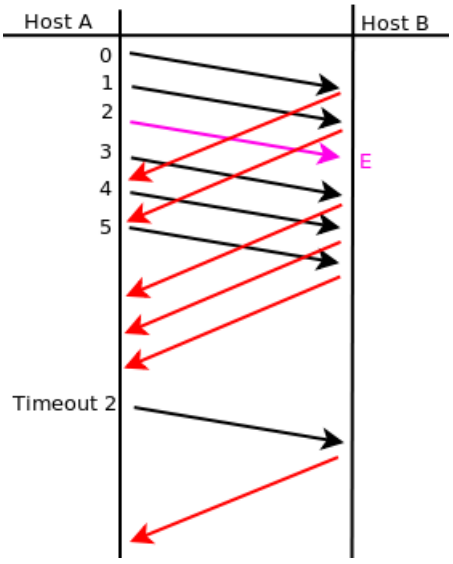


7. Explique la lógica de Go BackN.

8. Suponiendo Go Back N; tamaño de ventana 4 y sabiendo que E indica que el mensaje llegó con errores y que D significa que el mensaje será descartado por llegar fuera de secuencia. Indique en el siguiente gráfico, la numeración de los ACK que el host B envía al Host A.



9. Suponiendo Selective Repeat; tamaño de ventana 4 y sabiendo que E indica que el mensaje llegó con errores. Indique en el siguiente gráfico, la numeración de los ACK que el host B envía al Host A.



10. ¿Qué restricción existe sobre el tamaño de ventanas en el protocolo Selective Repeat?

11. Investigue cómo funciona el protocolo de aplicación FTP teniendo en cuenta las diferencias en su funcionamiento cuando se utiliza el modo activo de cuando se utiliza el modo pasivo ¿En qué se diferencian estos

tipos de comunicaciones del resto de los protocolos de aplicación vistos?

12. Utilizando el Live CD conéctese al servidor ftp utilizando el comando ftp ftp.redes.unlp.edu.ar utilizando los siguientes datos:

    a. Nombre de usuario: **redes**
    b. Password: **redes**
    c. Pruebe la transferencia de un archivo cualquiera hacia y desde el servidor.
    d. Utilice Wireshark para obtener capturas de transferencias de archivos usando primero el modo activo y luego el modo pasivo.

Programación de sockets

Resuelva los siguientes ejercicios utilizando el lenguaje de programación que prefiera (por simpleza, se recomiendan Python o Ruby).

13. Desarrolle un cliente y un servidor, donde el cliente envíe un mensaje al servidor y este último imprima en pantalla el contenido del mismo.

    a. Utilizando UDP.
    b. Utilizando TCP.

14. Compare ambas implementaciones. ¿Qué diferencia nota entre la implementación de cada una? ¿Cuál le parece más simple?

Ejercicio de parcial.

15. Dada la salida que se muestra en la imagen, responda los ítems debajo.

```
Netid  State      Local Address:Port      Peer Address:Port
udp    UNCONN               *:68                  *:*      (("dhclient",671,5))
udp    UNCONN               *:123                 *:*      (("ntpd",2138,16))
udp    UNCONN              :::123                :::*      (("ntpd",2138,17))
tcp    LISTEN               *:80                  *:*      (("nginx",23653,19),("nginx",23652,19))
tcp    LISTEN               *:22                  *:*      (("sshd",1151,3))
tcp    LISTEN         127.0.0.1:25                *:*      (("master",11457,12))
tcp    LISTEN               *:443                 *:*      (("nginx",23653,20),("nginx",23652,20))
tcp    LISTEN               *:3306                *:*      (("mysqld",4556,13))
tcp    ESTAB          127.0.0.1:3306        127.0.0.1:34338  (("mysqld",4556,14))
tcp    TIME-WAIT  10.100.25.135:443     43.226.162.110:29148
tcp    ESTAB          127.0.0.1:48717       127.0.0.1:3306   (("ruby",28615,10))
tcp    ESTAB          127.0.0.1:3306        127.0.0.1:48717  (("mysqld",4556,17))
tcp    ESTAB          127.0.0.1:34338       127.0.0.1:3306   (("ruby",28610,9))
tcp    ESTAB      10.100.25.135:22     200.100.120.210:61576  (("sshd",13756,3),("sshd",13654,3))
tcp    LISTEN              :::22                 :::*      (("sshd",1151,4))
tcp    LISTEN              :1:25                 :::*      (("master",11457,13))
```

- Suponga que ejecuta los siguientes comandos desde un host con la IP 10.100.25.90. Responda qué devuelve la ejecución de los siguientes comandos y, en caso que corresponda, especifique los flags.

a. hping3 -p 3306 –udp 10.100.25.135

b. hping3 -S -p 25 10.100.25.135

c. hping3 -S -p 22 10.100.25.135

d. hping3 -S -p 110 10.100.25.135

- ¿Cuántas conexiones distintas hay establecidas? Justifique.

16. Complete en la columna Orden, el orden de aparición de los paquetes representados en cada fila.

Host A				Host B			Orden
Seq	ACK	Len		Seq	ACK	Len	
100	2421	0	->				
308	2821	0	->				
			<-	1419	100	1002	
156	2780	64	->				
220	2780	47	->				
			<-	2821	308	1418	
			<-	2780	220	0	
			<-	1	100	1418	**1**
100	2780	56	->				
			<-	2780	308	0	
267	2780	41	->				
			<-	2780	308	41	
			<-	2421	100	359	
100	1419	0	->				