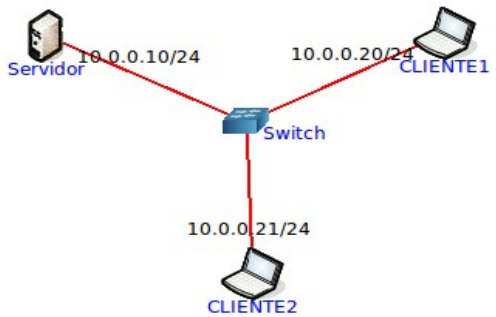
Práctica 3

Capa de Transporte

1. ¿Cuál es la función de la capa de transporte?
2. Describa la estructura del segmento TCP y UDP
3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?
4. Compare TCP y UDP en cuanto a:
   A) Confiabilidad
   B) Multiplexación
   C) Orientado a la conexión
   D) Controles de congestión
   E) Utilización de puertos
   F) ¿Cuál es el campo del datagrama IP y los valores que se utilizan en este para diferenciar que se transporta TCP o UDP? (Ayuda: buscar en /etc/protocols y contrastarlo con una captura de tráfico)
5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el término Datagrama, indique cuándo.
6. Describa el saludo de tres vías de TCP.
7. ¿Qué sucede si llega un segmento TCP a un host que no tiene a ningún proceso esperando en el puerto destino de dicho segmento?
   A) Utilice **hping3** para enviar paquetes TCP al puerto destino 40 del mismo Live CD con el Flags ACK activado.
8. ¿Qué sucede si llega un datagrama UDP a un host que no tiene a ningún proceso esperando en el puerto destino de dicho datagrama?
   A) Utilice **hping3** para enviar datagramas UDP al puerto destino 40 del mismo Live CD.
9. Investigue qué es multicast. ¿Sobre cuál de los protocolos de capa de transporte funciona? ¿Se podría adaptar para que funcione sobre el otro protocolo de capa de transporte? ¿por qué?
10. Utilice el comando netstat para obtener la siguiente información de su PC:
    A) Para listar las comunicaciones TCP establecidas
    B) Para listar las comunicaciones UDP establecidas
    C) Obtener solo los servicios TCP que están esperando comunicaciones
    D) Obtener solo los servicios UDP que están esperando comunicaciones
    E) Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión
11. Use CORE para armar una topología como la siguiente, sobre la cual deberá realizar:



    A) En Servidor, utilice la herramienta **netcat** para levantar un servicio que escuche en el puerto 8001/TCP. Utilice la opcion **-k** para que el servicio sea persistente
    B) Desde CLIENTE1 conectarse a dicho servicio utilizando también la herramienta **netcat**
    C) Inspeccionar el estado de las conexiones con el comando netstat en ambos equipos

Ayuda: **watch -n 1 'netstat -nat'**

D) Cerrar la conexión desde CLIENTE1 y ver estados de las conexiones en ambos equipos.

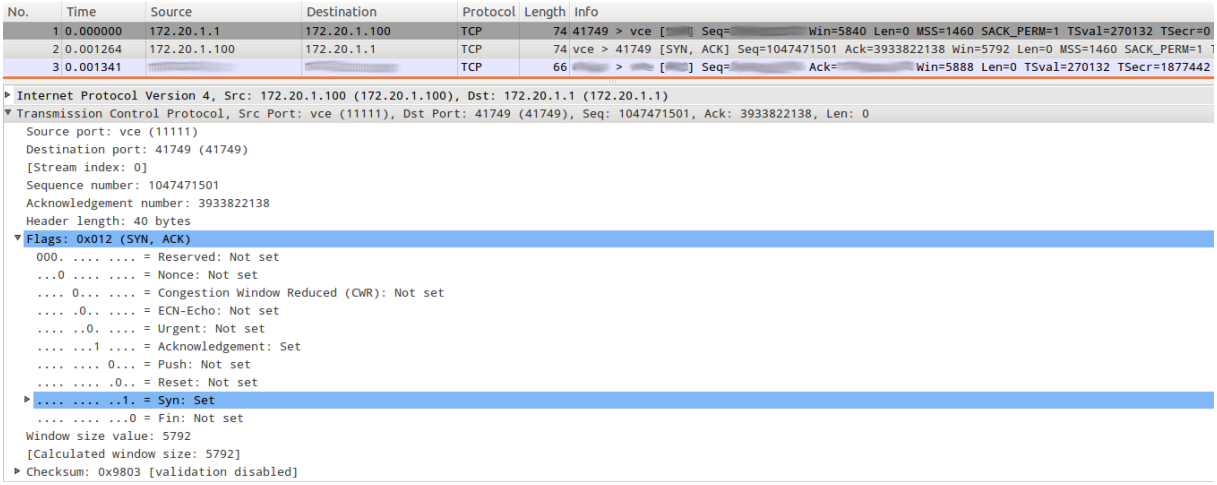
E) Intentar nuevamente realizar la conexión utilizando el mismo port origen. Usar opción **-p** de **netcat**

i. ¿Seria posible realizar la conexión desde CLIENTE2 utilizando dicho puerto origen?

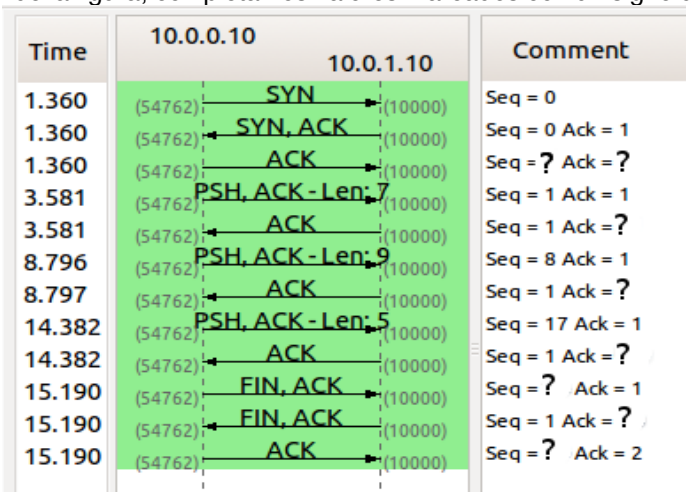
F) Volver a correr el servidor y lograr varias conexión desde los clientes.

G) En base a lo observado, ¿cuántas conexiones son posibles al servidor desde un host?

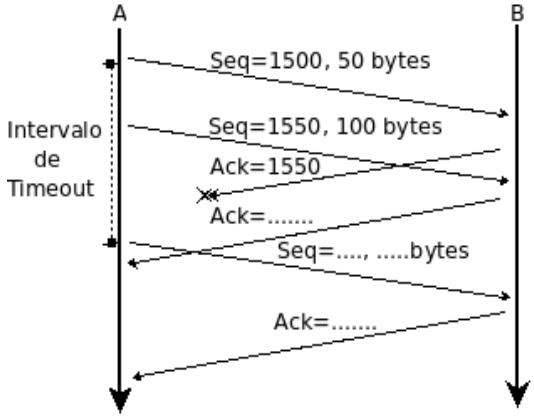
12. De acuerdo a la captura de la siguiente figura, indique los valores de los campos borroneados



13. Dada la sesión TCP de la figura, completar los valores marcados con un signo de interrogación



14. Completar los datos que faltan en el intercambio de mensajes del siguiente diagrama de flujo TCP:



15. Utilizando el Live CD, use Wireshark para capturar paquetes enviados y recibidos en cada uno de los siguientes casos. Para ello, arranque la captura antes de realizar los incisos A, B, C y D

A) *Abra un navegador e ingrese a la URL: www.redes.unlp.edu.ar*

i. Analice la secuencia de segmentos TCP que permiten la apertura del canal de comunicación por el cual posteriormente viajarán los mensajes HTTP intercambiados. ¿Con que 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:

i. 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 simultanea 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 netstat.

D) Desde la consola de root use el servicio tftp:

i. Inicie el servicio tftp: "service tftpd-hpa start".

ii. Verifique con el comando netstat que el servicio efectivamente arranco.

iii. Ejecute "tftp localhost" y copie un archivo cualquiera desde su PC al servidor, a través de la opción put: "put captura.pcap" por ejemplo.

iv. Borre el archivo de su PC: "rm captura.pcap" y obténgalo ahora del servidor a través de la opción get: "get captura.pcap" por ejemplo.

E) ¿Qué diferencias encuentra en cuanto 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?

16. Investigue los distintos tipos de estado que puede tener una conexión TCP.

17. Dada la siguiente captura del comando netstat, responda:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 163.10.10.115:53        0.0.0.0:*               LISTEN      1369/named
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      1719/pure-ftpd (SER
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1369/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1823/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1642/cupsd
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      1776/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      1369/named
tcp        0      0 127.0.0.1:2628          0.0.0.0:*               LISTEN      1472/0
tcp        0      0 127.0.0.1:4038          0.0.0.0:*               LISTEN      1879/python
tcp        0      0 163.10.10.115:55054     200.17.202.197:443      TIME_WAIT   5076/chromium-brows
tcp        0      0 163.10.10.115:55055     200.17.202.197:443      ESTABLISHED 5076/chromium-brows
tcp        0      0 163.10.10.115:55050     200.17.202.197:443      ESTABLISHED 5076/chromium-brows
tcp        0      0 163.10.10.115:55051     200.17.202.197:443      ESTABLISHED 5076/chromium-brows
tcp        0      0 163.10.10.115:55052     200.17.202.197:443      CLOSE_WAIT  5076/chromium-brows
tcp        0      0 163.10.10.115:22        163.10.10.98:36595      ESTABLISHED 2977/sshd: lihuen [
tcp        0      0 127.0.0.1:42170         127.0.0.1:80            ESTABLISHED 3750/firefox-bin
tcp        0      0 163.10.10.115:60391     173.194.42.20:80        ESTABLISHED 5076/chromium-brows
tcp        0      1 163.10.10.115:38029     4.5.5.5:9000            SYN_SENT    3750/firefox-bin
tcp        0      0 127.0.0.1:80            127.0.0.1:42170         ESTABLISHED 4229/apache2
```

i. ¿Cuántas conexiones hay establecidas?

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

iii. El cliente y el servidor de las comunicaciones HTTP (puerto 80), ¿residen en la misma máquina?

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

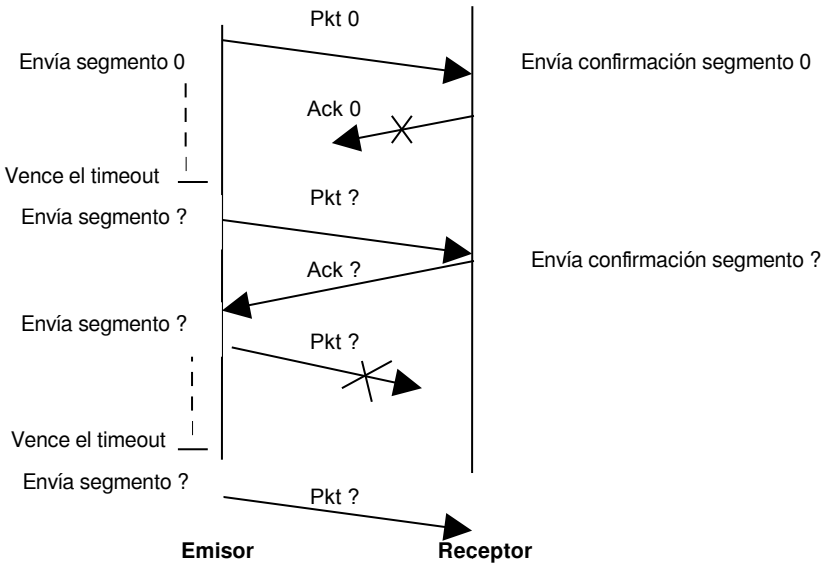
v. Liste los nombres de todos los procesos asociados con cada comunicación. Indique para cada uno si se trata de un proceso cliente o uno servidor

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

vii. ¿Cuántas conexiones están aún pendientes por establecerse?

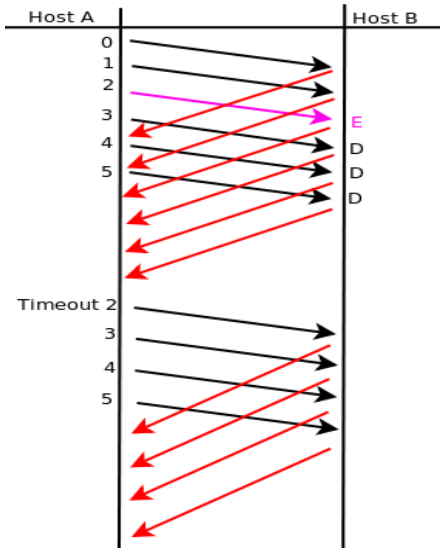
18. ¿Cual es el puerto por defecto que se utiliza en los siguientes servicios?
    - Web / SSH / DNS / Web Seguro / POP3 / IMAP / SMTP
    - Investigue en que lugar en Linux y en Windows está descripta la asociación utilizada por defecto para cada servicio

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

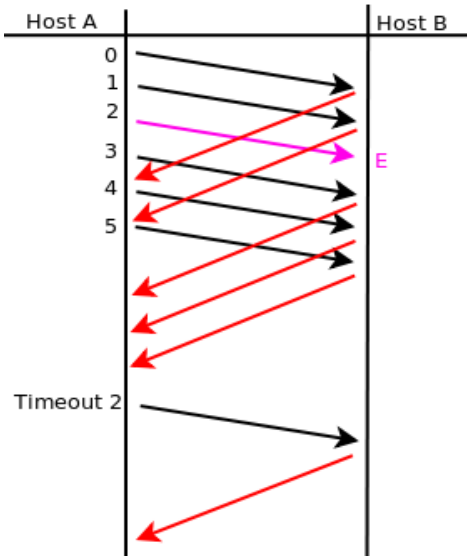


20. Explique la lógica de Go Back – N

21. 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.



22. 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.



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

24. 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?

25. 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: lihuen

    B) Password: lihuen

    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.