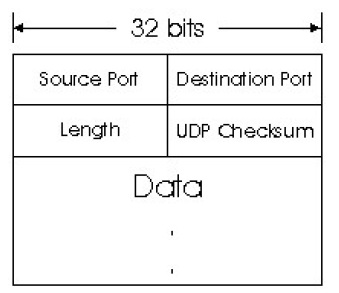
**Práctica 3**

**Capa de Transporte**

## 1. ¿Cuál es la función de la capa de transporte?

Un protocolo de la capa de transporte proporciona una comunicación lógica entre procesos de aplicación que se ejecutan en hosts diferentes. Los procesos de aplicación utilizan la comunicación lógica proporcionada por la capa de transporte para enviarse mensajes entre sí, sin preocuparse por los detalles de la infraestructura física utilizada para transportar estos mensajes.

## 2. Describa la estructura del segmento TCP y UDP



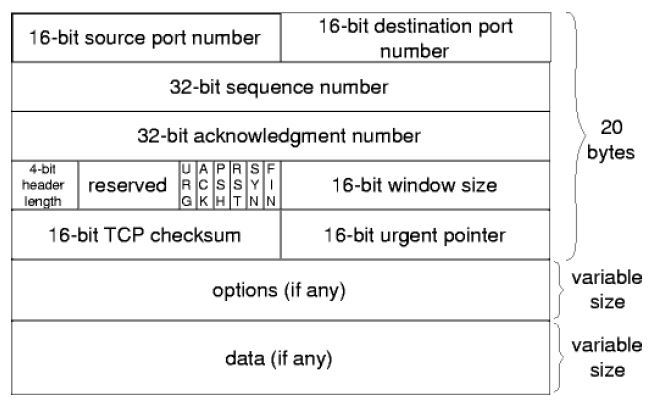
UDP:

Los puertos origen y destino se utilizan para multiplexar y demultiplexar los datos de y para las aplicaciones de la capa superior.

El campo longitud representa la longitud del segmento.

El campo checksum contiene la información para comprobar si hay errores en los datos.

Y el campo data contiene los datos.



TCP:

Los puertos fuente y destino se utilizan para multiplexar y demultiplexar los datos de y para las aplicaciones de la capa superior.

El campo de suma de comprobación (checksum) es como el de UDP.

El campo de número de secuencia es un número relativo al paquete, que se inicia desde un número random, y sirve para poder saber el orden de los paquetes.

El campo ventana de recepción se utiliza para el control de flujo.

Longitud de cabecera especifica la longitud de la cabecera TCP en palabras de 32 bits.

El campo opciones es opcional y de longitud variable. Se utiliza cuando un emisor y un receptor negocian el tamaño máximo de segmento (MSS) o como un factor de escala de la ventana en las redes de alta velocidad. También se define una opción de marca temporal.

El campo indicador (flags) tiene 6 bits: El bit ACK se utiliza para indicar que el valor transportado en el campo de reconocimiento es válido. Los bits RST, SYN y FIN se utilizan para el establecimiento y cierre de conexiones. El bit PSH indica que el receptor deberá pasar los datos a la capa superior de forma inmediata. El bit URG indica que hay datos que fueron marcados como urgentes.

## 3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?

El objetivo del uso de puertos es que cada socket tenga un identificador único, para que se pueda llevar a cabo la operación de multiplexación.

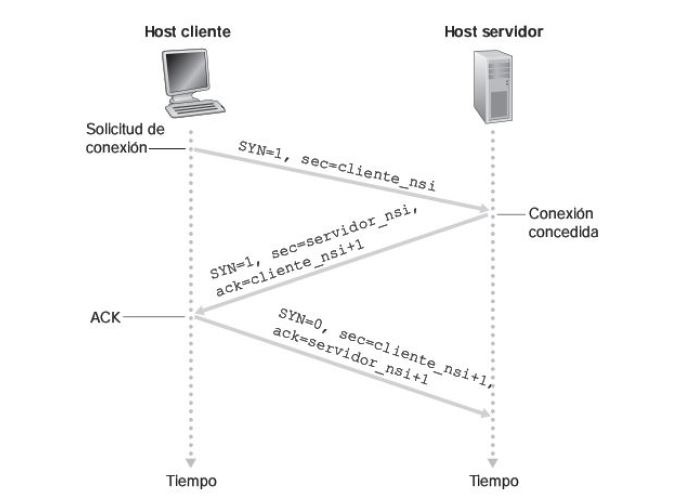
## 4. Compare TCP y UDP en cuanto a:

|  |  |  |
| --- | --- | --- |
|  | TCP | UDP |
| Utilización de puertos | Sí | Sí |
| Confiabilidad | Proporciona un servicio orientado a la conexión fiable. | Proporciona un servicio de conexión no fiable a la aplicación que lo invoca |
| Multiplexación | Sí | Sí |
| Orientado a la conexión | Sí | No |
| Controles de congestión | Evita que cualquier conexión TCP inunde con una cantidad de tráfico excesiva los enlaces y routers existentes entre los hosts que están comunicándose. | No proporciona. |

## 5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el término Datagrama, indique cuando.

Según la bibliografía, se usa el término datagrama para referirse a los paquetes de UDP y a los de la capa de red.

## 6. Describa el saludo de tres vías de TCP.

 Se le llama saludo de tres vías (o acuerdo de tres fases, o three way handshake) al procedimiento de establecimiento de conexión en el cual se envían tres paquetes entre los dos hosts.

En el paso 1, del lado del cliente se envía un segmento de TCP al servidor (SYN). El cliente selecciona de forma aleatoria un número de secuencia inicial (cliente\_nsi), y lo coloca en el campo de número de secuencia del segmento TCP inicial SYN.

Paso 2: Una vez que el segmento SYN llega al servidor, este extrae dicho segmento SYN del datagrama, asigna los buffers y variables TCP a la conexión y envía un segmento de conexión concedida al cliente TCP. Este segmento contiene 3 fragmentos de información importante: el bit SYN se pone a 1, el campo de reconocimiento de la cabecera del segmento se hace igual a cliente\_nsi + 1, y el servidor elige su número de secuencia inicial (servidor\_nsi), y almacena este valor en el campo de número de secuencia de la cabecera del segmento TCP.

Paso 3: Al concederse la conexión, el host cliente envía al servidor otro segmento, confirmado al segmento de conexión concedida del servidor. El cliente almacena el valor servidor\_nsi +1 en el campo de reconocimiento de la cabecera del segmento TCP. El bit SYN se pone en 0, ya que la conexión estaba establecida. Esta tercera etapa puede transportar datos del cliente al servidor dentro de la carga útil del segmento.

## 7. Investigue que es multicast. ¿Sobre qué protocolo de capa 4 funciona? ¿Se podría adaptar para que funcione sobre el otro protocolo de capa 4? ¿por qué?

Multicast funciona sobre UDP. Sí, se podría pero se necesitaría una conexión para cada cliente, que va en contra de la idea del multicast (paquetes de uno a muchos).

## 8. Utilizando el Live CD. Use el analizador de paquetes Wireshark para capturar los paquetes enviados y recibidos en cada uno de los siguientes casos. Para ello, arranque la captura antes de realizar cada una de las acciones indicadas:

## 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?

Es la secuencia del saludo de tres vías explicado anteriormente.

En el primer segmento viaja el flag SYN, en el segundo, ACK y SYN, y en el tercero ACK.

El flag SYN (synchronization) indica que se quiere iniciar una conexión TCP. El ACK (acknowledgement) indica que se aceptó la conexión.

## B) Cierre el navegador:

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

El objetivo de estos segmentos es cerrar la conexión con el servidor.

Utiliza FIN y ACK. El FIN indica que se quiere cerrar la conexión.

## 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.

Sí. Los puertos distinguen a una conexión de otra

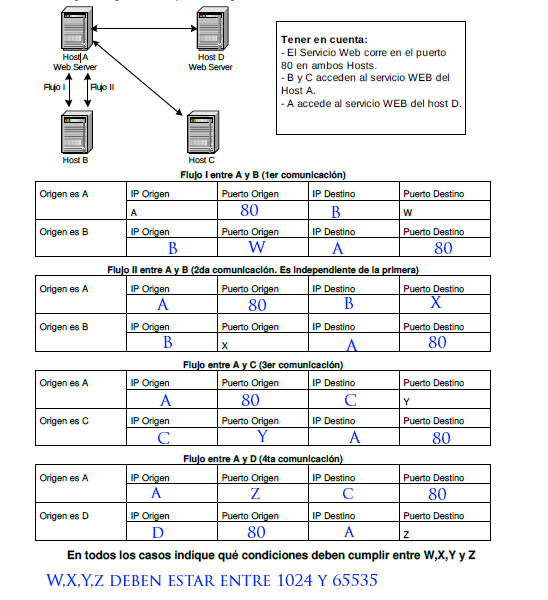
## E) ¿Qué diferencias encuentra en cuanto a mensajes intercambiados entre los puntos A, B respecto del punto D?

La principal diferencia es que en los puntos A y B se utiliza HTTP y TCP, mientras que TFTP usa UDP, ya que está pensado para redes locales

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

HTTP utiliza el puerto 80, y TFTP usa puertos aleatorios. (en el ejemplo que ejecutamos usó el 53808).

## 9. Dado el siguiente gráfico, complete los siguientes cuadros:



## 10.¿Qué es ARQ (Automatic Repeat Request)? ¿Qué capacidades requieren ser implementadas en los protocolos ARQ para detectar la presencia de errores en los datos?

ARQ son protocolos utilizados para el control de errores en la transmisión de datos.

Se requieren, fundamentalmente, tres capacidades:

* Detección de errores: Se necesita un mecanismo que permita al receptor detectar que se han producido errores de bit.
* Realimentación del receptor: Para controlar la correcta recepción de un paquete se utilizan ACKs (acknowledge) y NAKs (negative acknowledgement) de forma que cuando el receptor recibe un paquete correctamente el receptor asiente con un ACK y si no es correcto responde con un NAK.
* Retransmisión: Un paquete que se recibe con errores en el receptor será retransmitido por el emisor.

## 11.Complete los (?) de la siguiente secuencia Stop and Wait:C:\Users\Alfonso\Desktop\11.PNG

## 12. Explique la lógica de Go Back – N.

El protocolo GBN permite a emisor transmitir varios paquetes sin tener que esperar a que sean reconocidos, pero está restringido a no tener más de un número máximo permitido, N, de paquetes no reconocidos en el canal.

Las confirmaciones son acumulativas, o sea que por ejemplo, si se confirma el vigésimo paquete, se da por confirmado todos los paquetes anteriores hasta el décimo noveno.

Si no se confirma un paquete, puede ser porque no llegó, llegó erróneo o se perdió la confirmación. En ese caso, el emisor debe reenviar ese paquete y todos los que le siguen, ya que por más que hayan llegado, se descartan para no perder el orden.

## 13. 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.C:\Users\Alfonso\Desktop\13.PNG

## 14. 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.

## C:\Users\Alfonso\Desktop\14.PNG

## 16.Utilice el comando netstat durante la ejecución del ejercicio 8 (A,C y D) para determinar y completar la siguiente información:

## A) Comando utilizado (debe incluir los argumentos utilizados con el comando netstat)

## B) Protocolo de transporte utilizado

## C) Puerto del servidor y nombre de la aplicación.

## D) Puerto del o los clientes y nombre de la aplicación.

A)

a) netstat -natp

b) TCP

c) 80 apache2

d) 56543

C)

a) netstat –natp

b) TCP

c) 80 apache2

d) 56565chromium-brows

56567firefox-bin

D)

a)

b)

c)

d)

## 17.¿Investigue como 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 que se diferencian estos tipos de comunicaciones del resto de los protocolos de aplicación vistos?

**Modo activo**

En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado.

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias. Para solucionar esto se desarrolló el modo pasivo.

**Modo pasivo**

Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1023 del servidor. Ejemplo: 2040) al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control (Ejemplo: 1036) hacia el puerto del servidor especificado anteriormente (Ejemplo: 2040).

La diferencia entre ftp y los demás protocolos de aplicación es que usa dos conexiones, una de control y una de datos, mientras que las otras solo utilizan una.

## 19.Dada la siguiente captura del comando netstat.

## Captura

## A) Que puede decir respecto de:

## i. ¿Qué protocolo o protocolos de transporte se observan?

TCP

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

11

## iii. ¿Cuántas conexiones hay establecidas en este momento?

5

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

Si

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

No

## vi. Liste los nombres de todos los procesos que representan el lado del servidor de la

## comunicación.

sshd

apache2

## vii. Liste los nombres de todos los procesos que representan el lado del cliente de la comunicación.

firefoxbin

epiphanybrows

## 20- ¿Cúal es el puerto por defecto que utiliza?

## i. Un servidor Web

80

## ii. Un servidor SSH

22

## iii. Un servidor DNS

53

## iv. Un servidor Web Seguro

443

## v. Un servidor POP3

110

## vi. Un servidor IMAP

143

## vii. Un servidor SMTP

25

## viii. Analice el archivo /etc/services (Linux) o c:\windows\system32\drivers\etc\services (Windows)

## ¿Qué información contiene?

Contiene los números de puerto para los servicios conocidos definidos por IANA.