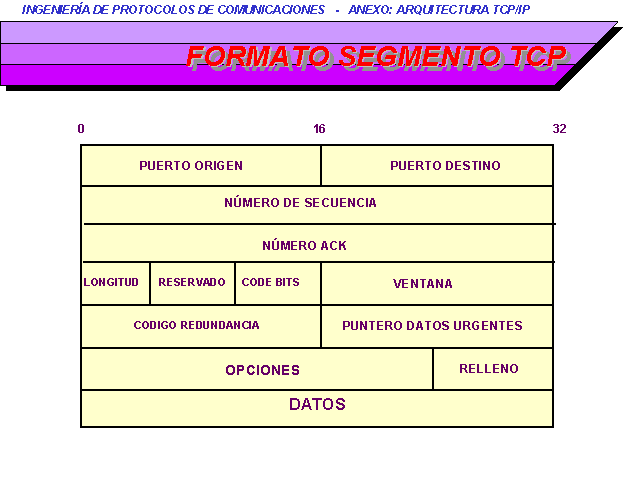
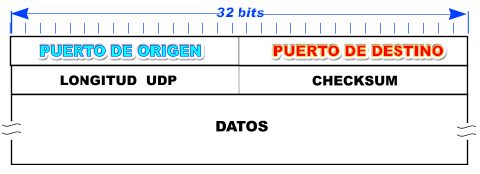
¿Cuál es la función de la capa de transporte?

La **capa de transporte** es el encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo. La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina destino, independientemente de la red de redes física en uno.

Describa la estructura del segmento TCP y UDP 

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

Los puertos son identificados por números de 16 bits, que indican a que aplicación corresponde cada dato entrante o saliente. Los primero 1023 puertos se encuentran restringidos para aplicaciones bien conocidas como el 80 que corresponde a HTTP y el 21 para FTP.

4. Compare TCP y UDP en cuanto a:

A) Confiabilidad

TCP asegura una conexión y transmisión de datos fiable mientras que UDP no asegura la correcta recepción de todos los datagramas.

B) Multiplexación

En UDP se envía un datagrama con numero de puerto origen y destino y se le asigna un puerto al socket que va a recibir el datagrama, en cambio en TCP el servidor tiene un puerto y socket (6789) asignado siempre esperando por conexiones nuevas, cuando se solicita una conexión a este socket se crea un nuevo socket del lado del cliente y por ese canal se empiezan a recibir y enviar datos, se identifican unívocamente gracias al puerto origen, ip de origen, puerto destino e ip destino

C) Orientado a la conexión

TCP es orientado a la conexión ya que genera un saludo de 3 vias antes de intercambiar datos, a diferencia de UDP que no necesita generar una conexión antes de inciar una transferencia.

D) Controles de congestión

TCP posee control de congestión y UDP no.

E) Utilización de puertos

TCP reserva el puerto 6789 para abrir conexiones entrantes en el lado del servidor

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)

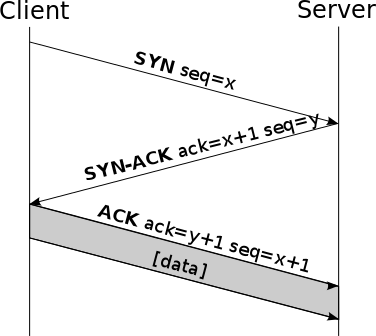
El campo protocolo.

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

A los paquetes UDP se los denomina datagrama, pero datagrama también se usa para definir a los paquetes de la capa de red .

6. Describa el saludo de tres vías de TCP.

### Establecimiento de la conexión (negociación en tres pasos)[[editar](http://es.wikipedia.org/w/index.php?title=Transmission_Control_Protocol&action=edit&section=7" \o "Editar sección: Establecimiento de la conexión (negociación en tres pasos))]

[](http://commons.wikimedia.org/wiki/File:Tcp-handshake.svg)

Negociación en tres pasos o *Three-way handshake*

Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un [*socket*](http://es.wikipedia.org/wiki/Socket_de_Internet) en un determinado [puerto TCP](http://es.wikipedia.org/wiki/Transmission_Control_Protocol#Puertos_TCP) y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete [SYN](http://es.wikipedia.org/wiki/SYN) inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor (este receptor también puede ser una PC o alguna estación terminal) se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto, pues se debe verificar que el dispositivo de destino tenga este servicio activo y esté aceptando peticiones en el número de puerto que el cliente intenta usar para la sesión. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit [RST](http://es.wikipedia.org/wiki/Flag_RST) activado, lo que significa el rechazo del intento de conexión. En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un [ACK](http://es.wikipedia.org/wiki/ACK), completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión. Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (*[spoofing](http://es.wikipedia.org/wiki/Spoofing" \o "Spoofing)*).

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?

Se devuelve un paquete RST

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?

Se devuelve un mensaje de unreacheable

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?

Multicast es el concepto de enviar datagramas a un grupo de hosts, trabaja con el protocolo UDP ya que envía información sin esperar respuesta, si tuviera que recibir una respuesta de cada uno de los participantes del grupo sería difícil de administrar

10.Utilice el comando netstat para obtener la siguiente información de su PC:

A) Para listar las comunicaciones TCP establecidas

Netstat- at

B) Para listar las comunicaciones UDP establecidas

Netstat -au

C) Obtener solo los servicios TCP que están esperando comunicaciones

Netstat -lt

D) Obtener solo los servicios UDP que están esperando comunicaciones

Netstat -lu

E) Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión

A los anteriores comandos se les agrega “ – p ” para mostrar el ID del proceso y el nombre del proceso que está asociado a ese socket

Web 80 / SSH 22 / DNS 53 / Web Seguro 443 / POP3 110 / IMAP 143 / SMTP 25

Se encuentran descriptos en la carpeta /etc/services