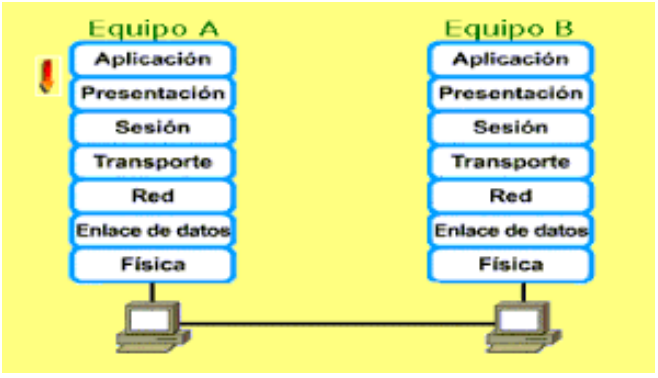
Jun Yamaki

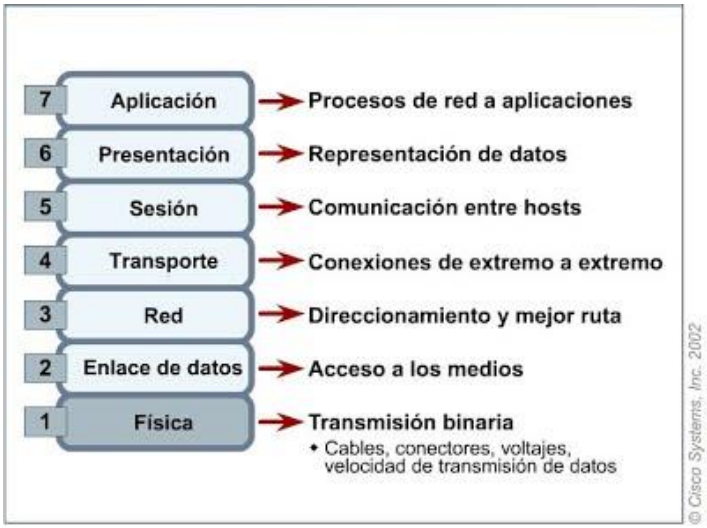
Entrega de carpeta de tarea individual: 11 de junio.
Preparación escrita 17 y 18 de junio 2019:

0) Complete la tabla:

Capa mod OSI	Capa mod TCP/IP	protocolo	MTU	device	Id source	Level function
7	Nivel de Aplicación	DHCP, FTP, etc.		Host		Procesos de red a aplicaciones
6	Nivel de Presentación	ASCII, SSL, etc.				Representación de datos
5	Nivel de Sesión	Puertos Lógicos				Comunicación entre hosts
4	Nivel de Transporte	TCP, UDP, SCTP				Conexiones extremo a extremo
3	Nivel de Red	IPv4, IPv6, ARP, ICMP	64KB, 4GB	Router		Direccionamiento y mejor ruta
2	Nivel de Enlace	MAC, PPP	1,5 KB	Switch		Acceso a los medios
1	Nivel Físico	Binario, Token Ring		Hub, repetidor		Trasmisión binaria

MODELO OSI





3ro BE
Año 2019

1) ¿Cuántos son los niveles o capas del modelo OSI y el objetivo del mismo?
2) ¿Qué funciones básicas describen los niveles?
3) ¿En qué niveles ubicaría los siguientes dispositivos: hub, switch, puente, adaptador de red, router, firewall, módem y servidor LAMP?
4) ¿A qué capas corresponden los siguientes protocolos: ETHERNET, ARP, TCP, ICMP. UDP, FTP, HTTPS, POP3, RIP ?

5)Indique a que nivel modelo OSI corresponden las siguientes funciones:

- Establecer una ruta para los datagramas CAPA: 3
- Diálogo horizontal que defina encriptación CAPA: 7
- Armar un archivo para visualizarse CAPA: 6
- Convertir señales en secuencia binaria CAPA: 1
- Verificar la integridad de los datos CAPA: 2
- Enviar un e-mail CAPA: 7
- Recibir un acuse recibo de segmento CAPA: 4
- Comprobar la dirección MAC destino. CAPA: 2

Respuestas

1) El modelo OSI es un modelo que consta de 7 capas con el objetivo de hacer una referencia normalizada para las comunicaciones, para lograr la comunicación entre los diferentes dispositivos.

2) **Capa 1:** Realizar la comunicación de la red a nivel físico, es decir por medio de bits ya sea por electricidad o luz, etc.
   Capa 2: Realizar direccionamiento físico mediante MAC u otras.
   Capa 3: Realizar enrutamiento mediante IP.
   Capa 4: Realizar el transporte de datos independizándole del tipo de red física utilizada
   Capa 5: Mantener y controlar el enlace establecido entre dispositivos.
   Capa 6: Se encarga de la representación de la información, de forma que los datos sean reconocibles.
   Capa 7: Ofrece a las aplicaciones la posibilidad de acceder a los servicios de otras capas y define los protocolos para intercambiar los datos.

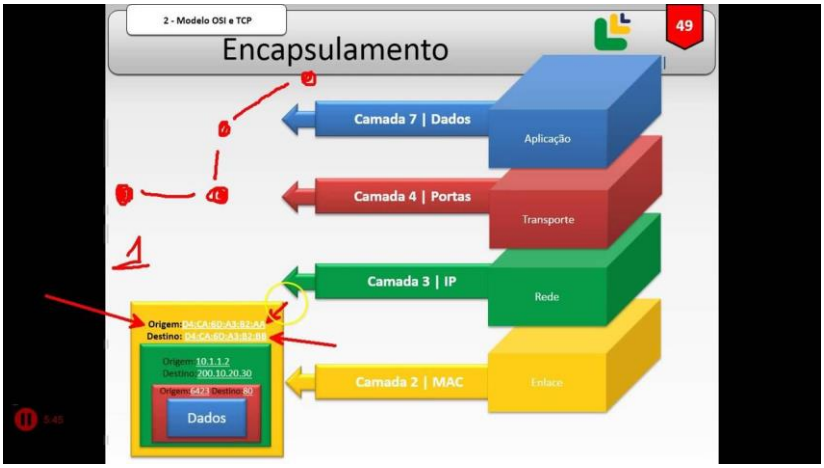
3) **Hub** capa 1 física
   Switch capa 2 enlace
   Puente capa 2 enlace
   Adaptador de red capa 2 enlace
   Router capa 3 red

Firewall Existen varios tipos que van desde las primeras 3 capas hasta los que aplican en capa de aplicación que serían los más modernos.
Modem capa 1 física
Servidor LAMP capa 7 aplicación

4) **ETHERNET:** capa 2 enlace
ARP: capa 2 enlace
TCP: capa 4 transporte
ICMP: capa 3 red
UDP: capa 4 transporte
FTP: capa 7 aplicación
HTTPS: capa 7 aplicación
POP3: capa 7 aplicación
RIP: capa 3 red

MODELO TCP/IP

1) ¿Qué diferencias existen entre modelos OSI y TCP/IP?
2) ¿Qué es TCP/IP?

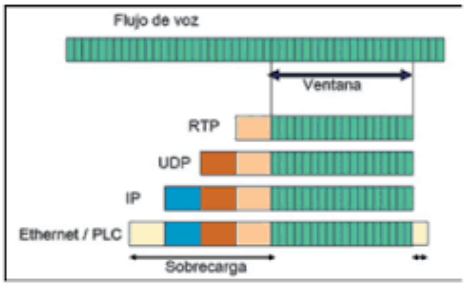


Respuestas

1) El modelo TCP/IP engloba lo correspondiente a la capa 7, 6 y 5 (que serían las capas lógicas del modelo OSI) como Capa de aplicación, también a la capa de red se le refiere como capa de internet y las capas 2 y 1 del modelo OSI las engloba como capa de acceso a la red
2) Hace referencia a el conjunto de protocolos resaltando el Protocolo de control de trasmisión (TCP) y el Protocolo de internet (IP)

ENCAPSULAMIENTO

Fig. 1. TRANSPORTE DE VOZ EN REDES PLC



Fuente: autores.

1) ¿Dónde se realiza la verificación total de un mensaje de red?
2) ¿Qué es el método CRC aplicado al FCS?
3) Ordene la secuencia de encapsulamiento:
   - datagrama
   - trama ethernet
   - segmento TCP
   - archivo normalizado
4) ¿Qué es un PDU? Indique los diferentes PDU.
5) ¿Qué es el MTU e indique los diferentes valores para diferentes PDU?
6) ¿CÓMO SE LLAMAN LOS MENSAJES DE RED SEGUN EL CONTENIDO?
   Lo que transportan los PDU en el área de datos.

Respuestas:

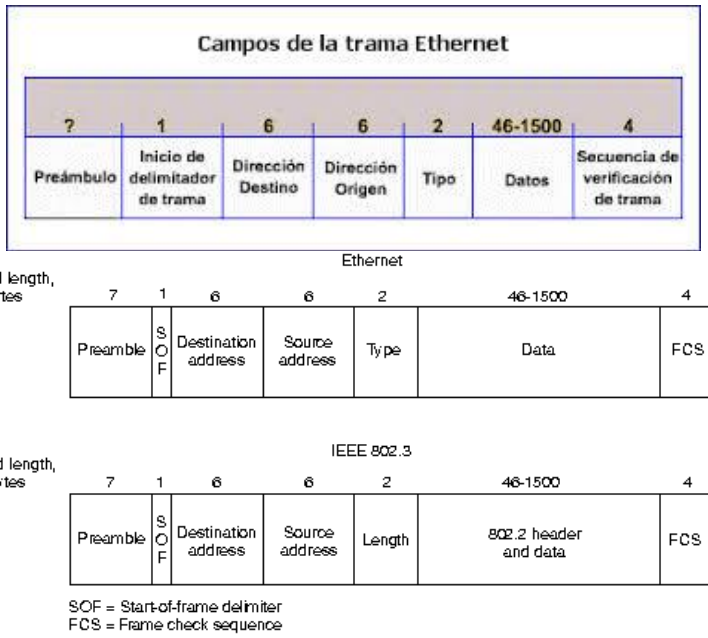
1) la última verificación se realiza en la capa 5.
2) el CRC es un código cíclico utilizado para detección de errores, el cual se usa como FCS
3) 1- Archivo normalizado
   2- Segmento TCP
   3- Datagrama
   4-Trama ethernet
4) PDU son las unidades de datos de protocolo, es decir la unidad de datos que se utiliza para el intercambio según la capa del modelo siendo estas correspondiente a su capa
   De la capa 7 a la 5 se utilizan Datos en sí mismos (clasificados como APDU, PPDU, SPDU correspondientemente), en la 4 se usan segmentos (TPDU), en los 3 paquetes, en la 2 trama, en la 1 bits.
5) MTU es la unidad de transferencia máxima:
   a. **IPv4** 64KB
   b. **IPv6** 4GB
   c. **Tokenring** 8KB
   d. **Ethernet** 1,5 KB

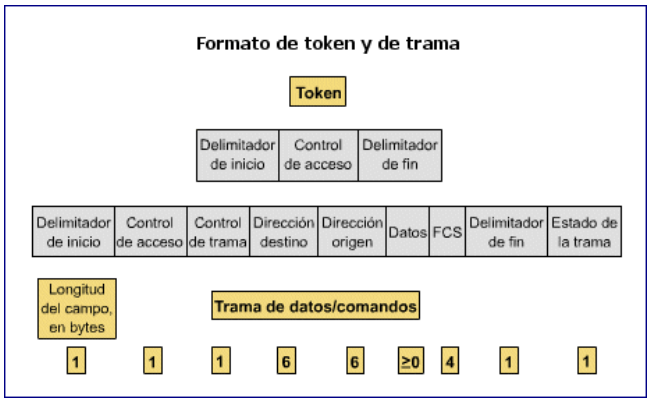
6) **No lo encontre**

TRAMA NIVEL ENLACE DE RED

1) ¿Cuál es la función del preámbulo?
2) ¿Cómo define las direcciones MAC?
3) ¿Para qué sirve el campo length de la cabecera IEEE802.3?
4) ¿Qué comprenden los protocolos IEEE802?
5) ¿Qué es un token?

6) ¿Qué es una red determinista?
7) ¿Cómo una red token ring nivela la velocidad de cada host?



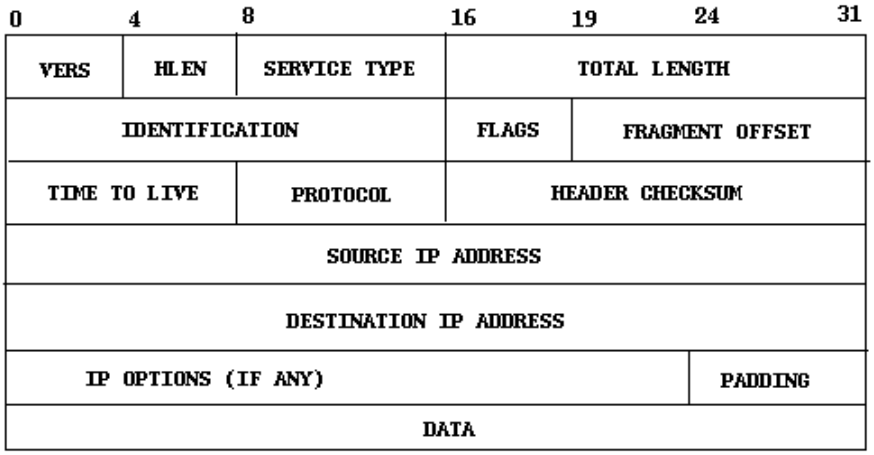


Respuestas

1) El preámbulo tiene como función portar la muestra para la sincronización de dispositivos
2) Son 6 bytes expresados en 4 campos hexadecimales de 2 dígitos cada uno, un total de 48 bits las cuales son asignadas a los dispositivos al momento de su fabricación

3) Indica el largo total de la trama el máximo valor aceptable es 1535 pese a esto, el largo total no debe ser superior a 1526
4) Los protocolos IEEE 802 comprenden los estándares a utilizar en redes LAN y MAN refiriéndose en las dos capaz inferiores del modelo OSI estando dentro de los mismos, por ejemplo, ethernet 802.3, wifi 802.11 entre otros
5) El token o testigo es el medio de trasmisión de datos en Tokenring significando que los mensajes se emiten en el cuando le corresponde a el ordenador tener el token, a este se le carga la información y el continua su camino hasta destino, solo puede ser cargado si no esta en uso ya actualmente y a este se le puede determinar prioridades sobre ciertos host de la red siendo así determinista.
6) Que sea determinista significa que no esta implicado el azar es decir que el sistema esta planeado su funcionamiento con exactitud siendo así predecible su comportamiento en las situaciones.
7) El sistema Tokenring prioriza de forma normal los que más información envían de esta forma nivela la velocidad de trabajo de la red, es decir que aquellos que requieren enviar mayor cantidad de información en menor tiempo perciben mas velocidad real y los que envían menos perciben menor velocidad, todo esto da como resultado que en cualquier caso la velocidad de la red se debería percibir como la misma sin importar si es el host que más información manda o el que menos manda

DATAGRAMA



1) ¿Cómo se forma el identificador de trama?
2) ¿Qué es la fragmentación de tramas y dónde se produce?
3) ¿Cómo define una dirección IPv4?
4) ¿Cuáles son las reglas para el direccionamiento IPv4?
5) ¿Cómo clasifica las direcciones IPv4?
6) ¿Qué función tiene el campo ttl y qué valores indica?

1) en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El emisor del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red. El valor asignado en este campo debe ir en formato de red.
2) es un mecanismo que fragmentar en diversos bloques de datos llamados fragmentos si su tamaño sobrepasa la MTU. El protocolo IP solamente fragmenta un datagrama cuando la

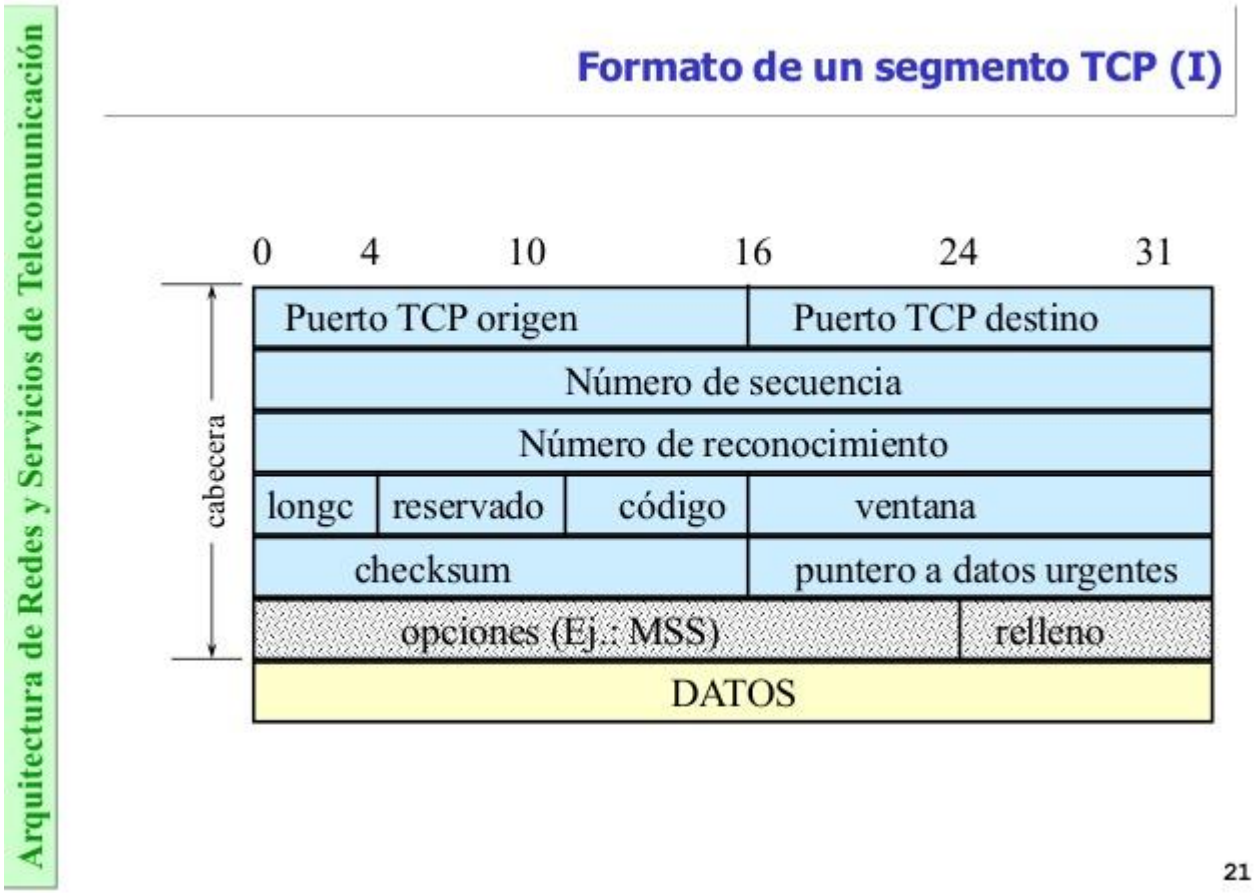
MTU del medio por donde se tiene que encaminar tiene un tamaño menor que el del datagrama.

3) Se define con 4 campos que van del 0 al 255 formando un total de 256 valores por campo que se separan por “. “se podría decir que son 8 bits por campo
4) Algunas IP tienen uso especial y no puede utilizarse para host ni red, los identificadores de red o host 0 están restringidos a indicar la red u el host de la red local y los campos 255 están restringidos a difusión siendo un 255.255.255.255 un mensaje a todos los de la red y si solo son los valores de host en 255 son la red que se dejó el identificador.
5)
    a. REDES CLASE A
       bit de mayor peso o de clasificación de Clase '0'.
       Rango: 1.0.0.0 hasta:127.255.255.255
       Privadas: 10.0.0.0 hasta: 10.255.255.255
       Redes Omitidas: 0.0.0.0 (default) y 127.0.0.1 (loopback).
       Máscara por defecto: 255.0.0.0
    b. REDES CLASE B
       bits de mayor peso o de clasificación de Clase '10'.
       Rango: 128.0.0.0 hasta: 191.255.255.255
       Privadas: 172.16.0.0 hasta: 172.31.255.255
       Máscara por defecto: 255.255.0.0
    c. REDES CLASE C
       bits de mayor peso o de clasificación de Clase '110'.
       Rango: 192.0.0.0 hasta: 223.255.255.255
       Privadas: 192.168.0.0 hasta: 192.168.255.255
       Máscara por defecto: 255.255.255.0
    d. REDES CLASE D
       bits de mayor peso o de clasificación de Clase '1110'.
       Rango: 224.0.0.0 hasta 239.255.255.255
       Máscara por defecto: 255.255.255.255
       Motivo de la Red: Direcciones de 'BroadCasting'.
    e. REDES CLASE E
       bits de mayor peso o de clasificación de Clase '1111'.
       Rango: 240.0.0.0 hasta: 255.255.255.255
       Motivo de la Red: Restringido.

6) Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en, como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado. Típicamente toma el valor 64 o 128 en los datagramas.

SEGMENTO TCP

1) ¿Qué es una dirección de puerto de red o virtual?
2) ¿Cuántos bits y qué forma de indicación la describen?
3) ¿Cuántos puertos existen?
4) ¿Qué son los puertos bien conocidos?
5) ¿Qué puerto predeterminado se usa para:?
    - SQUID O PROXY
    - FTP UDP
    - FTP TCP
    - POP3
    - HTTP
6) ¿Qué es el acuse recibo en TCP?
7) ¿Qué es el método de ventana deslizante para TCP?



1) Se denomina “puerto lógico” a una zona o localización de la memoria de acceso aleatorio (RAM) de la computadora que se asocia con un puerto físico o un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.
3) existen 65536 puertos
4) Son puertos asignados por la IANA, van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios. Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones. Algunos ejemplos son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80).
5)
    a. SQUID O PROXY Puerto: 3128
    b. FTP UDP Puerto: 69
    c. FTP TCP Puerto: 21
    d. POP3 Puerto: 110
    e. HTTP Puerto: 80

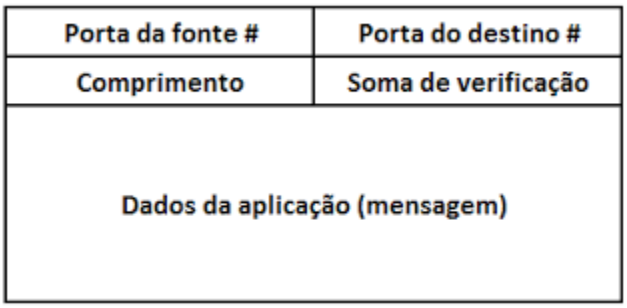
6) Una de las funciones del TCP es asegurar que cada segmento llegue a su destino. Los servicios TCP en el host de destino envían a la aplicación de origen un acuse de recibo de los datos recibidos.

El número de secuencia y el número de acuse de recibo del encabezado del segmento se utilizan para confirmar la recepción de los bytes de datos contenidos en los segmentos. El número de secuencia es el número relativo de bytes que ha sido transmitido en esta sesión más 1 (que es el número del primer byte de datos en el segmento actual). TCP utiliza el número de acuse de recibo en segmentos que se vuelven a enviar al origen para indicar el próximo byte de esta sesión que espera el receptor. Esto se llama acuse de recibo de expectativa.

7) La ventana deslizante es un dispositivo de control de flujo de tipo software, es decir, el control del flujo se lleva a cabo mediante el intercambio específico de caracteres o tramas de control, con los que el receptor indica al emisor cuál es su estado de disponibilidad para recibir datos.
   Este dispositivo es necesario para no inundar al receptor con envíos de tramas de datos. El receptor al recibir datos debe procesarlo, si no lo realiza a la misma velocidad que el transmisor los envía se verá saturado de datos, y parte de ellos se pueden perder. Para evitar tal situación la ventana deslizante controla este ritmo de envíos del emisor al recepto

SEGMENTO UDP

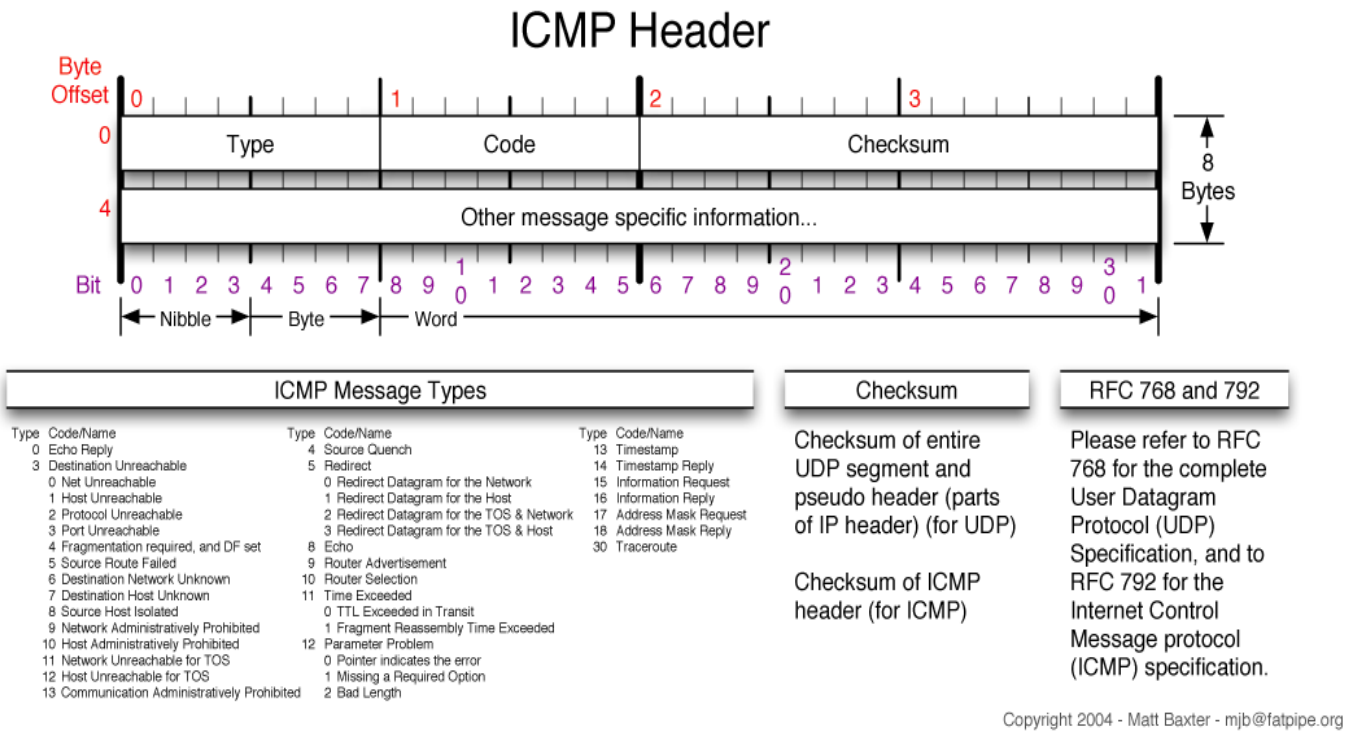
1) ¿Cuáles son las características del protocolo UDP?



1) Las características principales de este protocolo son:
   a. Trabaja sin conexión, es decir que no emplea ninguna sincronización entre el origen y el destino.
   b. Trabaja con paquetes o datagramas enteros, no con bytes individuales como TCP. Una aplicación que emplea el protocolo UDP intercambia información en forma de bloques de bytes, de forma que, por cada bloque de bytes enviado de la capa de aplicación a la capa de transporte, se envía un paquete UDP.
   c. No es fiable. No emplea control del flujo ni ordena los paquetes.
   d. Su gran ventaja es que provoca poca carga adicional en la red ya que es sencillo y emplea cabeceras muy simples.

MENSAJE ICMP

1) Qué comandos de red usan ICMP?
2) Cuál es el uso del mensaje echo reply?
3) ¿Cuáles son los tipos de mensajes del código de ICMP?



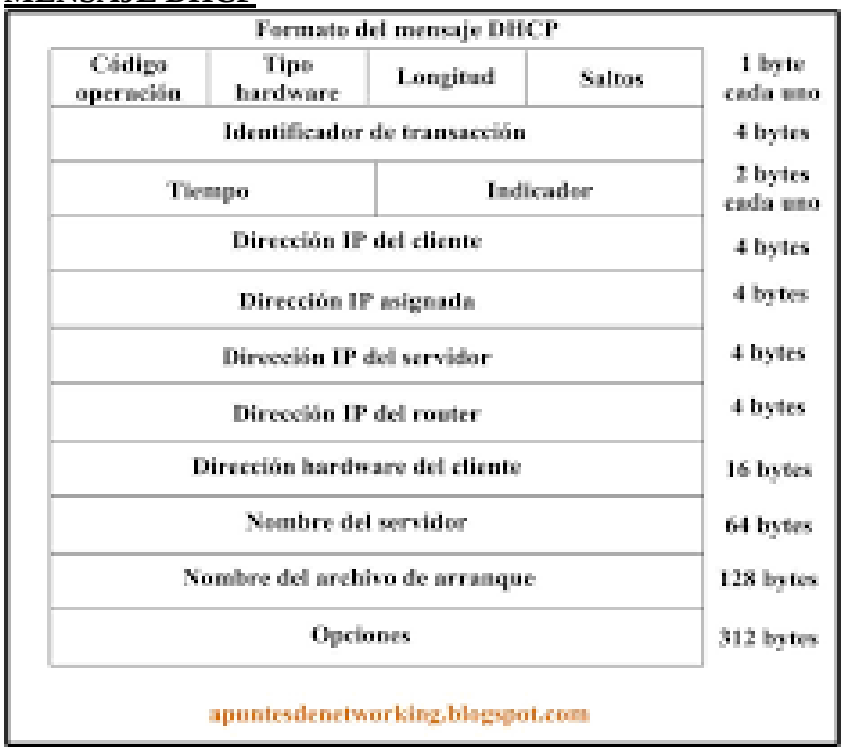
1) El principal comando que usa ICMP es Ping
2) Es la respuesta generada a un echo request que es como funciona el conocido ping
3)

TIPO	CÓDIGO	Descripción
0	0	Echo Reply (respuesta de eco a un comando ping)
3	0	Network Unreachable (red inalcanzable)
3	1	Host Unreachable (host inalcanzable)
3	2	Protocol Unreachable (protocolo inalcanzable)
3	3	Port Unreachable (puerto inalcanzable)
3	4	Fragmentation needed but no-frag. bit set (es necesaria la fragmentación, pero se ha establecido el bit de no-fragmentar)
3	5	Source routing failed (ha fallado el encaminamiento exigido en origen: se ha especificado el camino/enrutado que deben seguir los paquetes y uno de los puntos de la ruta no está disponible)
3	6	Destination network unknown (dirección de destino desconocida)
3	7	Destination host unknown (host de destino desconocido)
3	8	Source host isolated (host de origen aislado; este tipo está obsoleto)
3	9	Destination network administratively prohibited (red

TIPO	CÓDIGO	Descripción
		de destino prohibida administrativamente)
3	10	Destination host administratively prohibited (host de destino prohibido administrativamente)
3	11	Network unreachable for TOS (red inalcanzable para el TOS, el tipo de servicio)
3	12	Host unreachable for TOS (host inalcanzable para el TOS)
3	13	Communication administratively prohibited by filtering (comunicación prohibida administrativamente mediante filtrado)
3	14	Host precedence violation (violación del precedente del host)
3	15	Precedence cutoff in effect (está actuando el límite de precedente)
4	0	Source quench (le indica al origen "que se calme un poco" porque está saturando la capacidad de proceso del receptor; actualmente está en desuso para no saturar aún más la comunicación)
5	0	Redirect for network (indica que debes redireccionar tus comunicaciones a otra red)
5	1	Redirect for host (indica que debes redireccionar tus comunicaciones a otro host)
5	2	Redirect for TOS and network (indica que debes redireccionar tus comunicaciones con otro TOS y a otra red)
5	3	Redirect for TOS and host (indica que debes redireccionar tus comunicaciones con otro TOS y a otro host)
8	0	Echo request (petición de eco/ping)
9	0	Router advertisement (aviso de existencia del enrutador: "¡Hola, estoy aquí!")
10	0	Router solicitation (solicitud de existencia de enrutador: "¿Hay alguien ahí?")
11	0	TTL equals 0 during transit (TTL igual a 0 durante el tránsito: al paquete se le ha acabado su tiempo de vida antes de alcanzar su destino)
11	1	TTL equals 0 during reassembly (TTL igual a 0 durante el reensamblado: si un paquete ha sido fragmentado y durante su reensamblaje el TTL llega a 0, se genera este error)
12	0	IP header bad (catchall error) [cabecera IP errónea (error de "cajón de sastre", o error para todo lo que no

TIPO	CÓDIGO	Descripción
		esté especificado en otro sitio; o si lo prefieres, error por defecto)]
12	1	Required options missing (faltan opciones requeridas)
13	0	Timestamp request (petición de la hora en origen: "¿Qué hora es ahí?"; está obsoleto)
14		Timestamp reply (respuesta a la petición de hora: "Son las ..."; está obsoleto)
15	0	Information request (petición de información; está obsoleto)
16	0	Information reply (respuesta a la petición de información; está obsoleto)
17	0	Address mask request (petición de máscara de red: cuando un host sin disco duro se inicializa, efectúa una petición para saber qué máscara de red debe utilizar)
18	0	Address mask reply (respuesta a la petición de máscara de red)

MENSAJE DHCP



1) ¿Qué características posee DHCP?
2) ¿Qué variables son incluidas en el PDU DHCP?

1) **Características de DHCP.**
   a. Administración más sencilla.
   b. Configuración automatizada.
   c. Permite cambios y traslados.
   d. Posibilidad de que el cliente solicite los valores de ciertos parámetros.
   e. Nuevos tipos de mensajes de **DHCP** que soportan interacciones cliente/servidor robustas.

2)

Código	Nombre	Largo	Nota
0	Pad	0 octetos	Puede ser usada para acolchar otras opciones para que se alineen al límite de la palabra; no es seguida por el byte de largo
1	Subnet Mask	4 octetos	Debe ser enviada después de la opción Router (opción 3) si ambos están incluidos
2	Time Offset	4 octetos	
3	Router	múltiplos de 4 octetos	Enrutadores disponibles, listados en orden de preferencia
4	Time Server	múltiplos de 4 octetos	Servidores de tiempo de red con los cuales sincronizarse, listados en orden de preferencia.

Código	Nombre	Largo	Nota
5	Nombre Server	múltiplos de 4 octetos	Servidores de nombres IEN 116 disponibles, deben ser listados en orden de preferencia.
6	Domain Nombre Server	múltiplos de 4 octetos	Servidores de DNS disponibles, deben ser listados en orden de preferencia.
7	Log Server	múltiplos de 4 octetos	Servidores de registros disponibles, deben ser listados en orden de preferencia.
8	Cookie Server	múltiplos de 4 octetos	"Cookie" en este caso significa "galleta de la fortuna" o "cita del día", una anécdota humorística enviada frecuentemente como parte del proceso de logon en grandes computadores; no tiene nada que ver con las cookies enviadas por sitios web.
9	LPR Server	múltiplos de 4 octetos	
10	Impress Server	múltiplos de 4 octetos	
11	Resource Location Server	múltiplos de 4 octetos	
12	Host Nombre	mínimo de 1 octeto	
13	Boot File Size	2 octetos	Largo de la imagen de boot en bloques de 4KiB
14	Merit Dump File	mínimo de 1 octeto	Ruta donde los vaciados en caso de error deben guardarse
15	Domain Nombre	mínimo de 1 octeto	
16	Swap Server	4 octetos	
17	Root Path	mínimo de 1 octeto	
18	Extensions Path	mínimo de 1 octeto	
255	End	0 octetos	Usado para marcar el final del campo de opciones del fabricante