Modelo de parcial

TL 5 y 6

Redes

FRBA - 2o cuatrimestre 2022

1. En relación con el Nivel 2 (TCP/IP).

1.1 ¿Es una trama de comunicación unicast, multicast o broadcast? ¿Qué valor tiene el campo que verifica la respuesta anterior?

1.2 ¿Es una trama correspondiente a la VLAN por defecto o a una VLAN de negocios?¿Qué valor o característica del encabezado verifican su respuesta?

1.3 ¿Qué valor tiene el grupo HEXA que indica el inicio de los datos de la trama?¿Cuál es la longitud del campo de datos?

1.4 ¿Este campo de datos será del mismo tamaño en otra trama que tenga los mismos hosts origen y destino? ¿Qué longitud deberá tener?

1.5 ¿Qué valor HEXA indica el inicio del encabezado de la PDU especificada en IEEE802.2?

1.6 ¿Qué valor HEXA indica el inicio del encabezado de la PDU especificada en IEEE802.3?

1.7 ¿Qué valor HEXA indica el protocolo de nivel 3 (TCP/IP) encapsulado en la trama?

1.8 ¿Cuál es el protocolo encapsulado en la trama?

Contenidos posibles capa 2

Protocolos:

- **802.3 (CSMA/CD)**
- VLAN tagging (802.1Q)
- 802.2 (LLC).
- Ethernet. 802.11 (wireless)

Cómo reconocer

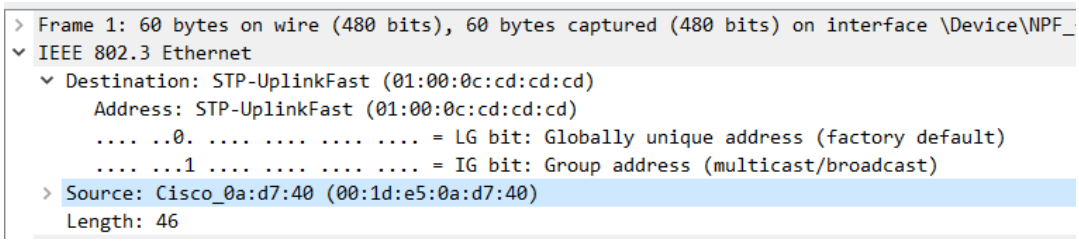
1.1 Trama uni-, multi- o broadcast?

En Ethernet:

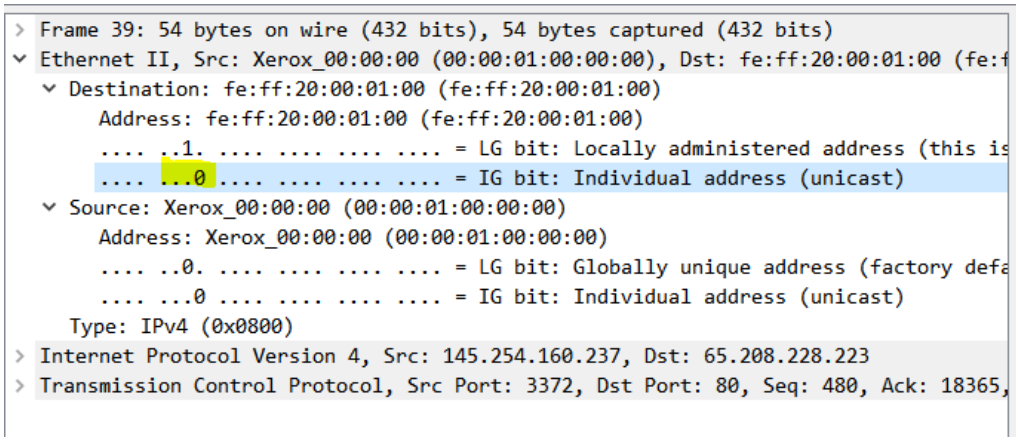
Se revisa la dirección MAC destino (primeros 6 bytes o 12 dígitos hexa):

- Broadcast: FF FF FF FF FF FF (12x F, o todos 6 bytes de 1s en binario).
- Multicast: el último bit del primer byte es 1 (esto es el último bit de la segunda letra hexa de la MAC. Hay que pasarla a binario!).
    - Si es una multicast de ipv4, empieza con 01:00:5e y el siguiente bit a eso es 0. A esto se suma que la IP destino debería empezar con 1110 y estar entre 224.0.0.0 y 239.255.255.255.
    - Según Koval: 0000 5e00 0000 hasta 0000 5eff ffff son multicast
- Unicast: todas las demás MAC.

Trama multicast:



Trama unicast:

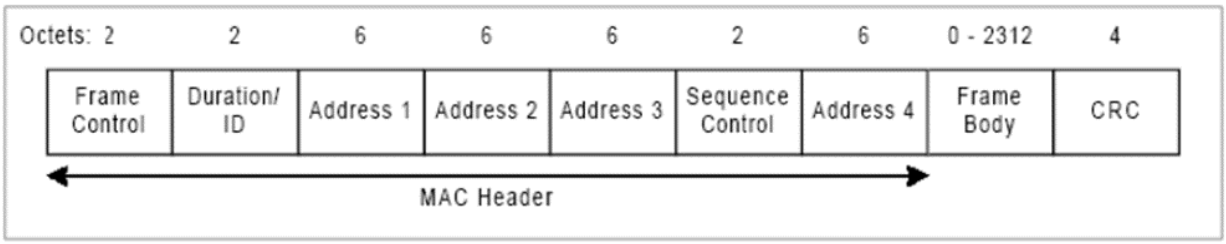


```
fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
00 28 0f 5c 40 00 80 06  91 d8 91 fe a0 ed 41 d0
e4 df 0d 2c 00 50 38 af  ff f3 11 4c a9 48 50 10
24 14 31 71 00 00
```

En 802.11 /wireless

- Las direcciones MAC relevantes empiezan en el 5o byte.
- ToDS y FromDS determinan qué dirección hay en cada campo. Estos son los primeros 2 bits del segundo byte del Frame Control
- Revisar si la DA (o quizás RA) es uni-, multi- o broadcast.

Trama completa:



Frame control:

Address fields:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Address fields: son 4 campos, aunque la mayoría de las veces se transmiten sólo 3. Los valores de cada dirección dependen de los valores de los campos ToDS y FromDS en Frame Control (to/from Distributed System, o sea, enviado al AP o por el AP).

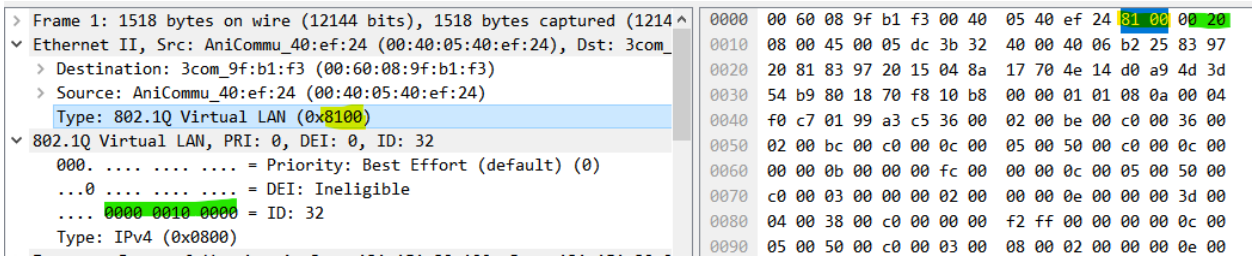
- DA: Destination adress (destino final de la transmisión)
- SA: Source Addresss (dirección de origen real, la que inicia la transmisión)
- BSSID: ID del BSS.

Si ToDS = FromDS = 1 (transmisión de un Access Point a otro):

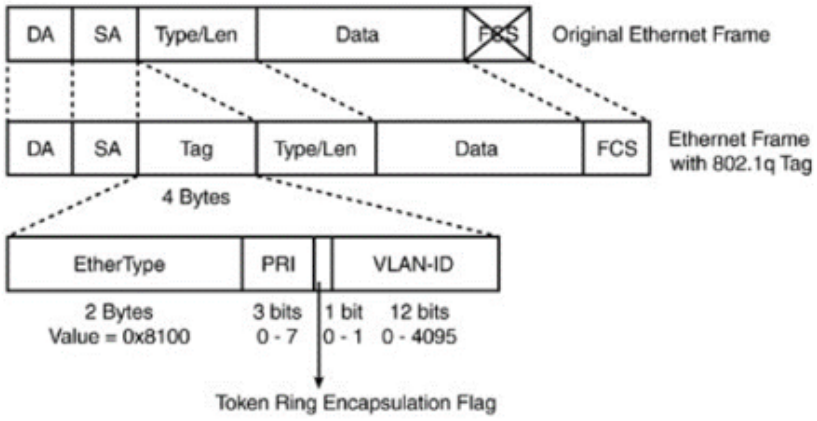
- RA: Receiver Address. El dispositivo que va a recibir esa trama
- TA: Transmitter Address. AP que transmite el mensaje.

1.2 VLAN de negocio o por defecto?

- Trama 802.1Q (con VLAN): en la cabecera Ethernet, el type es 0x8100 (amarillo)
    - ID de VLAN: En el tag VLAN, el ID son los bits 5 a 16 (verde) (saltea la primer letra hexa, y son las siguientes 3 letras).
- Si no hay tag, es por defecto.



VLAN tagging (802.1Q)



1.3 Dónde empiezan los datos?

- Empiezan después de:
  - Ethernet Tag (sin VLAN): 14 bytes (14 pares de letras)
  - Ethernet + Tag VLAN 802.1Q: 14 bytes + 4 bytes
  - Si hay LLC????

Si tiene VLAN, los campos vienen en este orden:

- DA / SA (MACs destino y origen Ethernet)
- Ethertype: 8100
- 4 bits (PRI y Token encapsulation Ring)
- VLAN ID (12 bits)
- Type/Len: 2 bytes. Normalmente esto va a ser 0x0800 (IPv4), pero podría ser ARP, RARP, etc.
  - LEN: Si el valor es menor a 0x600 (1536 decimal), este campo es LENGTH.
  - Ethertype: Si el valor es mayor a 0x600 (1536 decimal), es un campo type. Lista completa de tipos en Wikipedia.
    - 0x0800 → IPv4
    - 0x0806 → ARP
    - 0x8035 → RARP (NO es respuesta a ARP)
    - 0x86DD → IPv6
    - 0x8100 → VLAN TAGGING (ojo, cambia el formato del resto del paquete! El tag tiene 4 bytes, y después lo sigue el Ethertype de 2 bytes)

1.4 Tamaño del campo de datos

- El campo de datos de Ethernet puede tener entre 0 y 1500 bytes. Si tiene menos de 46 bytes, se usa el campo padding después de los datos para rellenar hasta ese tamaño
    - A veces, la longitud está indicada en el campo len/type (en 802.3, después de dirección destino / origen - en 802.1q, al final del VLAN tag).
- El tamaño posible de su contenido puede ser:
    - IPv4: variable, máximo: 2^16 bytes (65.536). Se ve en el campo longitud total (da tamaño de todo el PDU IP, incluyendo cabecera).
    - ARP: 28 bytes exactos (+ 18 de padding para completar el tamaño mínimo de trama de Ethernet)
    - LLC: variable. Variable. Múltiplos de 8 bits.

1.5 y 1.6 Inicio de PDU

- En IEEE802.2 (LLC):
    - Este campo sólo está presente cuando se usa 802.3 (y no Ethernet 2). Por eso empieza después del campo LEN (que es un campo Ethertype/Length con valor menor a 0x0600). Este campo puede estar al final de la cabecera de una trama ~~Ethernet 2~~, 802.3 o un VLAN tag.
      Teoría de Vicky: en todos los ejemplos de LLC que vi, el campo anterior es LEN, y no Ethertype (o sea, el valor es menor a 0x0600)
- En 802.3 (LAN/Ethernet):
    - MAC destino. Esto es el inicio del PDU visible en la trama capturada.
    - ~~Preámbulo (técnicamente, empieza con esta porción para sincronizar, pero no se ve en Wireshark)~~
        - ~~En 802.3: 7 octetos de 10101010 + 1 de 10101011 (7x 0xAA + 1x 0xAB)~~
        - ~~En Ethernet: 8 octetos de 10101010 (8x 0xAA)~~

1.7, 1.8 Qué protocolo de nivel 3 hay encapsulado?

Opciones encapsuladas posibles	No son de nivel 3!
Ethertype • 0x0800 → IPv4 (capa 3) • 0x86DD → IPv6 (capa 3)	Cosas de otros niveles indicadas por el Ethertype:

• 0x0806 → ARP (CAPA 3 ~~o 2~~) • 0x8035 → RARP (CAPA 3 ~~o 2~~ - NO es respuesta a ARP) • ICMP (según Koval, ICMP es capa 3, pero está encapsulado dentro de IP, también capa 3 - el protocolo ICMP está indicado en el campo protocolo de IP)	• 0x8100 → VLAN TAGGING (ojo, cambia el formato del resto del paquete! (capa 2) Otros protocolos • Nivel 2: HDLC, LAP-B, PPP, **LLC** • Nivel 4: TCP, SPX, UDP • Otros superiores a 3: Telnet, DNS, FTP, HTTP, SNMP, SMTP, Ping, FTP

Caso 1: Trama Ethernet común

- Empieza con 2 MAC address (2x 6 bytes)
- PROTOCOLO: Ethertype or length (2 bytes). (Ethertype > 0x600, LEN < 0x600)

Caso 2: Trama Ethernet 802.1Q (VLAN tagging)

- Empieza con 2 MAC
- Ethertype: 0x8100 (VLAN tagging)
- 2 bytes adicionales (flags + ID de VLAN)
- Type/Len con el protocolo encapsulado (ver opciones en caso 1). (Ethertype > 0x600, LEN < 0x600)

Caso 3: Trama con LLC

- LLC es capa 2, hay que detectar dónde termina.

Caso 4: Trama wireless

- ????

Respuestas de parcial original

GG (1C22)	AM (2C21 - Promocionó)
1.1) Es una trama de comunicación unicast. El bit que indica que tipo de trama de	1.1) Unicast. C0 01 14 7C 00 01 1.2) No tiene VLAN. No implementa 802.1Q 1.3) 00 . Longitud: 0 1.4) No lo sabes porque no conoces el

comunicación es el IG bit que es el último bit del primer octeto y tiene valor 0 1.2) Es una trama correspondiente a una VLAN por defecto ya que sino el campo de Type debería tener el hexa 8100 indicando que se trata del protocolo 802.1Q. 1.3) El valor del grupo hexa que indica el inicio de los datos es "0x73" y la longitud es de 536 bytes. 1.4) No necesariamente, el campo de datos en el protocolo IPv4 no tiene una longitud fija. ~~1.5) El valor en Hexa es "0xAB" que representa el primer octeto y pertenece al preambulo~~ ~~1.6) El valor en Hexa es "0xAB" que representa el primer octeto y pertenece al preámbulo~~ **1.7) 0x0800** ~~1.8) El protocolo encapsulado en la trama es TCP IPv4~~	contexto de la otra trama. Podría ser otro protocolo. 1.5) 94 (inicio de la MAC destino) 1.6) No hay 802.3. **1.7) 0800** ~~1.8) Se encapsula el protocolo TCP.~~

2. En relación con el Nivel 3 (TCP/IP)

2.1 ¿Esta captura representa una PDU única, un fragmento intermedio o el último fragmento?, en cualquier caso ¿qué valor tiene el grupo HEXA del campo que identifica el paquete?

2.2 ¿Cuál es la dirección de la RED destino (Nivel IP) a la cual se encamina este paquete?

2.3 ¿qué valor tiene la dirección del HOST origen desde donde proviene el paquete?

2.4 ¿en algún campo del encabezado y con qué valor HEXA se indica que es un paquete que ofrece un servicio confiable?

2.5 ¿qué valor HEXA del encabezado IP indica que el protocolo brinda un servicio de entrega ordenada?

2.6 ¿qué valor HEXA del encabezado IP indica que el fragmento podrá ser reensamblado por el HOST destino, en la posición correcta dentro de la PDU en caso de ser necesario?

Contenidos posibles de nivel 3

- Técnicamente, capa 3 es: IP, ARP, RARP, ICMP o RP.
    - Dentro de IP, en capa 4, puede haber: UDP (no confiable) o TCP (confiable).

Respuestas posibles

2.1 Reconocer fragmentación

- ARP/RARP no se fragmenta
- ICMP
    -
- IP
    - Revisar los flags
        - 1) El primero no importa
        - 2) No fragmentar (DF). Debería estar en 0 si se fragmentó.
        - 3) Más fragmentos (MF). Debería estar en 1 si vienen más fragmentos. Pero puede estar en 0 tanto si es el último fragmento como si no se fragmenta.

- Revisar el desplazamiento de fragmento. Si es 0, o no se fragmentó o es el primer fragmento. Si es > 0, es un fragmento. Si es > 0 y MF = 0, es el último fragmento.

2.2 y 2.3 IPs de origen y destino

Ver campos Dirección IP origen y Direccion IP destino. Están en este orden, que es al revés que en Ethernet.

Si pide la RED de origen o destino, se podría decir que se asume que es de clase X y que tiene la máscara correspondiente a la clase.

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0 /8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0 /16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0 /24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*

2.4 Es un servicio confiable?

- IP: NO. IP no es confiable
- ARP/RARP:
- ICMP:
- RP:

2.5 Servicio de entrega ordenada en encabezado IP

- IP: NO. No orientado a la conexión, por lo que no necesariamente entrega paquetes ordenados.
- ARP/RARP: No necesita ser ordenado. Su tamaño es menor a un MTU.
- ICMP: No necesita ser ordenado. Su tamaño es menor a un MTU.

2.6 Indicación de que el fragmento puede ser reensamblado en la posición correcta.

El campo desplazamiento de fragmento permite reensamblar el paquete. Se puede mencionar también el flag Más Fragmentos, que nos indica si termina el paquete ahí o no.

Respuestas originales

GG (1C22)	AM (2C21 - Promocionó)
2.1) Representa una PDU única. El grupo hexa que identifica el paquete tiene el valor "0x0000" 2.2) 1.1.23.0 2.3) 1.1.12.1 2.4) No aplica 2.5) "0xa6c89a16" que representa el número de secuencia ~~2.6) No aplica, es parte del protocolo de Nivel 2 indicar en qué posición del fragmento se encuentra~~	2.1) PDU única. 00. 2.2) 1.1.12.1 /8 2.3) 1.1.23.3 2.4) TCP es un servicio confiable. Checksum: 15AB. 2.5) 0A AF 60 F0. 2.6) 00 00

3. En relación con los Niveles 4 y 5 (TCP/IP)

1.1 ¿Qué protocolos de nivel 4 y 5 (TCP/IP) se encapsularon en el paquete?

1.2 Indique el valor del grupo HEXA que indica el comienzo del segmento.

1.3 ¿La captura indica una comunicación orientada a la conexión? ¿a qué etapa pertenece la captura (establecimiento, transferencia o cierre)?

1.4 ¿la PDU de capa 4 tiene campos en su encabezado que se usan para el control de flujo?, ¿indique 2 valores HEXA y su significado que correspondan a 2 campos utilizados para regular el flujo?

1.5 ¿qué valor HEXA tiene el campo del encabezado en el sistema origen para multiplexar el servicio dado al nivel 5?

1.6 ¿Esta captura representa una PDU única, un fragmento intermedio o el último fragmento?

1.7 En este caso ¿qué campo se utiliza para identificar este fragmento?

1.8 ¿qué valor HEXA tiene el campo que garantiza la provisión de una entrega confiable con el destino?

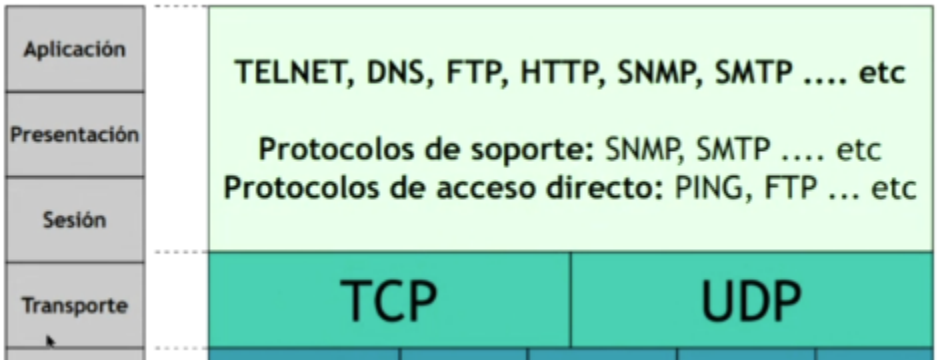
1.9 Indique la secuencia de encapsulamiento desde el más alto nivel al inferior, dando el nombre de cada protocolo.

1.10 ¿Qué valor HEXA da inicio al encabezado y cuál es la longitud particular de cada uno en su nivel, de todos los protocolos encapsulados?

Respuestas posibles

1.1 Protocolos de capa 4 y 5 encapsulados

Opciones: todas las mencionadas en la captura.



1.2 Comienzo del segmento

- Dónde termina el encabezado IP?
    - Ver el tamaño del header, que es el segundo caracter hexa del encabezado. Esto representa la cantidad de palabras de 4 bytes que tiene el header. El tamaño casi siempre es 20 bytes. Cuando pasan los 20 bytes, empieza el contenido.
- TCP y UDP empiezan con el puerto de origen.

1.3 Comunicación orientada a la conexión? TCP/UDP? Etapa de conexión.

Capa 4:

- UDP: no orientado a la conexión. No aplica la etapa de conexión.
- TCP: orientado a la conexión. La etapa de conexión se ve en los flags:
    - RST (reiniciar conexión - o no se acepta iniciación o se necesita reinicio forzoso por error)
    - SYN (hay que sincronizar números de secuencia - está estableciendo conexión)
    - FIN (etapa de cierre - se solicita cerrar la conexión)

  Si no está prendido ninguno de estos flags, está en etapa de transmisión de información.

Capa 5:

- Falta analizar capa 5?

1.4 Control de flujo en capa 4

Capa 4:

- UDP: no realiza control de flujo.
- TCP: realiza control de flujo.
    - Campo window. Indica cuántos octetos puede enviar el otro sin esperar confirmación antes
    - Campo ACK. Indica el campo que se espera en el próximo paquete (y confirma recepción de todos los bytes anteriores al próximo esperado).

Capa 5: no importa. Pregunta específicamente por capa 4.

1.5 Multiplexación

De Wikipedia: Multiplexar un paquete de datos, significa tomar los datos de la capa de aplicación, etiquetarlos con un número de puerto (TCP o UDP) que identifica a la aplicación emisora, y enviar dicho paquete a la capa de red. Se hace en la capa de transporte del modelo OSI.

- En TCP y UDP, los campos de puerto destino (según el profe, no incluye origen)

1.6 Fragmentación

La fragmentación de paquetes se hace a nivel IP (nivel 3), así que esto no representa un fragmento del mensaje de nivel 4 o 5. Explicación en nivel 3.

1.7 Qué campo se usa para identificar este fragmento

Respuestas posibles:

1) Ni TCP ni UDP tienen fragmentación. Sí la hay a nivel 3, con IP. Explicación en nivel 3.
2) A nivel TCP, se identifica **la trama** con el sequence number, que indica la cantidad de datos transferidos y el orden de los datos dentro del mensaje de capa superior.

1.8 Entrega confiable

Capa 4:

- UDP: no es confiable. No hay campos asociados
- TCP: es confiable.

- Confirmaciones, con campos: Número de secuencia / Número de confirmación / Flag ACK.
- Checksum de la cabecera y el cuerpo.

Respuestas originales

GG (1C22)	AM (2C21 - Promocionó)
1.1) Protocolo TCP. 1.2) No aplica. 1.3) Indica una comunicación orientada a la conexión y pertenece a la etapa de transferencia. 1.4) Si, 0x0aaf60f0 representa el número de secuencia y el valor "0x1020" representa el tamaño de la ventana de datos que puede recibir. 1.5) No aplica. 1.6) Representa una PDU única 1.7) No aplica. El campo de Fragment offset se encuentra con todos 0s y el flag de more fragments indica un 0 1.8) No aplica. 1.9) El protocolo Ethernet 2 encapsula una trama de protocolo IPv4 y este encapsula una trama del protocolo TCP. 1.10) Para ethernet 2 es "0xc001147c0001". Para IPv4 el valor hexa es "0x45". Para TCP el valor hexa es "0xb5dd"	1.1) TCP 1.2) El segmento TCP comienza en B5 DD (source port) 1.3) Ethernet es un protocolo no orientado a la conexión. 1.4) Si. 10 20 (window size) y 0A AF 60 F0 (SEQ). 1.5) 00 50 (Destination port). 1.6) PDU única. 1.7) Fragment offset en 0. 1.8) Por ejemplo, el ACK number (A6 C8 6C 34). 1.9) TCP --> IPv4 --> Ethernet 1.10) Ethernet: C0 (comienzo del destination address) con longitud de 14 bytes. IPv4: 45 con longitud de 20 bytes; TCP: B5 con longitud de 20 bytes.

Practica

Como se cual es la ip red de la ip? Tengo la 192.168.0.1

Por la clase ➜ 192.168.0.0/24

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0** **/8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0** **/16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0** **/24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*