

Herramientas

<https://hpdp.gasm.net/>

15-2-2023 (Cicerchia)

<https://www.utnianos.com.ar/foro/tema-redes-final-febrero-2023-15-2-2023>

3. Dada la trama #28, responda lo siguiente:

Trama#28

No.	Time	Source	Destination	Protocol	Length	Info
28	8.128256	IntelCor_b4:6c:39	Broadcast	ARP	42	Who has 192.168.0.27? Tell 192.168.0.214

Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{65D2C6C4-CCF5-4AC4-8597-48136E8E6988}, id 0
Ethernet II, Src: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39)
Sender IP address: 192.168.0.214
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.27

ARP

0000 ff ff ff ff ff e4 f8 9c b4 6c 39 00 00 00 01 .. 19 ..
0010 00 00 00 00 01 e4 f8 9c b4 6c 39 c0 a8 00 d6 .. 19 ..
0020 00 00 00 00 00 c0 a8 00 1b ..

14-2-2024 (Cicerchia)

<https://www.utnianos.com.ar/foro/tema-final-redes-14-02-2024>

22-2-2023 (Alsina)

<https://www.utnianos.com.ar/foro/tema-aporte-final-redes-22-02-2023>

24-7-2024 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-de-redes-24-07-2024>

1-3-2023 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-aporte-redes-final-01-03-2023>

21-2-2024 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-21-02-2024>

3-8-2022 y 6-9-2022 (KOVAL) (ALSINA)

<https://www.utnianos.com.ar/foro/tema-aporte-redes-finales-agosto-y-septiembre-2022>

28-04-2022 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-28-04-2022-koval-con-resolucion>

20-07-2022 (Echazu)

<https://www.utnianos.com.ar/foro/tema-final-20-07-2022-echazu-resuelto>

6-12-2023 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-de-informaci%C3%B3n-6-12-2023>

4-4-2024 (Fusario)

<https://www.utnianos.com.ar/foro/tema-aporte-final-mesa-especial-abril-redes>

5-12-2018 (Fusario)

<https://www.utnianos.com.ar/foro/tema-aporte-final-redes-05-12-18>

9-10-24 (Echazú?)

<https://imgur.com/a/QzeaFDJ>

14-2-2018 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-de-informaci%C3%B3n-14-2-2018>

11-2-2015 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-11-02-2015>
<https://www.utnianos.com.ar/foro/tema-aporte-final-redes-de-informaci%C3%B3n>

13-7-2016 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-aporte-redes-final-13-7-2016?pid=444465#pid444465>

PARCIALES KOVAL

<https://imgur.com/a/8BRY3TT>

 Koval

14-2-2024 (Cicerchia)

1) LAN/WLAN - IEEE 802.3 - NAV - CSMA

1. LAN / WLAN (1 punto).

1.1. Describa el mecanismo de control de acceso al medio empleado por el estándar IEEE 802.3, indicando una breve descripción y, claramente, qué ocurre en las siguientes situaciones:

1.1.1. Síntesis:

1.1.2. 1. Si el medio se encuentra libre:

1.1.3. 2. Si el medio se encuentra ocupado:

1.1.4. 3. Si se detecta una colisión durante la transmisión:

1.2. ¿Para qué se utiliza el NAV (Network Allocation Vector) en las redes que utilizan el estándar IEEE 802.11?

1.1)

Se basa en CSMA/CD. Soluciona la ineficiencia de CSMA haciendo que la estación siga escuchando el medio mientras dura la transmisión.

Si el medio está libre => transmite

Si el medio está ocupado => escucha hasta que el canal se libere

Colisión => se transmite una pequeña señal de interferencia (jam signal) para asegurarse de que todas las estaciones constaten la colisión y se deja de transmitir.

1.2)

NAV se usa para reducir las ambigüedades con respecto a qué estación va a transmitir. Se define la detección del canal como un proceso física y virtual:

- **Detección física:** solo se verifica el medio para ver si hay una señal válida.
- **Detección virtual:** cada estación mantiene un registro lógico del momento en que se usa el canal rastreando el **NAV**.

Cada trama lleva un campo NAV que indica cuánto tiempo tardará en completarse la secuencia a la que pertenece esa trama. Las otras estaciones que escuchen la trama saben que el canal estará ocupado durante el período indicado por el NAV, sin importar si pueden detectar o no una señal física.

INTERNET

2. INTERNET (2 puntos).

- 2.1. ¿Qué capas de la suite TCP/IP emplean un mecanismo sin conexión y cuáles son los protocolos que lo implementan? Explíquelo brevemente e indique en qué casos se utilizan.
- 2.2. Describa para qué se utiliza y cómo funciona CIDR (Classless InterDomain Routing) en redes de datagramas IPv4.

2.1

UPD. Es un protocolo de la capa de transporte. Es un servicio no fiable, lo que permite reducir la sobrecarga del protocolo. Se sitúa encima de IP y le incorpora la capacidad de direccionamiento de puerto. UDP transmite segmentos. Se utiliza para aplicaciones que no requieren un flujo continuo de datos y para DNS.

IP. Es un protocolo de capa de red. Define la unidad básica para la transferencia de datos, selección de rutas (ruteo) y conjunto de reglas para la entrega de paquetes no confiable.

2.2

CIDR.

Se usa para asignar bloques de direcciones sin pertenecer a ninguna clase. Uso de máscara en notación CIDR. Se determinan la primera dirección, la longitud y el broadcast del bloque. La dirección IP se escribe seguida de "/" junto con la longitud de prefijo.

3. WAN (2 puntos).

- 3.1. Describa la tecnología de conmutación mediante etiquetas y MPLS, indicando:
 - 3.1.1. Cómo funciona la conmutación mediante etiquetas:
 - 3.1.2. Encabezado MPLS:

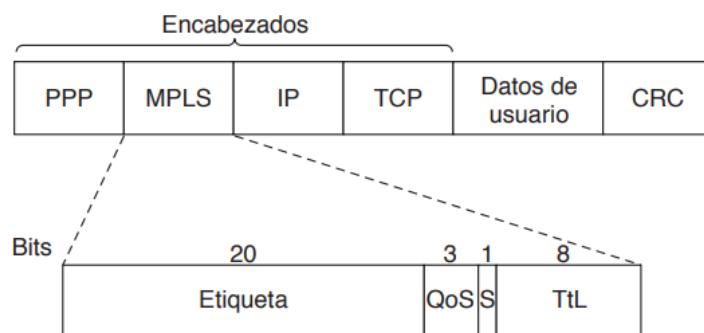
MPLS agrega una etiqueta en frente de cada paquete. El reenvío se basa en la etiqueta, no en la dirección de destino. La etiqueta se convierte en un índice de una tabla interna, permitiendo un reenvío mucho más rápido.

1. Cuando un paquete IP llega al extremo de la red MPLS, el LER inspecciona la dirección IP de destino y origen, y el tipo de servicio para determinar la FEC. Si

la FEC existe, ya tiene una etiqueta asignada. Si es nueva, se tiene que asignar una nueva etiqueta. Se define el LPS.

2. Cuando un paquete llega a un LSR, la etiqueta se utiliza como un índice en una tabla para determinar la línea de salida y la nueva etiqueta a utilizar. La etiqueta solo tiene importancia local.
3. En el otro extremo, la etiqueta se elimina para revelar el paquete IP a la siguiente red.

Se usan distintos protocolos para el intercambio de etiquetas (**LDP**, **RSVP**, **BGP**).



4. PROBLEMA 1 (2 puntos).

Dada la dirección de red: **122.16.5.0/24**, se requiere dividirla en subredes con las siguientes capacidades de asignación, indicando la dirección de cada subred y su máscara en formato decimal y cantidad de bits en "1", el rango assignable y la dirección de broadcast de cada una en la siguiente la tabla. La subred cero es assignable.

- 1 subred de 10 hosts
- 1 subred de 100 hosts

Indique para cada asignación la dirección de cada subred y su máscara, rango assignable y dirección de broadcast. Complete la siguiente tabla y agregue aparte los cálculos de la solución:

122.16.5.0/24 24 para red y 8 PARA HOST

Uso VLSM. Necesito 2 subredes. 128 para cada una. Desperdicio muchas para el caso de 10 hosts. Entonces tengo /25 y el segundo espacio de 128 lo vuelvo a dividir. Me queda en /28

01111010.00010000.00000101.|**0|host**

01111010.00010000.00000101.|**1000|host**

1 subred de 100 hosts

- Requerimiento: 100
- Asignados: 126 (128 - 2)

- CIDR: /25
- Dirección de Subred: 122.16.5.0
- Máscara: 255.255.255.128
- Rango Asignable: 122.16.5.1 - 122.16.5.126
- Dirección de broadcast: 122.16.5.127

Reviso solo el último octeto:

0|0000000

1|0000000 = 128

1 subred de 10 hosts

- Requerimiento: 10
- Asignados: 14 (16 - 2)
- CIDR: /28
- Dirección de Subred: 122.16.5.128
- Máscara: 255.255.255.240
- Rango Asignable: 122.16.5.129
- Dirección de broadcast: 122.16.5.143

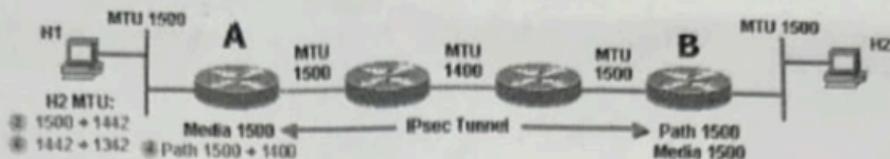
Reviso solo el último octeto:

0000|0000

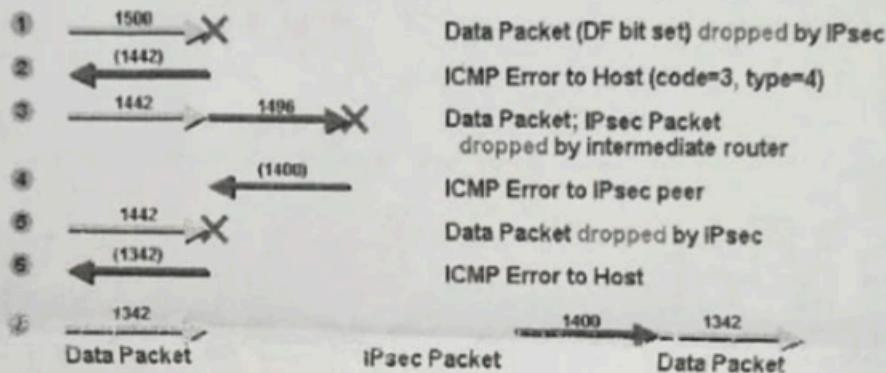
1111|0000 = 240

5. PROBLEMA 2 (2 puntos).

Se ha configurado el siguiente escenario de red con túnel IPsec entre una sucursal en la ARGENTINA (H1) y la casa matriz en CANADÁ (H2):



El administrador de la sucursal ARGENTINA detecta anomalías en el tráfico mediante el túnel IPsec entre los routers A y B, le pide un informe a CANADÁ y recibe del administrador de B el siguiente resumen gráfico con su explicación:



1. El router A recibe un paquete de 1500 bytes (encabezado IPv4 de 20 bytes + carga útil del TCP de 1480 bytes) destinado al host 2.
2. El paquete de 1500 bytes se cifra mediante IPv4Sec y se agregan 52 bytes de sobrecarga (encabezado IPv4Sec, cola y encabezado IPv4 adicional). Ahora IPv4Sec debe enviar un paquete de 1552 bytes. Dado que la MTU saliente es 1500, este paquete debe fragmentarse.
3. Se crean dos fragmentos fuera del paquete de IPv4Sec. Durante la fragmentación, se agrega un encabezado IPv4 de 20 bytes adicional para el segundo fragmento, que da como resultado un fragmento de 1500 bytes y un fragmento IPv4 de 72 bytes.
4. El router B (par del túnel IPv4Sec) recibe los fragmentos, elimina el encabezado IPv4 adicional y fusiona los fragmentos de IPv4 nuevamente en el paquete de IPv4Sec original. A continuación, IPv4Sec descifra este paquete.
5. Luego, el router B reenvía el paquete de datos original de 1500 bytes al Host 2.

Se tiene seteado el flag DF (No fragmentar). El MTU es de 1500 bytes, pero el datagrama es mayor, por lo que falla.

6. PROBLEMA 3 (1 punto).

Considere la siguiente captura de una trama Ethernet:

0000	00 40 05 40 ef 24 00 60 08 9f b1 f3 81 00 00 20	@ @ \$..
0010	08 00 45 00 00 34 8a 1b 40 00 40 06 68 e4 83 97	.. E .. 4 .. @ @ . h ..
0020	20 15 83 97 20 81 17 70 64 8a 4d 3d 54 b9 4e 14 p .. M=T .. N ..
0030	de 3d 80 10 7c 70 31 ed 00 00 01 01 08 0a 01 99	= .. p1 ..
0040	a3 f3 00 04 f0 c7

PREGUNTAS:

- 6.1. En la capa 2 ¿es una comunicación a uno, a varios o a todos los hosts de la red? Fundamente la respuesta.
- 6.2. ¿Se trata de tráfico en una red conmutada con VLANs? Fundamente la respuesta.

Trama Ethernet:

Mac Destino	Mac Origen	Tipo		
00.40.05.40.ef.24	00.60.08.9f.b1.f3	81 00		

El valor 0x8100 indica VLAN

15-2-2023 (Cicerchia)

1.

PROBLEMAS / EJERCICIOS

1. Dada la dirección de red: 192.168.1.0/24, se requiere dividirla en subredes con las siguientes capacidades de asignación, indicando la dirección de cada subred y su máscara en formato decimal y cantidad de bits en "1", el rango assignable y la dirección de broadcast de cada una en la siguiente tabla y agregue aparte los cálculos de la solución (la subred cero es assignable).

- 1 subred de 12 hosts
- 1 subred de 67 hosts

REQUERIMIENTO	DIRECCIÓN DE SUBRED / MÁSCARA	RANGO IP HOSTS ASIGNABLES / MÁSCARA	DIRECCIÓN DE BROADCAST SUBRED / MÁSCARA
1 subred de 67 hosts			
1 subred de 12 hosts			

192.168.1.0/24

La divido en dos de 128: /25

	Subnet 1	Subnet 2
Network ID	192.168.1.0	192.168.1.128
First	192.168.1.1	192.168.1.129
Last	192.168.1.126	192.168.1.254
Broadcast	192.168.1.127	192.168.1.255

Necesito 16 hosts. Divido la Subnet 2

	Subnet 2
Network ID	192.168.1.128
First	192.168.1.129
Last	192.168.1.142
Broadcast	192.168.1.143

2.

2. Obtener el o los resúmenes de ruta (superred/es) para implementar CIDR, que "sumarize" las redes indicadas a continuación:
- 192.168.4.0/22
 - 192.168.2.0/23
 - 192.168.0.0/23
 - 192.168.8.0/21

Reviso el tercer octeto

192.168.4.0/22 => 11000000.10101000.00000100.00000000

192.168.2.0/23 => 11000000.10101000.00000010.00000000

192.168.0.0/23 => 11000000.10101000.00000100.00000000

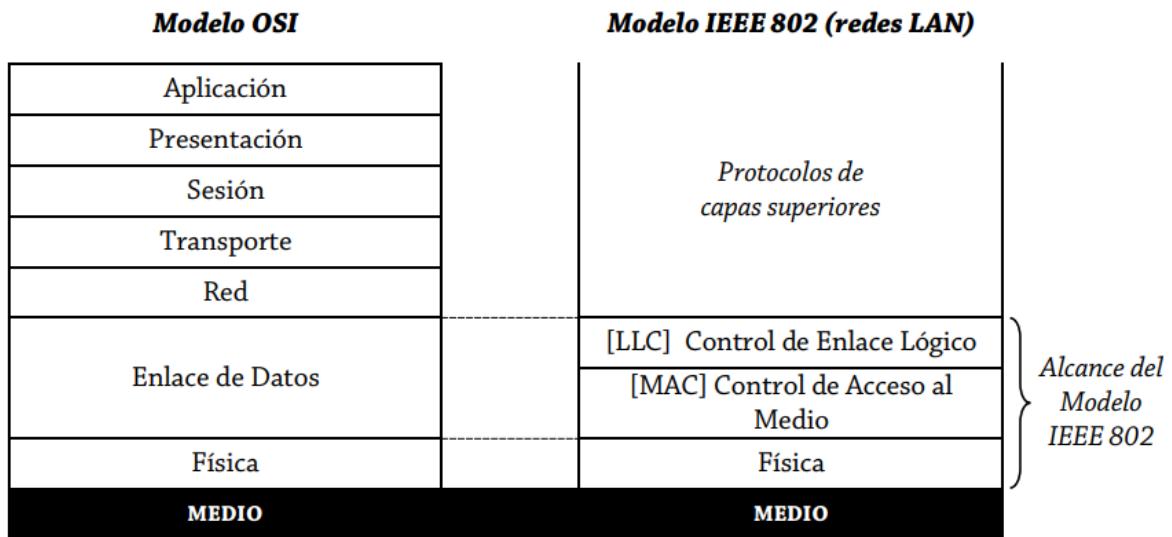
192.168.8.0/21 => 11000000.10101000.00001000.00000000

192.168.0.0/20

4. LAN / WLAN.

- a. Explique de manera gráfica y descriptiva en base a los estándares IEEE 802 la arquitectura y protocolos de una red cableada Ethernet, indicando en referencia al modelo OSI sus capas, subcapas y qué protocolos se utilizan para las funciones de direccionamiento y control de flujo. (no se requieren detalles de la capa Física)
- b. ¿Qué algoritmo utiliza una red basada en IEEE 802.11 como mecanismo de control de acceso distribuido al medio de comunicaciones? Explíquelo brevemente.

A)



MAC

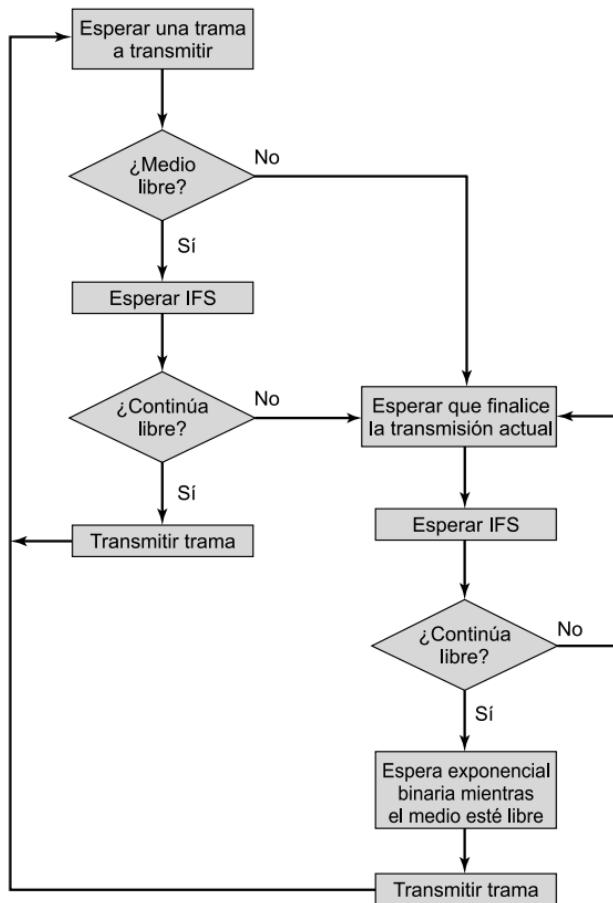
Funciones

1. En transmisión, ensamblado de datos en tramas con campos de dirección y detección de errores.
2. En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
3. Control de acceso al medio de transmisión LAN.

LLC

- Funciones
 - Especificar los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios.
 - Interfaz con capas superiores.
 - Corrección de errores y de flujo (Opcional).

B) Usa CSMA/CA refinado (distintos IFS con distintas prioridades)



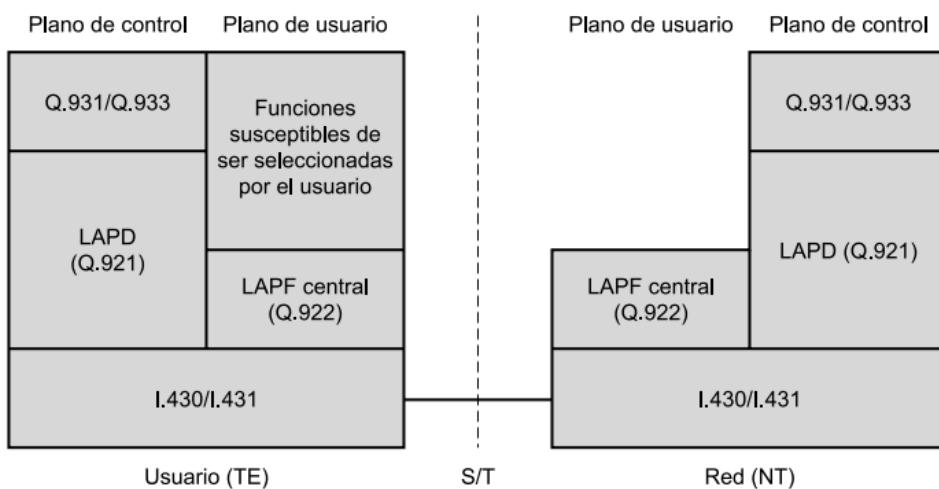
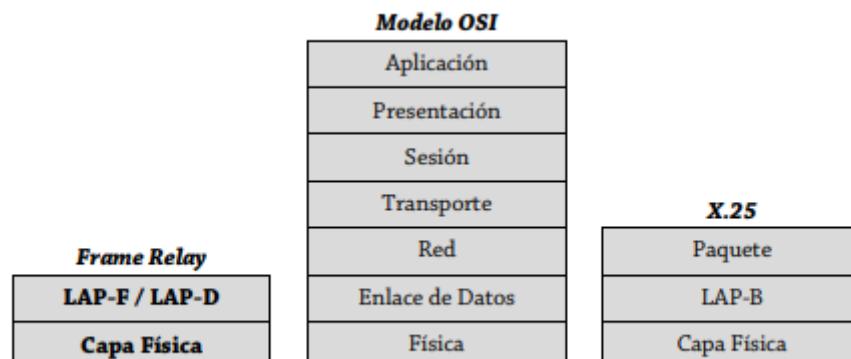
- **SIFS (Short IFS).** La estación que use un SIFS tiene la prioridad más alta. Enviar el siguiente fragmento después de esperar sólo un tiempo SIFS es lo que evita que otra estación irrumpa con una trama a mitad del intercambio. Se usa en:
 - **ACK.**
 - **CTS/RTS.**
 - ***Poll response.***
- **PIFS (Point coordination function IFS).** Lo usa el controlador central en el esquema PCF cuando emite sondeo.
- **DIFS (Distributed coordination function IFS).** Se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio.

5. WAN

- a. Explique el mecanismo de conmutación de paquetes para la comunicación entre redes. Describa un caso de aplicación que lo utilice en la capa 2 del modelo OSI (arquitectura, protocolos y breve síntesis de su funcionamiento).
- b. Describa cómo funciona el protocolo TCP para proporcionar el servicio de multiplexación a un protocolo de capa superior. Dé un ejemplo.

a)

Los datos se envían en pequeñas unidades (**paquetes**). Cada paquete se pasa de nodo en nodo siguiendo un camino determinado. En cada nodo, el paquete se almacena temporalmente y después se transmite al siguiente nodo. Los paquetes contienen información de control (header) + datos de usuario. Puede ser de **datagramas** o **circuitos virtuales**. Frame Relay es un protocolo de capa 2 que utiliza circuitos virtuales



b) La multiplexación en TCP se implementa mediante el uso de puertos. Para definir otro punto extremo se utiliza la combinación de IP + Puerto. Por ejemplo, un máquina puede correr distintas aplicaciones en distintos puertos.

22-2-2023 (Alsina)

<https://www.utnianos.com.ar/foro/tema-aporte-final-redes-22-02-2023>

1) FRAME RELAY

1. Una consola de monitoreo sondea dispositivos en la red utilizando SNMP.
Para monitorear 50 routers de una red Frame Relay, envía mensajes GetRequest-PDU (44 bytes) sobre el siguiente acceso:
Access Rate: 256 Kbps
CIR: 50 %
EIR: 64 Kbps
SNMP trabaja sobre UDP
Indique:
- ¿Con qué frecuencia máxima (Poll/Sec) puede sondear a los dispositivos, asegurando que TODOS los mensajes se transporten garantizados (sin marcar)?
 - ¿Cuántos dispositivos podrá sondear (por segundo) como máximo, si ningún mensaje debe ser rechazado por la red (descartado)?
 - ¿Qué se debe hacer para monitorear con esta estación a 2000 routers? Indique tres alternativas.

a)

SMNP = 44 BYTES

UDP = 8 BYTES

IP= 20 BYTES

FR = 1 + 2 + 2 +1 = 7

SUMA = 79 BYTES

TOTAL (Todos los routers) = 3950 Bytes = Bc = 31.600 kb

CIR = 0,5 . Access Rate = 128 Kbps

CIR = Bc/T => T = Bc/CIR = 0,246875 s (Esto es lo que dura un sondeo)

Poll/s = 4,05 Poll/s

b)

EIR+CIR = 64 kbps + 128 kbps = 192 kbps -> capacidad sin descarte

por router -> 78 B/router = 624 b/router

$$\frac{(EIR + CIR) * 1s}{624} \cdot \frac{[b] \cdot [router]}{[b]} = 307 \text{ routers}$$

c)

- Aumentar el AR
- Disminuir el tamaño de la trama
- Monitorear en intervalos por grupo

2)

2. Particione el rango de direcciones 10.16.0.0/22 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de las siguientes redes: a) 256 host, b) 70 host y c) 58 host. Indique en cada caso, la dirección de sub-red y la máscara o prefijo asignados.

10.16.0.0/22 => 10 bits para los hosts

El cálculo es Requerimiento = Hosts + 2 (broadcast y network id)

Para a) 512 b) 128 c) 64

Aplico VLSM. Primero divido el rango de direcciones para tener 512 hosts (/23)

Máscara = 255.255.254.0

	Subnet 1	Subnet 2
Network ID	10.16.0.0	10.16.2.0
First	10.16.0.1	10.16.2.1
Last	10.16.1.254	10.16.3.254
Broadcast	10.16.1.255	10.16.3.255
Mask	255.255.254.0	255.255.254.0

La subnet 2 la divido otra vez para cumplir con B. Necesito un bloque de 128 (/25)

	Subnet 2	Subnet 3
Network ID	10.16.2.0	10.16.2.128
First	10.16.2.1	10.16.2.129
Last	10.16.2.126	10.16.2.254
Broadcast	10.16.2.127	10.16.2.255
Mask	255.255.255.128	255.255.255.128

La subnet 3 la divido para tener bloques de 64 para (c) (/26)

Subnet 3	
Network ID	10.16.2.128
First	10.16.2.129
Last	10.16.2.190
Broadcast	10.16.2.191
Mask	255.255.255.192

3)

3. Analice la captura a continuación y responda:

```
0000 00 1c 25 7e b8 10 00 23 33 cf 43 74 81 00 00 14 ..%~...# 3.Ct....  
0010 08 00 45 00 00 a2 dc af 00 00 ff 06 b4 0b ac 15 ..E..... ....  
0020 69 0b ac 15 69 64 01 bb 1c 85 bb 02 31 a4 66 32 i...id... ....1.f2  
0030 90 48 50 16 20 00 2e 58 00 00 17 03 01 00 75 fb .HP. ...x .....u.  
0040 0d d9 b7 19 f9 a8 a2 de f8 0c c2 e0 8d 9f 25 3c ..... ....%<
```

Ethernet:

MAC Destino
MAC Origen
Protocolo:

VLAN

- ¿A qué VLAN va dirigida la trama?
- ¿Qué entrada existirá en el caché ARP del remitente? Indique MAC e IP.
- ¿A qué clase pertenecen la dirección IP origen y destino?

0b ac 15 69 0b ac 15 69

MAC Destino = 00 1c 25 7e b8 10

MAC Origen = 00 23 33 cf 43 74

ID PROTOCOLO VLAN = 81 00

PRIORIDAD + CFI = 0

ID VLAN = 0 14 = 20

Protocolo = 08 00 = IP

b) Una entrada que relacione la dirección MAC con la IP. Como es el remitente, debería ser la dirección origen (quiero saber quién mandó el mensaje).

172.21.105.100 -> 00 23 33 cf 43 74

c) Las primeras 3 palabras (32 bits c/u) no me importan. Serían 12 pares de hexa.

Dir Ip Destino = ac 15 69 0b = 172.21.105.11

Dir ip origen = ac 15 69 64 = 172.21.105.100

4)

4. El protocolo de nivel 2 de un vínculo que interconecta 2 redes LAN tiene un MTU de 1000 bytes. Si un host transmite un segmento TCP de 1460 bytes:
- ¿Cuántos fragmentos se crearán, si la cabecera IP tiene el bit DF = 1?
 - ¿Cuántos, si el bit DF = 0?
 - ¿Quién realizará la fragmentación, en caso de ser necesaria y posible?
 - ¿Quién se encarga del reensamblado?

TCP e interactúa con la capa IP. Una entidad TCP acepta flujos de datos de usuario de procesos locales, los divide en fragmentos que no excedan los 64 KB (en la práctica, por lo general son 1460 bytes de datos para ajustarlos en una sola trama Ethernet con los encabezados IP y TCP), y envía cada pieza como un datagrama IP independiente. Cuando los datagramas que contienen datos TCP llegan a una máquina, se pasan a la entidad TCP, la cual reconstruye los flujos de bytes originales. Con el afán de simplificar, algu-

como veremos a continuación.

La entidad TCP emisora y receptor intercambian datos en forma de segmentos. Un **segmento TCP** consiste en un encabezado fijo de 20 bytes (más una parte opcional), seguido de cero o más bytes de datos. El software de TCP decide qué tan grandes deben ser los segmentos. Puede acumular datos de varias escrituras para formar un segmento, o dividir los datos de una escritura en varios segmentos. Hay dos límites que restringen el tamaño de segmento. Primero, cada segmento, incluido el encabezado TCP, debe caber en la carga útil de 65 515 bytes del IP. Segundo, cada enlace tiene una **MTU (Unidad Máxima de Transferencia**, del inglés *Maximum Transfer Unit*). Cada segmento debe caber en la MTU en el emisor y el receptor, de modo que se pueda enviar y recibir en un solo paquete sin fragmentar. En la práctica, la MTU es por lo general de 1500 bytes (el tamaño de la carga útil en Ethernet) y, por tanto, define el límite superior en el tamaño de segmento.

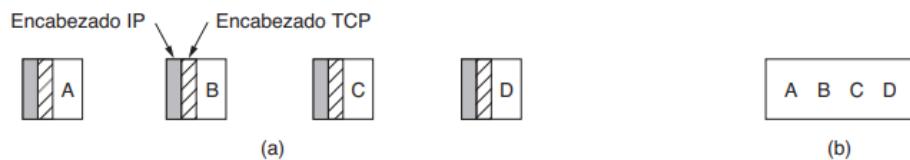


Figura 6-35. (a) Cuatro segmentos de 512 bytes que se envían como diagramas IP separados. (b) Los 2048 bytes de datos que se entregan a la aplicación en una sola llamada READ.

Una opción muy utilizada es la que permite a cada host especificar el **MSS (Tamaño Máximo de Segmento**, del inglés *Maximum Segment Size*) que está dispuesto a aceptar. Es más eficiente usar segmen-

a) (Leer texto de arriba). Se puede asumir dos cosas:

1. Previamente (o ahora si se está estableciendo la conexión en este momento) se envía la opción MSS que es el tamaño máximo del campo de datos posible ($MSS = MTU - 20 - 20 = 960 \text{ B}$). Esto es para que al agregarse la cabecera IP y TCP, el segmento sea de 1000 B y se pueda mandar por el enlace sin fragmentar (que es lo que busca TCP). En este caso, como nunca se fragmenta, no me interesa el flag DF, porque siempre mando varios segmentos TCP, cada uno con su propia cabecera. Entonces, los fragmentos IP creados son 0 (si hay varios segmentos).
2. Por algún motivo se necesita fragmentar, entonces sí me importa el DF.

Para el caso 2, necesito fragmentar, pero DF está activado. Entonces se produce un error y se responde un mensaje ICMP de "destino inalcanzable - Se necesita fragmentar pero DF está activado".

b) Partimos del análisis previo. Si no se fragmenta, se van a mandar dos segmentos TCP.

Datos TPC = $1460 - 20 = 1440 \Rightarrow$ Segmentos = Datos/MSS = $1,5 \Rightarrow$ 2 segmentos TCP

Si se fragmenta (o sea, hay un único segmento TCP)

Fragmentos = Segmento / (MTU - 20) = 1,48 \Rightarrow 2 fragmentos.

c) Lo realiza el router de origen.

d) El router destino.

Teoría

1. ¿Qué indica la recepción de un mensaje "destino inalcanzable"? Indique 3 situaciones
2. ¿De qué manera se realiza la delimitación de tramas en HDLC? ¿En qué consiste el mecanismo de inserción de ceros y para qué se utiliza?

1) Es un mensaje de ICMP que indica que el router no puede alcanzar el destino.

Casos:

- a) Network Unreachable. No es posible alcanzar la red de destino.
- b) Host unreachable. No es posible alcanzar el host de destino.
- c) Protocol unreachable. El host responde que el protocolo no está activado o no es alcanzable.

- d) Fragmentation needed and DF Set
- 2) Mediante el delimitador 01111110 . Los receptores buscan detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama, y detectar el final. Para evitar que esa combinación de bits aparezca en otro lugar dentro de la trama, se realiza una *inserción de bits*. Si aparece el patrón “11111” se inserta un “0” al final. El receptor analiza el sexto bit: si es un cero, lo elimina; si es un uno y el séptimo un 0, es un delimitador.

24-7-2024 (KOVAL)

1. Analizando la siguiente captura, responda:

0000	6c 99 61 f7 cc ef c8 cb 9e 51 28 86 08 00 45 00	l.a.....Q(...E.
0010	00 28 b4 76 40 00 80 06 00 00 c0 a8 00 fe 1f ba	.(.v@.....
0020	ef 5f dd f4 01 bb 25 01 b8 54 e1 46 a6 2a 50 14	._....%..T.F.*P.
0030	00 00 9a 99 00 00

- a. ¿Quién envía el segmento (Cliente o Servidor)? Indique cómo lo infiere
- b. ¿Contiene datos? ¿Cuántos? Explique
- c. ¿En qué estado está la conexión para el remitente de este mensaje?
- d. ¿Cómo responderá el receptor del mensaje?

Dir MAC Destino = 6c 99 61 f7 cc ef

Dir MAC Origen = c8 cb 9e 51 28 86

Ethertype = 08 00 (IPv4)

-- IP --

Version = 4

Header Length= 5

Service Type = 00

Length = 00 28 = 40 B

ID = B4 76

Flags + Offset = 40 00

TTL = 80

Protocol = 06 (TCP)
Checksum = 00 00
Dir Origen = c0 a8 00 fe = 192.168.0.254
Dir Destino = 1f ba ef 5f
Relleno = 0
-- TCP ---
Origin Port = dd f4
Dest. Port = 01 bb = 443 (HTTPS)
Sequence = 25 01 b8 54
Confirmation = e1 46 a6 2a
Header Length = 5
Reserva = 0
Flags = 14 = 0 0 0 ACK= 1 0 RST = 1 0 FIN = 0
WINDOW = 00 00
CHECKSUM = 9A 99
URGENT = 00

- a) Es un cliente porque el puerto destino es el 443 (HTTPS)
- b) No contiene datos. ~~El tamaño de la ventana es 0~~ (El tamaño de la ventana no importa). No contiene datos porque el campo de Total Length del datagrama IP es 40, siendo $40 = 20 \text{ B (H IP)} + 20 \text{ B (H TCP)}$.
- c) El remitente envía el RST=1 que indica que se tiene que restablecer la conexión debido a un error en el host o alguna otra razón.
- d) Cómo el flag de reset esta on, el receptor tiene que finalizar la conexión

2. Analice la captura a continuación y responda:

0000	33 33 00 00 00 01 6c 99 61 f7 cc ef 86 dd 60 06	33....l.a.....
0010	98 12 00 c8 3a ff fe 80 00 00 00 00 00 00 6e 99:.....n.
0020	61 ff fe f7 cc ef ff 02 00 00 00 00 00 00 00 00	a.....
0030	00 00 00 00 00 01 86 00 29 15 40 80 01 2c 00 00)@...,
0040	75 30 00 00 00 00 03 04 40 c0 00 2f d4 3c 00 2f	<u>u0.....@.../.<</u>

a. ¿A quién va dirigido el mensaje?

MAC DESTINO = 33 33 00 00 00 01

MAC ORIGEN = 6C 99 61 F7 CC EF

ETHERTYPE = 86 DD (IPv6)

IPv6

VERSION = 6

CLASE DE TRÁFICO = 00

ETIQUETA DE FLUJO = 6 98 12

LONGITUD DE PAYLOAD = 00 C8

HEADER SIGUIENTE = 3A

LÍMITE DE SALTOS = FF

DIR IPV6 ORIGEN = FE 80 00 00 00 00 00 00 6E 99 61 FF FE F7 CC EF
= FE::6E 99 61 FF FE F7 CC EF

DIR IPV6 DESTINO = FF 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
= FF02:: (Dirección multicast)

3)

3. Dada la dirección de red 171.17.58.0, se desean armar 10 subredes. Hallar la dirección de difusión (broadcast) de la sexta subred y el último host de la novena.

171.17.58.0

X.X.00111010.00000000

Si quiero que mi dirección de red se mantenga como 171.17.58.0, entonces voy a usar los últimos 9 bits para manejar las subredes y los hosts. Necesito 10 subredes, entonces voy a usar 4 bits para las subredes (16 subredes posibles) y el resto para los hosts (30 hosts posibles después de restar el broadcast y network id).

$$5 * 32 = 160$$

Subnet	Network ID	Broadcast	First	Last
1	171.17.58.0	171.17.58.31	171.17.58.1	171.17.58.30
2	171.17.58.32			
3	171.17.58.64			
4	171.17.58.96			
5	171.17.58.128			
6	171.17.58.160	171.17.58.191	171.17.58.161	171.17.58.190
7	171.17.58.192			
8	171.17.58.224			
9	171.17.59.0	171.17.58.31	171.17.58.1	171.17.59.30
10	171.17.59.32			

4. Explique los mecanismos utilizados por cada uno de estos protocolos para la detección y la corrección de errores:
- Ethernet
 - IP
 - ATM
 - MPLS
5. ATM
- ¿Qué es la capa de adaptación al ATM?
 - ¿Qué variantes existen y qué características tienen?
6. Protocolos de ruteo
- ¿Qué función cumplen?
 - Compare las características de al menos dos de ellos

4) Detección y corrección de errores

a. Ethernet.

Detección: tiene un campo de FCS en su cabecera (mecanismo CRC32) que alcanza a todos los campos de la cabecera, menos al preámbulo .

Corrección: No hace. Si se detecta un error en la trama, la misma se descarta.

b. IP.

Detección: tiene un campo Checksum en la cabecera. El mismo cubre los demás datos de la cabecera (no el payload).

Corrección: IP no realiza corrección. Si se detecta un error en el datagrama, se descarta.

c. ATM

Detección: la cabecera tiene un campo HEC. Se usa un algoritmo CRC8 sobre los primeros 4 bytes de la cabecera. ATM es capaz de corregir hasta 1 bit erróneo. Si errores en más de 1 bit, no puede realizar la corrección y descarta la celda.

d. MPLS

No tiene control de errores. Delega esa función a los demás protocolos.

5) ATM

a. ¿Qué es la capa de adaptación al ATM?

Su propósito es dar soporte a protocolos de transferencia de información que no estén basados en ATM. Sus funciones son: manejar los errores en la transmisión; segmentación y reensamblado; manejo de las celdas perdidas o mal insertadas; y control de flujo. Las dos subcapas lógicas son:

- . Convergencia. Tiene las funciones necesarias para dar soporte a aplicaciones que hacen uso de AAL.
- . Segmentación y ensamblado. Empaquetan la información (generan las celdas de tamaño fijo) y desempaquetan la información en el destino.

b. ¿Qué variantes existen y qué características tienen?

Existen 5 variantes (AAL 1 ... AAL 5). Cada variante (o protocolo) surge para satisfacer distintos requerimientos de velocidad y tipos de datos a transferir (clases de servicios).

AAL 1. Audio y vídeo sin comprimir (servicio en tiempo real con velocidad constante)

AAL 2. Vídeo Comprimido (servicio en tiempo real con velocidad variable)

AAL 3/4. Datos en general. No orientado a la conexión.

AAL 5. Emulación LAN, Frame Relay, ATM, IP sobre ATM.

6) Protocolos de ruteo

a. ¿Qué función cumplen?

Debe proveer una rápida adaptación a los cambios en la topología de red. Si una red deja de estar disponible, el protocolo debe poder detectar eso y determinar el próximo camino hacia esa red.

Debe poder elegir la mejor ruta. Para eso, utiliza distintas métricas (cantidad de saltos, retardo de la red, ancho de banda, etc).

Intercambio de información entre los routers de una red para reflejar los cambios en la red (esa información se encuentra en la tabla de ruteo).

Si es un protocolo de interior (IRP), distribuye la información entre los dispositivos dentro de una misma AS (red gestionada por una misma organización). Si es un protocolo de exterior (ERP), intercambia información entre distintos AS.

b. Compare las características de al menos dos de ellos

RIP es de tipo Distance Vector. Su métrica es la cantidad de saltos (máximo 15). OSPF es de tipo Link State y su métrica es el ancho de banda y el delay. Los de tipo Distance Vector utilizan la cantidad de saltos (distancia) como métrica. Los Link State usan la cantidad de saltos + otras características de la red (retardo, ancho de banda, fiabilidad, MTU, etc).

1-3-2023 (KOVAL)

1)

1. A continuación, se muestra el establecimiento de una conexión TLS (HTTPS). Donde el cliente envía un mensaje "Client Hello" y el servidor responde con un mensaje "Server Hello".

Time	Source	Destination	Protocol	Info
573 0...	192.168.0.208	40.101.70.194	TCP	51426 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
578 0...	40.101.70.194	192.168.0.208	TCP	443 → 51426 [SYN, ACK] Seq=0 Ack=1 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM=1
579 0...	192.168.0.208	40.101.70.194	TCP	51426 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
580 0...	192.168.0.208	40.101.70.194	TLSv1.2	Client Hello
582 0...	40.101.70.194	192.168.0.208	TCP	443 → 51426 [ACK] Seq=1 Ack=531 Win=4194048 Len=0
583 0...	40.101.70.194	192.168.0.208	TCP	443 → 51426 [ACK] Seq=1 Ack=531 Win=4194048 Len=0 [TCP segment of a reassembled PDU]
584 0...	40.101.70.194	192.168.0.208	TCP	443 → 51426 [ACK] Seq=1461 Ack=531 Win=4194048 Len=0 [TCP segment of a reassembled PDU]
585 0...	40.101.70.194	192.168.0.208	TCP	443 → 51426 [ACK] Seq=2921 Ack=531 Win=4194048 Len=0 [TCP segment of a reassembled PDU]
586 0...	40.101.70.194	192.168.0.208	TLSv1.2	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
587 0...	192.168.0.208	40.101.70.194	TCP	51426 → 443 [ACK] Seq=531 Ack=4435 Win=131328 Len=0
588 0...	192.168.0.208	40.101.70.194	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
592 0...	40.101.70.194	192.168.0.208	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

- a. ¿Cuántos bytes de longitud tiene el mensaje Client Hello?

El mensaje Server Hello debió ser fragmentado.

- b. ¿Cuál es la longitud de dicha respuesta?
 c. ¿Cuántos segmentos ocupa la respuesta del servidor?
 d. ¿De qué longitud cada uno?

- A) El primer ACK=1 (Se confirma hasta el byte 1). El segundo ACK=531 (se confirma hasta el byte 531) => 531 - 1 = 530 B (Longitud del mensaje).
 B) El ACK=4435 => 4435 - 1 = 4434 B
 C) MSS = 1460 => 4434/1460 = 3,03 => 4 segmentos
 D) 3 de 1460B y uno de 54 B

2)

2. Se desea enviar una PDU de aplicación de 4800 bytes. Compare las alternativas de utilizar los protocolos de transporte TCP y UDP. Si el host está conectado a una red Ethernet.
 a. ¿Cuántos segmentos/datagramas se crearán en cada caso?
 b. ¿Cuál lo hará de forma más eficiente?

A)

PDU DE APLICACIÓN = 4800 B

CABECERA TCP = 20 B (SIN OPCIONES)

CABECERA UDP = 8 B

CABECERA IP = 20 B

MTU ETHERNET = 1500 B

Cantidad de datos posibles a enviar en un segmento (Total-Cabecera):

TCP = 1500 - (20+20) = 1460 B

UDP = 1500 - (8+20) = 1472 B

Respuesta de Koval

Con respecto al cálculo de TCP. Partís de asumir:

$$\text{Segmento TCP} = 4800 \text{ B (Datos)} + 20 \text{ B (Cabecera)} = 4820 \text{ B}$$

Es decir, armas un solo segmento TCP gigante. Sabemos que TCP tiene un tamaño máximo del segmento (MSS) limitado por el MTU de la interfaz. TCP va a encapsular cada segmento de tamaño MSS, por lo que tendrás una cabecera TCP + IP en cada uno de ellos.

Si bien en UDP no está muy claro cómo se determina el tamaño del datagrama UDP ya que no existe algo parecido al MSS, en la práctica sabemos que este también está limitado por el MTU de la interfaz. Por lo que yo contemplaría el uso de una cabecera UDP + IP en cada datagrama.

Los segmentos utilizados para establecer la conexión se pueden considerar overhead, pero no fragmentos ya que no contienen datos de aplicación.

Saludos

TCP e interactúa con la capa IP. Una entidad TCP acepta flujos de datos de usuario de procesos locales, los divide en fragmentos que no excedan los 64 KB (en la práctica, por lo general son 1460 bytes de datos para ajustarlos en una sola trama Ethernet con los encabezados IP y TCP), y envía cada pieza como un datagrama IP independiente. Cuando los datagramas que contienen datos TCP llegan a una máquina, se pasan a la entidad TCP, la cual reconstruye los flujos de bytes originales. Con el afán de simplificar, algunos

como veremos a continuación.

La entidad TCP emisora y receptora intercambian datos en forma de segmentos. Un **segmento TCP** consiste en un encabezado fijo de 20 bytes (más una parte opcional), seguido de cero o más bytes de datos. El software de TCP decide qué tan grandes deben ser los segmentos. Puede acumular datos de varias escrituras para formar un segmento, o dividir los datos de una escritura en varios segmentos. Hay dos límites que restringen el tamaño de segmento. Primero, cada segmento, incluido el encabezado TCP, debe caber en la carga útil de 65 515 bytes del IP. Segundo, cada enlace tiene una **MTU (Unidad Máxima de Transferencia)**, del inglés *Maximum Transfer Unit*. Cada segmento debe caber en la MTU en el emisor y el receptor, de modo que se pueda enviar y recibir en un solo paquete sin fragmentar. En la práctica, la MTU es por lo general de 1500 bytes (el tamaño de la carga útil en Ethernet) y, por tanto, define el límite superior en el tamaño de segmento.

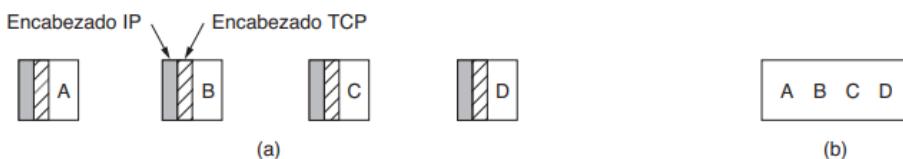


Figura 6-35. (a) Cuatro segmentos de 512 bytes que se envían como diagramas IP separados. (b) Los 2 048 bytes de datos que se entregan a la aplicación en una sola llamada READ.

Segmentos/Datagramas:

$$\text{TCP} = 1 \text{ (Siempre se envía uno con los headers para iniciar la conexión)} + 4800/1460 = 5$$

$$\text{UDP} = 4800/1472 = 4$$

B) UDP lo hará de manera más eficiente debido a que envía 4 segmentos/datagramas en lugar de 5. La contra es que la eficiencia se paga no garantizando una entrega fiable (es un protocolo no orientado a la conexión).

- D. ¿Cuál sería la mejor forma de hacerlo?
3. Particione el rango de direcciones 172.16.128.0/22 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de las siguientes redes: a) 256 hosts, b) 70 hosts y c) 58 hosts
Indique en cada caso, la dirección de sub-red y la máscara o prefijo asignados

172.16.128.0/22

256 hosts => 9 bits para el host (/23)=> 510 hosts posibles

70 hosts => 7 bits para el host (/25)=> 126 hosts posibles

58 hosts => 6 bits para el host (/26)=> 64 hosts

172.16.10000000.00000000

Requerimiento/ Bloque Asignado	Network ID	Broadcast	Mask	Prefix
256/512	172.16.128.0	172.16.129.255	255.255.254.0	/23
70/128	172.16.130.0	172.16.130.127	255.255.255.128	/25
58/64	172.16.130.128	172.16.130.191	255.255.255.192	/26

4) Explique el mecanismo de control de flujo. ¿Cómo operan Stop&Wait and Sliding Window?

Stop & Wait. La entidad origen transmite una trama. El destino, después de recibir el mensaje, indica que puede aceptar otro mediante el envío de un ACK. El origen debe esperar el ACK antes de enviar la trama siguiente. Es una operación half-duplex.

Sliding Window. Funciona en un enlace full-duplex. Se permite que varias tramas viajen al mismo tiempo sobre el enlace, mejorando la eficiencia. Hay dos estaciones (A y B). B puede almacenar W tramas (puede aceptar W), entonces le permite enviar W tramas sin tener que esperar ninguna confirmación. Cada trama se etiqueta con un número de secuencia. B confirma la trama enviando el número de secuencia de la siguiente trama que espera recibir. Una **ventana** es la lista de los números de secuencia que A puede transmitir y B espera recibir.

5) IPSec.

A) ¿Qué servicios ofrece AH y ESP?

AH. Verificación de integridad y seguridad antirrepetición, pero no la confidencialidad (no hay encriptación).

ESP. Privacidad del contenido y del flujo de tráfico (limitado). También puede llegar a proveer servicio de autenticación.

B) ¿En qué se diferencian el modo túnel y el modo transporte?

Modo Túnel. Todo el paquete IP se encapsula en el cuerpo de un paquete IP nuevo con un encabezado IP totalmente nuevo. Es útil cuando

Modo Transporte. El encabezado IPSec se inserta después del encabezado IP. El campo protocolo indica que sigue un encabezado IPSec (antes del encabezado TCP).

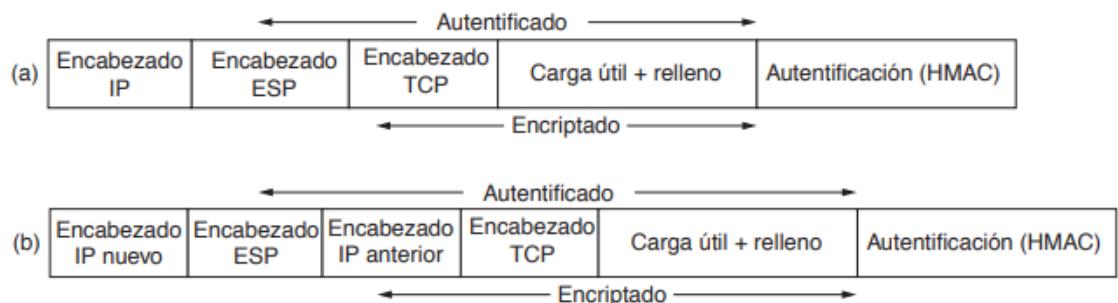


Figura 8-28. (a) ESP en modo de transporte. (b) ESP en modo de túnel.

C) ¿Qué variantes de encriptación y hash conoce?

Simétrica. Utiliza una clave única.

Asimétrica. Utiliza dos claves (pública y privada).

21-2-2024 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-21-02-2024>

1) Análisis de Trama

1. Analizando la siguiente captura, responda:

0000	00 0b cd 3b 22 5b	00 50 54 ff 25 9e	08 00 45 00	...;" .PT.%...E.
0010	00 30 00 00 40 00	3a 06 ea 9d c8 45	02 36 0a c8	.0..@.:.....E.6..
0020	80 e7 00 50 08 7c	eb 19 49 bc 56 cb	bb b2 70 12	...P. ..I.V...p.
0030	16 d0 c6 44 00 00	02 04 05 64 01 01	04 02	...D.....d....

a. ¿Quién envía el segmento (Cliente o Servidor)? Indique cómo lo infiere
b. ¿En cuál de ellos fue realizada la captura de esta trama? Explique
c. ¿En qué estado está la conexión para el remitente de este mensaje?
d. ¿Cuál es el ISN (número de secuencia inicial) del cliente?
e. ¿Cuántos bytes podrá enviar el cliente sin esperar confirmación del servidor?
f. ¿Qué aplicación están utilizando?

a) Repetido. Me tengo que fijar el puerto. Si el origen es un puerto de origen bien conocido, es del servidor. Si no, de un cliente.

DIR MAC DESTINO = 00 0B CD 3B 22 5B

DIR MAC ORIGEN = 00 50 54 FF 25 9E

ETHERTYPE = 0800 (IP)

---- IP ---- (20 BYTES)

Version = 4

Dir Origen = c8 45 02 36 = 200.xxx.xxx.xxx (es una pública)

Dir Destino = 0a c8 80 e7 = 10.xxx.xxx.xxx (Es una privada)

---- TCP ----

Puerto origen = 00 50 = 80 (HTTP) => El servidor envía el segmento.

Puerto destino = 08 7c = 2172

Número de secuencia = eb 19 49 bc

Número de confirmación = 56 cb bb b2

Header Length = 7

Reservado = 0

Flags = 12 = 000|ACK=1|00|SYN=1|0

Window = 16 d0 =

Checksum = c6 44

Urgent Pointer = 00 00

b) La captura se realiza en el dispositivo donde está ingresando el segmento porque la dirección destino es una dirección privada y la origen una pública

c) El server responde con SYN=ACK=1 => El cliente cambia el estado a ESTABLISHED y tendría que mandar el último ACK del handshake de tres pasos al server.

d) El server responde SEQ = eb 19 49 bc y ACK = 56 cb bb b2. Ese ACK es igual al ISN que envió el cliente - 1 => ISN_CLIENTE = ACK - 1

e) El tamaño de ventana es 5840. Puede enviar 5840 octetos sin esperar confirmación.

f) HTTP

2)

2. Analice la captura a continuación y responda:

0000 33 33 00 00 00 01 | 6c 99 61 f7 cc ef | 86 dd | 0 0 | 33....l.a.....
0010 98 12 | 00 c8 | 3a { ff } fe 80 00 00 00 00 00 00 6e 99 ..:.:.:.n.
0020 61 ff fe f7 cc ef ff 02 00 00 00 00 00 00 00 00 00 a.....
0030 00 00 00 00 00 | 01 86 00 29 15 40 80 01 2c 00 00).@...
0040 75 30 00 00 00 00 00 03 04 40 c0 00 2f d4 3c 00 2f u0.....@.../.<

a. ¿A quién va dirigido el mensaje?

DIR MAC DESTINO = 33 33 00 00 00 01

DIR MAC ORIGEN = 6C 99 61 F7 CC EF

ETHERTYPE = 86 DD (IPV6)

--- IPv6 ---

Version = 6

Clase de Tráfico = 0 0

Etiqueta de Flujo = 6 98 12

Longitud Payload = 00 c8

Header siguiente = 3a

Límite de saltos = ff

Dirección Origen = fe 80 00 00 00 00 00 6e 99 61 ff fe fe cc ef
= fe8::6e991fffffeccef

Dirección Destino = ff 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
= ff02:: (Es una dirección multicast)

3)

3. Particione el rango de direcciones 172.16.0.0/23 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de las siguientes redes: a) 139 hosts, b) 14 hosts y c) 58 hosts
Indique en cada caso, la dirección de red y la máscara o prefijo asignados

172.16.0.0/23 => 23 bits para la red => 9 para el host

139 hosts => voy a usar 8 bits => 256 direcciones posibles (254 hosts) => (/24)

14 hosts => voy a usar 4 bits => 16 direcciones posibles (14 hosts) => (/28)

58 hosts => voy a usar 6 bits => 64 direcciones posibles (62 hosts) => (/26)

Requerimiento/ Bloque Asignado	Network ID	Broadcast	Mask	Prefix
139/256	172.16.0.0	172.16.0.255	255.255.255.0	/24
58/64	172.16.1.0	172.16.1.63	255.255.192	/26
14/16	172.16.1.64	172.16.1.79	255.255.240	/28

4)

4. Explique los mecanismos utilizados por TCP para:
- Detección de errores
 - Corrección de errores
 - ¿Cuál es la función del RTO?
 - ¿Qué utilidad incorpora la opción WS (Window Scale Factor)?

Explique los mecanismos utilizados por TCP para:

a. **Detección de errores**

Checksum sobre el header, los datos y un pseudoencabezado IP.

b. **Corrección de errores**

TCP no tiene una confirmación de rechazo, sino que se basa en la confirmación positiva de la recepción y retransmite cuando la confirmación no llega dentro del RTO.

c. **¿Cuál es la función del RTO?**

Es uno de los temporizadores de TCP. Cuando se envía un segmento, se inicia el temporizador. Si la confirmación del segmento llega antes de que RTO expire, se detiene. Si RTO termina antes de que llegue el segmento, se retransmite el mismo.

d. **¿Qué utilidad incorpora la opción WS (Window Scale Factor)?**

Permite que el emisor y receptor negocien un factor de escala

de ventana al inicio de la conexión. En algunos casos (alto ancho de banda o alto retardo) conviene utilizar un mayor tamaño de ventana.

5)

5. Protocolo ICMP
- ¿Cuál es su función?
 - ¿Qué mensajes conoce?
 - Dé un ejemplo en que se produciría el mensaje "Se necesita fragmentar pero DF está activado"

Protocolo ICMP

a. ¿Cuál es su función?

Proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. Proporciona feedback sobre problemas del entorno de comunicación. ICMP es un usuario de IP.

b. ¿Qué mensajes conoce?

Tipo de mensaje.	Descripción.
<i>Destination unreachable</i>	El router no puede localizar el destino. En algunas redes, el router puede detectar si un computador es inalcanzable. El mismo computador de destino puede devolver este mensaje si algún punto de acceso de un nivel superior no es alcanzable. Un paquete con el bit DF no puede entregarse porque hay una red de paquetes pequeños que se interpone.
<i>Time exceeded</i>	Se descartó un paquete porque su TTL ha llegado a cero.
<i>Parameter problem</i>	Valor inválido en el header.
<i>Source quench</i>	Se usaba para el control de flujo
<i>Redirect</i>	El router detecta que el paquete está mal enrutado. El router avisa al host emisor que se actualice con una mejor ruta.
<i>Echo and echo reply</i>	Se usan para ver si un destino es alcanzable y está vivo. El destino debería responder <i>ECHO REPLAY</i> luego de recibir un <i>ECHO</i> . Se usan en la herramienta ping .
<i>Timestamp request/replay</i>	Similares a <i>echo</i> . El tiempo de llegada y de salida de la respuesta se registran.
<i>Router advertisement/solicitation</i>	Permiten que los hosts encuentren routers cercanos.

- c. De un ejemplo en que se produciría el mensaje "Se necesita fragmentar pero DF está activado.

Se tiene un MTU de 1500 bytes y un mensaje de 3000 bytes. Se necesita fragmentar en ese caso (se debería enviar dos segmentos IP). Si DF=1, ICMP responderá con ese mensaje (que es del tipo DESTINATION UNREACHABLE).

6)

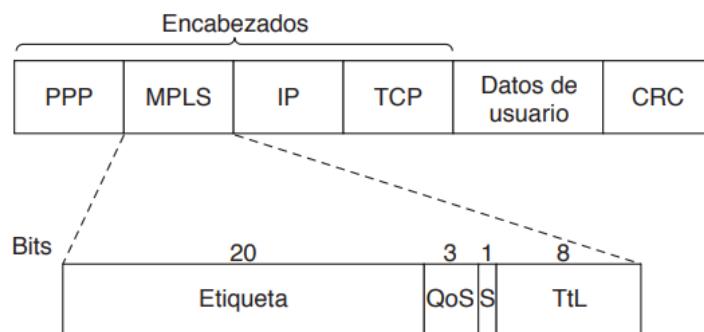
6. Protocolo MPLS
- ¿Qué es un LSR (Label Switching Router)?
 - ¿Qué campos contiene una etiqueta?

Protocolo MPLS

- a. ¿Qué es un LSR (Label Switching Router)?

Es un router que soporta MPLS, es decir, es capaz de entender las etiquetas MPLS y de recibir y transmitir paquetes etiquetados. Pueden ser: Ingress (reciben un paquete que no está etiquetado y le insertan una etiqueta); Egress (reciben un paquete etiquetado, le sacan la etiqueta y lo envían por un enlace de datos); Intermediate (reciben un paquete etiquetado, realizan un operación sobre él, y lo envían por el enlace correcto). Los primeros dos son edge, es decir, se encuentran al borde de la red MPLS (al comienzo y final).

- b. ¿Qué campos contiene una etiqueta?



3-8-2022 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-aporte-redes-finales-agosto-y-septiembre-2022>

1)

NO SE VE NADA

✓ 1. Analizando la siguiente captura, responda:

2343 138.. 52.114.74.222	192.168.0.14	TLSv1.2	Application Data
2342 138.. 192.168.0.14	52.114.74.222	TCP	58769 + 443 [ACK] Seq=1419 Ack=5639 Win=517 Len=0
2979 178.. 52.114.74.222	52.114.74.222	TLSv1.2	Application Data
2981 178.. 52.114.74.222	192.168.0.14	TLSv1.2	Application Data
2991 178.. 192.168.0.14	52.114.74.222	TCP	58769 + 443 [ACK] Seq=1477 Ack=5606 Win=512 Len=0
3109 175.. 52.114.74.222	192.168.0.14	TLSv1.2	Application Data
3110 175.. 192.168.0.14	52.114.74.222	TCP	58769 + 443 [ACK] Seq=1738 Ack=1730 Win=2009 Len=0
3132 175.. 52.114.74.222	192.168.0.14	TLSv1.2	Application Data
3129 178.. 52.114.74.222	192.168.0.14	TCP	443 + 58769 [ACK] Seq=7030 Ack=1738 Win=2009 Len=0

✓ a. ¿Cuántos bytes llevan intercambiados el cliente y el servidor?
✓ b. ¿Cuántos bytes transporta el segmento #3110?
✓ c. ¿Quién inicio la conexión?
✓ d. ¿Cuál será el número de secuencia del segmento #3129?

- En el último segmento se ve SEQ=7030 (?) y ACK=1730. Esto indica que el server está mandando a partir del byte 7030 y confirmando la recepción hasta el byte 1730. Por lo tanto, se intercambiaron $7030 + 1730 = 8760$ bytes.
- El cliente envía la SEQ=1477 y el server contesta con el ACK=1738 => $1738-1477= 261B$
- El puerto 443 es un puerto bien conocido (HTTPS), por lo que el otro proceso es el cliente. Por lo tanto, 58769 es quien comienza la conexión.
- 7030

2)

✓ 2. Analice la siguiente traza y responda:

3c f0 11 34 c5 92 | 60 99 61 f7 cc e5 | 08 00 45 00 | <.4..1.a....E.
| 04 8c | 75 94 40 00 | 6f 06 51 d1 | 34 72 4a de | c0 a8 ..u.B.o.Q.4rJ...
00 0e 01 bble5 91 ee 56 83 a2 af 6e 43 67 | 50 18 |V...nCap.
08 01 | 81 6b 00 00 | 17 03 03 04 5f 00 00 00 00 00 ...K.....

✓ Quién envía el segmento? (Client / Servidor) y cuál es su dirección IP

DIR MAC DESTINO = 3C F0 11 34 C5 92

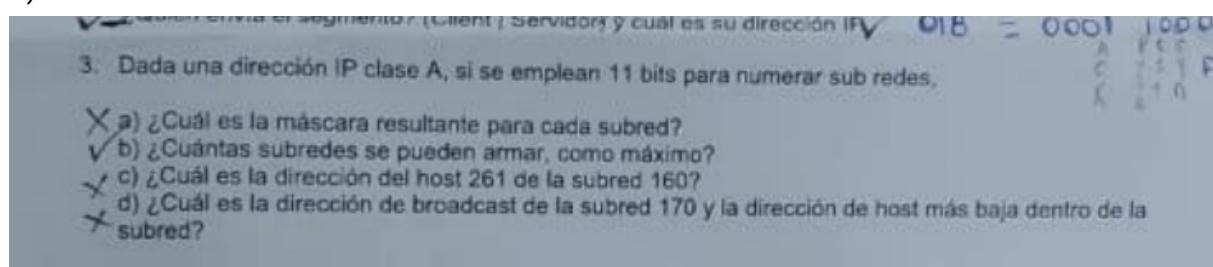
DIR MAC ORIGEN = 60 99 61 F7 CC EF

```

ETHERTYPE          = 08 00 (IPv4)
--- IP ---
VERSION = 4
IHL = 5
TOS = 00
TOTAL LENGTH = 04 8C
IDENTIFIER = 75 94
FLAGS + FRAGMENT OFFSET = 40 00
TTL = 6F
PROTOCOL = 06 (TCP)
CHECKSUM = 51 D1
DIR ORIGEN= 34 72 4A DE = 52.114.74.22
DIR DESTINO= C0 A8 00 0E
--- TCP ---
PUERTO ORIGEN = 01 BB = 443 (HTTPS) => Es el server
PUERTO DESTINO = E5 91

```

3)



CLASE A => 0.0.0.0 a 127.255.255.255 (/8)

Si se emplean 11 bits para la subred, la nueva máscara va a quedar de /19 (8 bits para la red, 11 para la subred y 13 para el host)

Hosts = $2^{13} - 2 = 8192 - 2 = 8190$

Saltos = $8192/256 = 32$ (esto representa los saltos en el tercer octeto)

(VER DE RESOLVERLO MEDIANTE EL MÉTODO DE LOS SALTOS, NO CON BINARIO)

- a. 255.255.224.0
- b. $2^{11} = 2048$
- c. La primera subred es X.0.0.0.

La subred 160 tendría el ID=159 (comienza en 0).

El host 261 se representa tal cual (todos 0s está reservado)

para la dirección de red y todos 1s para broadcast).

159 = 00010011111

261 = 0000100000101

Juntando todo

XXXXXXX.00010011.11100001.00000101 => X.19.225.5

d. 169 = 10101001

XXXXXXX.00010101.00100000.00000000 => X.21.32.0

Network= X.21.32.0

Broadcast= X.21.63.255

First= X.31.32.1

4) IP

4. IP

- a. ¿Cuál es la función del protocolo ICMP? Indique 3 mensajes del protocolo.
- b. ¿Qué es una dirección clase D? ¿Para qué servicio se utiliza?
- c. Explique la función del campo Desplazamiento/Offset de la cabecera.

a. **¿Cuál es la función del protocolo ICMP? Indique 3 mensajes del protocolo.**

Proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. Proporciona feedback sobre problemas del entorno de comunicación. ICMP es un usuario de IP.

Destination Unreachable; Echo Replay; Time exceeded.

b. **¿Qué es una dirección clase D? ¿Para qué servicio se utiliza?**

Son direcciones IP reservadas (224.0.0.0 - 239.255.255.255) para multidifusión.

c. **Explique la función del campo Desplazamiento/Offset de la cabecera.**

Indica dónde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits.

5) MPLS

5. MPLS

- a. ¿Qué dispositivos son los encargados de insertar y retirar las etiquetas?
- b. ¿En qué capa del Modelo OSI opera?
- c. ¿Cómo se distribuye la información de etiquetas dentro de una red MPLS?

a. **¿Qué dispositivos son los encargados de insertar y retirar las etiquetas?**

Los LSRs (Label switch router), es decir, routers que soportan MPLS: entienden la etiqueta y pueden recibir y reenviar paquetes etiquetados.

b. **¿En qué capa del Modelo OSI opera?**

MPLS se encuentra entre el protocolo IP de la capa de red y el protocolo PPP de la capa de enlace. En realidad no es un protocolo de capa 3, pues depende de direcciones IP o de otra capa de red para establecer las rutas de las etiquetas. En realidad tampoco es un protocolo de capa 2, pues reenvía los paquetes a través de varios saltos, no de un solo enlace. Por esta razón, algunas veces se denomina protocolo de capa 2.5.

c. **¿Cómo se distribuye la información de etiquetas dentro de una red MPLS?**

MPLS agrega una etiqueta en frente de cada paquete. El reenvío se basa en etiquetas, no en la dirección de destino. La etiqueta es un índice en una tabla interna del router, permitiendo un reenvío mucho más rápido. Cuando el paquete llega a la red MPLS, el LER (Label Edge Router) inspecciona la dirección de IP destino y origen, y el tipo de servicio para determinar la FEC. Si no existe, se crea.

Las tablas se establecen: al encenderse un router, revisa cuáles son las rutas para las que será destino final. Crea una o más FECs para esas rutas y asigna una etiqueta para cada una de las rutas y pasa las etiquetas a sus vecinos. Los vecinos introducen las etiquetas en sus tablas de reenvío y envían nuevas etiquetas a sus vecinos, hasta que todos los routers hayan adquirido la ruta. Se usan varios protocolos que son una combinación de protocolos de routing y de establecimiento de conexión (OSPF, ISIS, RIP).

6) TCP

6. TCP

a. ¿Qué son las opciones TCP? ¿Cuáles conoce?

b. ¿Qué función cumple el campo "Puntero Urgente" de la cabecera?

c. ¿Qué es el "tiempo de espera de retransmisión" (RTO)? ¿Qué sucede si es demasiado breve?

a. **¿Qué son las opciones TCP? ¿Cuáles conoce?**

MSS Option. Se declara al momento de establecer la conexión.

Determina el tamaño máximo del segmento de datos que es capaz

de aceptar.

Escala de Ventana. Permite al emisor y receptor negociar un factor de escala de ventana al inicio de la conexión.

Timestamp. El origen pone el stamp y el destino responde con otro al confirmar. Permite calcular el RTT de forma más precisa.

SACK. Permite a un receptor indicar al emisor los rangos de números de secuencia que ha recibido. Complementa el Número de confirmación de recepción y se utiliza después de haber perdido un paquete y de la llegada de los datos subsiguientes (o duplicados).

b. **¿Qué función cumple el campo “Puntero Urgente” de la cabecera?**

Cuando se suma al número de secuencia del segmento, contiene el número de secuencia del último octeto de la secuencia de datos urgentes. Permite al receptor conocer la cantidad de datos urgentes que llega.

c. **¿Qué es el tiempo de espera de retransmisión (RT0)? ¿Qué sucede si es demasiado breve?**

RT0 es uno de los temporizadores de TCP. Cuando un emisor envía un segmento, el temporizador inicia. Cuando recibe la confirmación del segmento por parte del receptor, se detiene. En caso de que el RT0 termine antes de recibir la confirmación, se vuelve a enviar el segmento. Si RT0 es muy grande, voy a esperar mucho en reenviar; si es muy chico, tal vez tenga que reenviar muchas veces el segmento.

6-9-2022 (ALSINA)

1. Ventajas y desventajas de segmentar una LAN. ¿Cómo se hace?

????

2. Ventajas y desventajas de usar firma digital.

Ventajas: provee autenticidad, integridad y no repudio.

Desventaja: no provee privacidad, es decir, el mensaje está protegido de alteraciones, pero podría ser leído por terceros.

3. Red 200.10.10.0. Tomar 3 bits del host para la red. ¿Cuál es la cantidad máxima de subredes que se pueden tener y cuántos hosts por cada una?

No se indica, pero esa IP pertenece a las IPs Clase C (192.0.0.0 hasta 223.255.255.255). Su prefijo es /24. Si se toman 3 bits para

las subredes, me quedan 5 para los hosts.

$$\text{Subredes} = 2^3 = 8$$

$$\text{Hosts} = 2^5 - 2 = 30 \text{ (Se le resta la dirección de subred y el broadcast)}$$

**4. Red 172.21.10.0 /23. Se quieren 3 subredes. Direccionar de la forma más eficiente si quiero: a) 129 hosts b) 12 hosts c) 58 hosts
(Nota: "Más eficiente" = Usar VLSM)**

Requerimiento/ Bloque Asignado	Network	Broadcast	Mask	Prefix
129/256	172.21.10.0	172.21.10.255	255.255.255.0	/24
58/64	172.21.11.0	172.21.11.63	255.255.255.192	/26
12/16	172.21.11.64	172.21.11.79	255.255.255.240	/28

5. ¿Cómo se realiza el direccionamiento IP dinámico? (Protocolo y mensajes) ¿Por qué tiene un tiempo limitado y cuál es?

Mediante DHCP. Al iniciar una computadora, se difunde una solicitud de dirección IP en su red usando un paquete DHCP DISCOVER que debe llegar al servidor DHCP. El servidor asigna una dirección IP libre y la envía al host en un paquete DHCP OFFER. El servidor identifica al host mediante su dirección ETHERNET. El tiempo que el host tiene asignada la IP se llama *arrendamiento*. Justo antes de que expire, el host debe pedir una renovación al DHCP. Si no hace la solicitud o si se rechaza, el host tal vez ya no pueda usar esa dirección. El tiempo limitado permite justamente la asignación dinámica, ya que los hosts que estén inactivos no necesitan esas direcciones.

6. Se tiene un paquete IP de 5MBytes, una red que transmite a 1000Mbps y un tiempo de acceso de tramas de 9,5 microSegundos. ¿Cuánto tiempo se tardará en enviar el paquete?

$$5 \text{ MBytes} = 40 \text{ Mbits}$$

$$40 \text{ Mbits} / 1000 \text{ Mbps} = 0,04 \text{ s}$$

$$\text{Tiempo Total} = 0,04\text{s} + 9,5 \text{ microsegundos} = 0,0400095$$

28-04-2022 (KOVAL)

<https://www.utnianos.com.ar/foro/tema-final-redes-28-04-2022-koval-con-resolucion>

1)

```
ac 3b 77 9c 4f dc 3c f0 11 34 c5 92 08 00 45 00 .;w.O.<..4....E.
00 5c 5a b9 00 00 01 01 5f c0 c0 a8 00 0d 62 8a .\Z....._....b.
db e8 08 00 f3 c7 00 01 04 37 00 00 00 00 00 00 00 .....7.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....7.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....7.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....7.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....7.....
```

- a. ¿Cuál es la pila completa de protocolos utilizados?
- b. ¿Quién es el destinatario final del datagrama?
- c. ¿Quién es el destinatario de la trama?
- d. ¿Cree Ud. que llegará a destino? ¿Por qué?
- e. ¿Qué entrada existirá en la tabla ARP del remitente?

A)

DIR MAC DESTINO = AC 3B 77 9C 4F DC

DIR MAC ORIGEN = 3C F0 11 34 C5 92

ETHERTYPE = 08 00 (IPv4)

--- IP ---

VERSION = 4

HEADER LENGTH = 5

TOS = 00

TOTAL LENGTH = 00 5C

IDENTIFICATION = 5A B9

FLAGS = 0

FRAGMENT OFFSET = 0 00

TTL = 01

PROTOCOL = 01 (ICMP)

HEADER CHECKSUM = 5F C0

DIR ORIGEN = C0 A8 00 0D = 192.168.0.13

DIR DESTINO = 62 8A DB E8 = 98.138.219.232

--- ICMP ---

La pila completa es **ETHERNET(IPv4(ICMP))**

B) Destinatario datagrama = Destinatario IP = 98.138.219.232

- C) Destinatario trama = Destinatario Ethernet = AC 3B 77 9C 4F DC
 D) Una entrada que asocie la dir MAC AC 3B 77 9C 4F DC con la IP 98.138.219.232

2. Siendo los parámetros de acceso a una red Frame Relay los siguientes: Access Rate 768 kbps, CIR 50% del A.R., EIR 50% del CIR.
 Hallar Bc, Be y la cantidad de tramas con DE=0 ; DE=1 y rechazadas suponiendo que un proceso de streaming genera continuamente tramas de 9.600 bits a una velocidad de 800 kbps. Tc=1seg.

CIR = 0,5 AR = 384 kbps

EIR = 0,5 CIR = 192 kbps

Tc = 1s

Trama = 9600 bit = 9,6 kb

Velocidad = 800 kbps

En T=1s puedo transmitir 800 kb /9600b = 83,33 tramas => 84 tramas

CIR = Bc/T => Bc = CIR * T = 384 kb => Tramas DE=0 = 40

EIR = Be/T => Be = EIR * T = 192 kb => Tramas DE=1 = 20

Tramas descartadas = 24

3)

3. Sabiendo que un host está configurado con la siguiente información: 162.19.249.114/21, responda:
- ¿A qué red está conectado?
 - ¿Qué mascara tiene configurada?
 - ¿Cuál será su default gateway?
 - ¿Cuántos hosts "vecinos" posee como máximo?
 - ¿Podemos hacer Subneteo de este bloque de direcciones para asignar a dos redes de 780 y 1024 hosts respectivamente?

162.19.249.114/21 => 21 bits de red y 11 de host

- A) 162.19.11111|001. => 162.19.248.0
 B) 255.255.248.0
 C) 162.19.248.1
 D) $2^{11} - 2 - 1 = 2045$
 E) Si quiero dos subredes, tengo que ceder un bit de host. Me quedan 10, así que no alcanza para 1024 hosts (podría tener 1022).

4. IP versión 6
- ¿Cuál es la longitud de la dirección IPv6?
 - ¿Cómo está conformada una dirección IPv6?
 - ¿Cómo se identifica la dirección de "Broadcast"?
5. IPSec
- ¿Qué servicios ofrecen los protocolos AH y ESP?
 - ¿En qué difieren el modo transporte y el modo túnel?
 - ¿Qué variantes de encriptación y Hash conoce?
6. Ruteo IP
- ¿Qué elementos de información contiene una tabla de ruteo?
 - ¿En qué se diferencian los protocolos vector-distancia de los link-state?
 - Indique a qué grupo pertenecen los utilizados en las prácticas de laboratorio

4) IPv6

a. **¿Cuál es la longitud de la dirección IPv6?**

128 bits

b. **¿Cómo está conformada una dirección IPv6?**

Global Routing Prefix (48 bits) + Subnet ID (16 bits) + Interface ID (64 bits)

c. **¿Cómo se identifica la dirección de broadcast?**

En IPv6 no hay dirección de broadcast. Esta funcionalidad se realiza con direcciones multicast especiales. Las direcciones que empiezan con ff00::/12 son direcciones bien conocidas. Por ejemplo: FF02::1 (todos los nodos IPv6) y FF02::2 (todos los routers).

5) Ya resuelta más arriba (1-3-2023)

6) Ruteo IP

a. **¿Qué elementos de información contiene una tabla de ruteo?**

Se almacena la información de topología, la información que tiene el host acerca de la red. Las columnas son:

- **Destination network.** Red destino o prefijo.
- **Netmask.** Máscara o longitud de prefijo.
- **Gateway.** Próximo salto. Para llegar al destino debo enviar el datagrama al vecino gateway. Si el gateway es "On-link", ejecuto ARP porque cualquier destino que está en ese network
- **Interface.** El host debe saber por cuál interfaz debe conectarse/alcanzar un determinado destino.
- **Metric.** Si tengo dos entradas idénticas, gana la que tiene menos metric.

b. **¿En qué se diferencian los protocolos vector-distancia de los link-state?**

Vector distancia toma en cuenta únicamente la cantidad de

saltos entre el origen y el destino mientras que Link State (Estado de enlace) toma en cuenta la confiabilidad + delay + distancia y la capacidad

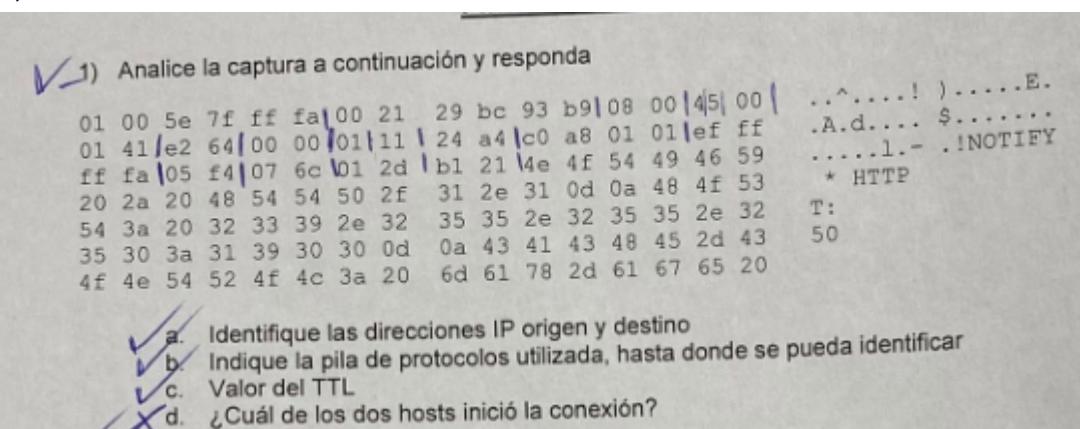
c. Indique a qué grupo pertenecen los utilizados en las prácticas de laboratorio

Vector distancia porque solo mediamos la cantidad de saltos.

6-12-2023 (Koval)

1)

1) Analice la captura a continuación y responda



The hex dump shows network traffic between two hosts. The source MAC addresses are 01:00:5e:7f:ff:fa and 00:21:29:bc:93:b9. The destination MAC address is 00:11:22:33:44:55. The ASCII dump shows an HTTP response starting with "HTTP/1.1 200 OK".

a. Identifique las direcciones IP origen y destino
 b. Indique la pila de protocolos utilizada, hasta donde se pueda identificar
 c. Valor del TTL
 d. ¿Cuál de los dos hosts inició la conexión?

DIR MAC DESTINO = 01 00 5E 7F FF FA

DIR MAC ORIGEN = 00 21 29 BC 93 B9

ETHERTYPE = 08 00 (IPv4)

-- IP --

VERSION = 4

HEADER LENGTH = 5

TOS = 00

TOTAL LENGTH = 01 41

IDENTIFICATION = E2 64

FLAGS = 0

FRAGMENT OFFSET = 0 00

TTL = 01

PROTOCOL = 11 (UDP)

CHECKSUM = 24 A4

DIR ORIGEN = C0 A8 01 01 = 192.168.1.1

DIR DESTINO = EF FF FF FA = 239.255.255.250

-- UDP --

PUERTO ORIGEN = 05 F4 = 1524

PUERTO DESTINO = 07 6C = 1900

- a. DIR ORIGEN = C0 A8 01 01 = 192.168.1.1
DIR DESTINO = EF FF FF FA = 239.255.255.250
- b. ETHERNET + IP + UDP
- c. TTL = 01
- d. Es UDP, por lo tanto, no se establece una conexión.

2)

V. c. Valor de TTL

d. ¿Cuál de los dos hosts inició la conexión?

2) Particione el rango de direcciones 172.16.0.0/23 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de 3 subredes de: a) 120 hosts, b) 8 hosts y c) 61 hosts
Indique en cada caso, la dirección de red y la máscara o prefijo asignados.

Requerimiento/ Bloque Asignado	Network	Broadcast	Mask	Prefix
120/128	172.16.0.0	172.16.0.127	255.255.255.128	/25
61/64	172.16.0.128	172.16.0.191	255.255.255.192	/26
8/16	172.16.0.192	172.16.0.207	255.255.255.240	/28

3)

Indique en cada caso, la dirección de red y

3) La IP 192.168.0.107 corresponde a la dirección de broadcast de una subred. Indique:
 a. ¿Cuál es la dirección de red?
 b. ¿Cuál es la máscara?
 c. ¿Cuántas subredes fueron creadas, respecto de la clase a la que pertenece esta dirección?

La dirección de broadcast es aquella que tiene todos 1s en la parte de host

192.168.0.01101011 => Los últimos dos bits representarían la dirección de broadcast.

La dirección de red es aquella que todos los bits del host son 0s
192.168.0.01101000

- a. 192.168.0.104
- b. 255.255.255.252
- c. Hay 6 bits para las subredes => se crearon 64 subredes.

4) TCP. Errores



- 4) Explique detalladamente el mecanismo utilizado por TCP para garantizar la entrega libre de errores. Indique qué campos de la cabecera intervienen para lograrlo.

En TCP no existe una confirmación de rechazo (RJ por ejemplo). TCP se basa en la confirmación positiva de la recepción, y se retransmite un mensaje cuando la confirmación no llega dentro de un determinado rango de tiempo RTT. Los campos intervenientes serían el número de secuencia (SN), el número de confirmación (AN) y el campo checksum. El checksum se aplica sobre el encabezado, los datos y un pseudoencabezado IP.

5) ATM



- 5) ATM indique que clases de servicio define y que capa de adaptación (AAL) implementa cada una.

Protocolos de AAL

Requerimiento	Clase A	Clase B	Clase C	Clase D
Tiempo entre Fuente y Destino	Requerido (sensible a demoras). rt	No requerido (no sensible a demoras). nrt		
Velocidad (Bit Rate)	Constante CBR	rt-VBR	Variable nrt-VBR	
Modo de Conexión	Con conexión	Sin conexión		
Protocolo	AAL 1	AAL 2	AAL 3	AAL 4
Tipos de Datos Transmitidos	Audio y Video sin comprimir	Video comprimido	Datos en general	

- **AAL 5** es otro protocolo → servicio con menor *overhead* y mejor detección de errores.
 - Emulación LAN, Frame Relay, ATM, IP sobre ATM.

14-2-2018 (KOVAL)

1)

1. Analizando la siguiente captura, responda:

0000	a0 1b 29 e6 e1 ef d8 fc 93 33 5b cb 08 00 45 00	...). 3{...E.	A=10
0010	00 28 18 0e 40 00 80 06:77 ad c0 a8 01 14 22 cc	.(...@....W....",	B=11
0020	86 8c ef 2e 01 bb 88 0f e7 c5 6d 83 4d 7f 50 11m.M.P.	C=12
0030	41 37 e7 c5 00 00	A7....	D=13

✓ a. A partir de las direcciones IP origen y destino, determine si el datagrama ingresa o egresa del dispositivo donde se realizó la captura. ¿Cómo lo deduce?

b. ¿A qué dispositivo corresponde la dirección MAC destino?

c. ¿Cuántos "saltos" lleva dados el datagrama y por qué?

d. ¿De qué aplicación se trata?

e. ¿En qué estado se encuentra la conexión?

DIR MAC DESTINO = A0 1B 29 E6 E1 EF

DIR MAC ORIGEN = D8 FC 93 33 5B CB

ETHERTYPE = 08 00 (IPv4)

-- IP --

VERSION = 4

HEADER LENGTH = 5

TOS = 00

TOTAL LENGTH = 00 28

IDENTIFICATION = 18 0E

FLAGS + FRAGMENTATION OFFSET = 40 00

TTL = 80

PROTOCOL = 06 (TCP)

CHECKSUM = 77 AD

DIR ORIGEN = C0 A8 01 14 = 192.168.1.20

DIR DESTINO = 22 CC 86 8C = 34.204.134.140

OPTIONS = NULL

-- TCP --

PUERTO ORIGEN = EF 2E = 61230

PUERTO DESTINO = 01 BB = 443 (HTTPS)

SN = 88 0F E7 C5

AN = 6D 83 4D 7F

HEADER LENGTH = 5

RESERVADO = 0

FLAGS = 11 = 0001 0001

- CWR = ECE = URG = 0
- ACK = 1

- PSH = RST = SYN = 0
 - FIN = 1
- a. La dirección origen es una dirección privada. Entonces está egresando.
 - b. Corresponde a un router porque la DIR de origen es una IP privada.
 - c. 0 saltos porque recién egresa. Esto se ve en el hecho de que se mandó desde un host a un router, y los saltos se incrementan de router en router, por lo tanto, hay 0 saltos.
 - d. HTTPS
 - e. FIN = 1 => CLOSE WAIT

2)

SNMP => Trabaja sobre UDP

CIR = 0,5 * Access Rate = 128 kbps

EIR = 64 kbps

Tamaño de la trama de Poll = 44 + 8 (UPD) + 20 (IP) + 6 (FR) = 78 bytes

Tamaño de todos los Polls = 78 * 50 = 3900 bytes

2. Una consola de monitoreo sondea dispositivos en la red utilizando SNMP. Para monitorear 50 routers de una red Frame Relay, envía mensajes GetRequest-PDU (44 bytes*) sobre el siguiente acceso:

Access Rate: 256 kbps
CIR: 50%
EIR: 64Kbps

Indique:

- a. ¿Con qué frecuencia máxima [Poll/Sec] puede sondear a los dispositivos, asegurando que TODOS los mensajes se transporten garantizados (sin marcar)?
- b. ¿Cuántos dispositivos podrá sondear [por segundo] como máximo, si ningún mensaje debe ser rechazado por la red (descartado)?
- c. ¿Qué se debe hacer para monitorear con esta estación a 2.000 routers? Indique 3 alternativas

- a. Poll/s <= CIR -> N*31200 b/s <= 128.000 b/s -> N = 4,1 poll/s/s
(Lo tengo que redondear en 4)

También se puede hacer así:

$$Bc=31200 \text{ b} \Rightarrow Bc = CIR * Tc \Rightarrow Tc = 0,24375 \text{ s} \Rightarrow 1/Tc = 4,10 \text{ poll/s}$$

- b. $Tc = 1\text{s} \Rightarrow (EIR+CIR) * Tc = \text{Trama} * \# \text{dispositivos} \Rightarrow \# \text{dispositivos} = 307$

c. Tamaño de todos los pools = $2000 * 78 \text{ B} = 156.000 \text{ B} = 1,248 \text{ Mb}$
=> se excede el AR. Puedo: aumentar el AR; disminuir el tamaño de la trama (si es posible); monitorear en intervalos por grupo.

3) IGUAL A LOS ANTERIORES

✓ 3. Particione el rango de direcciones 10.16.0.0/22 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de las siguientes redes: a) 256 hosts, b) 70 hosts y c) 58 hosts
Indique en cada caso, la dirección de sub-red y la máscara o prefijo asignados

4. Compare las cabeceras IP versión 6 y versión 4:
✓ a. ¿Qué campos están presentes en ambas cabeceras? Detalle las características
✓ b. ¿Cuáles ya no están presentes en la versión 6?
✓ c. ¿Cómo identifica cada uno de ellos la dirección de "Broadcast"?
5. Protocolo ICMP
✓ a. ¿Cuál es su función?
✓ b. ¿Qué mensajes conoce?
✓ c. ¿Qué condición genera un mensaje "Destino inalcanzable – Host destino inalcanzable".
✓ d. ¿Qué mensajes intercambia la aplicación PING?
✓ e. ¿Cómo descubre Traceroute los routers a lo largo del camino?

4) Compare las cabeceras IPv6 y IPv4

a. **¿Qué campos están presentes en ambas cabeceras? Detalle las características**

Direcciones de origen y destino.

TTL y Hop Limit. Cada router decrementa este campo en una unidad. Si llega a 0, el datagrama se descarta.

Versión. Son 4 bits que indican la versión del protocolo (4 o 6)

b. **¿Cuáles ya no están presentes en la v6?**

Longitud del header, Tipo de servicio, Longitud total, flags, Offset Fragment, Protocolo, Checksum, Opciones y Relleno.

c. **¿Cómo identifica cada uno de ellos la dirección Broadcast?**

IPv4 utiliza una IP reservada que corresponde a la última dirección de red (todos los bits correspondientes al host en 1).

IPv6 no tiene una dirección de Broadcast, si no que tiene direcciones especiales de Multicast (comienzan con 0xFF)

5) ICMP

a. **¿Cuál es su función?**

Proporciona feedback sobre problemas del entorno de la comunicación. El

mensaje ICMP se envía en respuesta a un datagrama desde el router o por el host destino.

b. ¿Qué mensajes conoce?

Tipo de mensaje.	Descripción.
<i>Destination unreachable</i>	El router no puede localizar el destino. En algunas redes, el router puede detectar si un computador es inalcanzable. El mismo computador de destino puede devolver este mensaje si algún punto de acceso de un nivel superior no es alcanzable. Un paquete con el bit DF no puede entregarse porque hay una red de paquetes pequeños que se interpone.
<i>Time exceeded</i>	Se descartó un paquete porque su TTL ha llegado a cero.
<i>Parameter problem</i>	Valor inválido en el header.
<i>Source quench</i>	Se usaba para el control de flujo
<i>Redirect</i>	El router detecta que el paquete está mal enrutado. El router avisa al host emisor que se actualice con una mejor ruta.
<i>Echo and echo reply</i>	Se usan para ver si un destino es alcanzable y está vivo. El destino debería responder <i>ECHO REPLAY</i> luego de recibir un <i>ECHO</i> . Se usan en la herramienta ping.
<i>Timestamp request/replay</i>	Similares a <i>echo</i> . El tiempo de llegada y de salida de la respuesta se registran.
<i>Router advertisement/solicitation</i>	Permiten que los hosts encuentren routers cercanos.

c. ¿Qué condición genera un mensaje “Destino inalcanzable - Host destino inalcanzable”?

El router logró llegar a la red destino, pero el host destino no responde.

d. ¿Qué mensajes intercambia la aplicación PING?

Echo y Echo Reply

e. ¿Cómo descubre Traceroute los routers a lo largo del camino?
???

11-2-2015 (KOVAL)

1)

0000	[a0 88 b4 16 c3 d4]	[c8 b3 73 03 55 e2]	[08 00]	[45 00]s.U....E.
0010	[00 28 1c 9e 40 00]	[31 06 63 14]	[c0 00 48 03]	[c0 a8]	.(..@.1.c....H...
0020	01 72 [00 50 cc 74]	[2d 8d 05 dc]	[a4 0e 23 4b]	[50 11]	.r.P.t-.....#KP.
0030	00 44 [1d ea 00 00]				.D....

- a. Indique quién envía este segmento: ¿Cliente o Servidor? ¿Cómo lo deduce?
- b. ¿En qué estado se encuentra la conexión? ¿Qué segmento se enviará a continuación?
- c. ¿El cliente y el servidor, se encuentran en la misma red LAN?

2) IGUAL A LOS ANTERIORES

- c. ¿El cliente y el servidor, se encuentran en la misma red LAN?
- 2. Particione el rango de direcciones 172.16.0.0/23 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de 3 redes de: a) 129 hosts, b) 10 hosts y c) 58 hosts
Indique en cada caso, la dirección de red y la máscara o prefijo asignados

2) YA RESUELTO EN 14-2-2018

3. Una consola de monitoreo sondea dispositivos en la red utilizando SNMP.
Para monitorear 50 routers de una red Frame Relay, envía mensajes GetRequest-PDU (44 bytes*) sobre el siguiente acceso:

Access Rate: 256 kbps
CIR: 50%
EIR: 64Kbps

Indique:

- a. ¿Con qué frecuencia máxima [Poll/Sec] puede sondear a los dispositivos, asegurando que TODOS los mensajes se transporten garantizados (sin marcar)?
- b. ¿Cuántos dispositivos podrá sondear [por segundo] como máximo, si ningún mensaje debe ser rechazado por la red (descartado)?
- c. ¿Qué se debe hacer para monitorear con esta estación a 2.000 routers? Indique 3 alternativas

* Calcule el tamaño del mensaje adicionando las cabeceras de capa 2,3 y 4 correspondientes

4. Explique el mecanismo de control de acceso al medio DCF utilizado por 802.11. ¿En qué difiere del PCF?

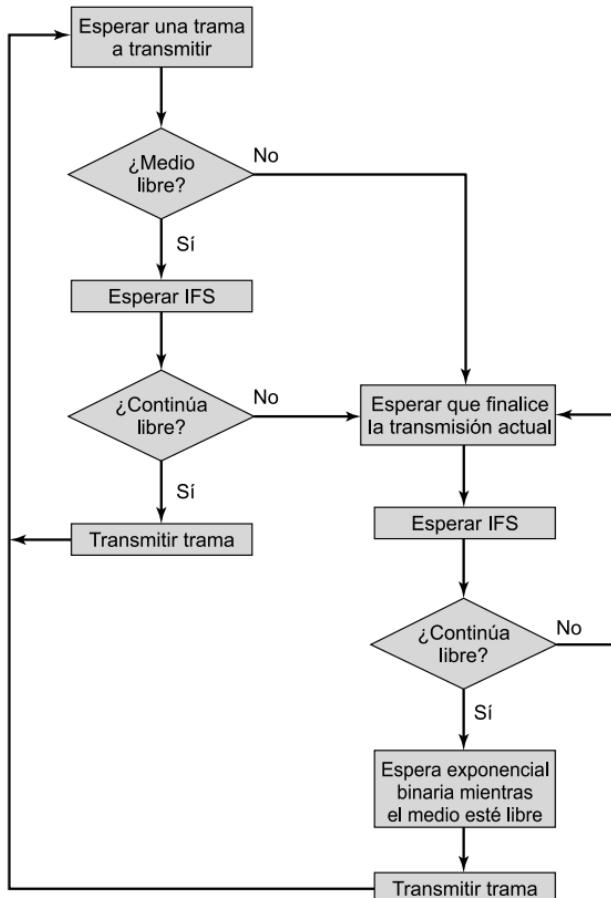
5. ¿Qué función cumple un protocolo de ruteo? ¿En qué se diferencia un protocolo "Link State" de uno "Distance Vector"?

6. TCP.

- a. ¿Qué mecanismo implementa el campo "Window" de la cabecera? ¿Qué longitud tiene este campo cuál es el "crédito" máximo? ¿Conoce algún mecanismo para extenderlo?
- b. RTO: Explique el significado y la utilidad de esta variable. ¿Cómo se calcula? ¿Qué efectos produce una subestimación/sobreestimación de su valor?

4) Explique el mecanismo de control de acceso al medio DCF utilizado por 802.11. ¿En qué difiere del PCF?

DCF (Función de coordinación distribuida). Se usa un algoritmo de contención para proporcionar acceso a la totalidad del tráfico. Ese algoritmo es el CSMA/CA refinado para hacer uso de distintos IFS (c/u con distintas prioridades).



SIFS. Es el tiempo más corto (con mayor prioridad). Se usa para los ACK, CTS/RTS y Poll/Response.

DIFS. Es el retardo mínimo para las tramas asíncronas que compiten por el acceso al medio.

PCF (Función de coordinación puntual).

Consiste en un sondeo realizado por un elemento central de sondeos (coordinador puntual). El coordinador hace uso de un PIFS cuando emite un sondeo. El PIFS es más pequeño que el DIFS, por lo tanto el coordinador puede adueñarse del medio y bloquear todo el tráfico asíncrono mientras emite un sondeo y recibe respuestas. Se garantiza un servicio libre de contención.

5) ¿Qué función cumple un protocolo de ruteo? ¿En qué se diferencia un protocolo “Link State” de uno “Distance Vector”? REPETIDA

6) TCP

- a. ¿Qué mecanismos implementa el campo “Window” de la cabecera?
¿Qué longitud tiene ese campo? ¿Cuál es el crédito máximo?
¿Conoce algún mecanismo para extenderlo?

Se implementa el mecanismo de Ventana Deslizante con asignación de créditos. Los créditos no son tramas. sino que son octetos. La ventana indica la cantidad de octetos que el emisor puede enviar sin tener que esperar confirmación.

La longitud del campo es de 16 bits, dando un total de 65535 B (Valor máximo).

Existe una opción en TCP “Window Scale” el cual permite a las partes negociar un factor de escala de ventana. El tamaño de venta se puede correr hasta 14 bits, dando un total de $2^{30} = 1 GB$

- b. RT0: Explique el significado y la utilidad de esta variable.
¿Cómo se calcula? ¿Qué efectos produce una subestimación/sobreestimación de su valor? REPETIDA

PARCIALES (KOVAL)

Primer Parcial

1º Parcial de REDES DE INFORMACION

1) Redes LAN

- ¿En qué difieren los formatos de trama Ethernet y 802.3? ¿Cómo determina el receptor de una trama 802.3 a qué capa superior entregar el PDU?
- ¿Cómo está compuesta una dirección MAC? ¿Cuál es la dirección de broadcast?
- ¿Cómo realiza Ethernet el control de errores?
- ¿Qué utilidad tiene el protocolo Spanning Tree? ¿Qué dispositivos lo ejecutan?

2) Wireless LAN

- ¿Cuáles son las bandas en que operan las diferentes normas? ¿Qué diferencias hay entre ellas?
- ¿Cómo opera un AP en modo PCF?
- ¿Cuántas direcciones MAC contiene la cabecera 802.11? ¿Qué dispositivos identifican?

3) IP

- ¿Qué es el Default Gateway? ¿Qué es el Default Route y como se relacionan?
- ¿Qué son "direcciones privadas"? ¿Qué rangos reserva la RFC1918?
- ¿Qué campos de la cabecera intervienen en el mecanismo de fragmentación?
- ¿Qué mensajes intervienen en la operación del ARP? ¿A quién/es va/n dirigidos?

1) REDES LAN

- ¿En qué se difieren los formatos de trama Ethernet y 802.3?
¿Cómo determina el receptor de una trama 802.3 a qué capa superior entregar el PDU?

Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos ↓↓	Relleno	Suma de verificación
(b)	Preámbulo	S o F	Dirección de destino	Dirección de origen	Longitud ↓↓	Datos	Relleno

Figura 4-14. Formatos de trama. (a) Ethernet (DIX). (b) IEEE 802.3.

La diferencia está en el campo **Tipo/Longitud**. En Ethernet clásico, el campo Tipo indica el protocolo de capa superior. En IEEE 802.3, el campo puede utilizarse para ambos casos: si el número es menor o igual a 1536 (0x600), representa una longitud; si es mayor a 0x600,

representa el tipo. Si en ese campo se envía la longitud, en el protocolo LLC se envía el dato del protocolo de capa superior.

- b. ¿Cómo está compuesta una dirección MAC? ¿Cuál es la dirección de broadcast?

Son 48 bits (representada mediante 6 pares de dígitos hexadecimales). Los primeros 24 bits representan el Identificador Único del fabricante (OUI) y los últimos 24 al Identificador del producto (UAA). La dirección de broadcast está representada por aquella que tiene todos los bits en 1 (FF:FF:FF:FF:FF:FF)

Dirección MAC

01:3A:1D:54:6B:32

Identificador Unico del fabricante (OUI) identificador del producto (UAA)

- c. ¿Cómo realiza Ethernet el control de errores?

En la cabecera de Ethernet, se tiene un campo FCS que utiliza CRC-32 sobre todos los campos de la trama, menos el preámbulo (y el propio FCS). Además, mediante el algoritmo CSMA/CD con retroceso exponencial binario, se realiza el manejo de colisiones (dos máquinas enviando tramas al mismo tiempo).

- d. ¿Qué utilidad tiene el protocolo Spanning Tree? ¿Qué dispositivos lo ejecutan?

El protocolo Spanning Tree es ejecutado por los bridges de la red. Su propósito es impedir la acción de bucles que se generan en los bridges cuando existen vínculos redundantes. Transforma una red de tipo malla con bucles en una red lógica de tipo árbol libre de bucles.

2) Wireless LAN TODO

- ¿Cuáles son las bandas en que operan las diferentes normas?
¿Qué diferencias hay entre ellas?
- ¿Cómo opera un AP en modo PCF?
- ¿Cuántas direcciones MAC contiene la cabecera 802.11? ¿Qué dispositivos identifican?

3) IP

a. **¿Qué es el default gateway? ¿Qué es el Default Route y cómo se relacionan?**

b. **¿Qué son direcciones privadas? ¿Qué rango reserva la RFC1918?**

Son direcciones que pueden estar repetidas (globalmente) ya que solo tienen alcance local (no se pueden usar para tener acceso a Internet). Se usa para comunicar dispositivos en una LAN. Son de clase A, B y C

CLASE A: 10.0.0.0 - 10.255.255.255

CLASE B: 172.16.0.0 - 172.31.255.255

CLASE C: 192.168.0.0 - 192.168.255.255

c. **¿Qué campos de la cabecera intervienen en la fragmentación?**

En IPv4 tenemos el campo Offset Fragment, el flag DF (Don't Fragment), el flag MF (More Fragments)

d. **¿Qué mensajes intervienen en la operación del ARP? ¿A quiénes van dirigidos?**

ARP Request: un nodo envía un datagrama ARP mediante un broadcast MAC indicando que busca la dirección física del host con una IP dada.

ARP Reply: el host al que corresponde esa IP responde con un reply diciendo que él es el nodo que se está buscando e indica su dirección física.

1) Modelo OSI

a. **¿Cuántas y cuáles son las capas del Modelo?**

APLICACIÓN (7)
PRESENTACIÓN
SESIÓN
TRANSPORTE
RED
ENLACE DE DATOS
FÍSICA (1)

b. ¿En qué se diferencia del modelo DARPA/TCP/IP?

La capa de Internet corresponde a la de Red. La de Acceso a red cubre la de enlace de datos y la física.

Aplicación
Transporte
Internet
Acceso a red

c. ¿En qué capa/s se realiza el control de errores?

En la capa de enlace de datos.

2) Redes LAN

a. ¿Cuál es la longitud mínima de una trama 802.3?

46 bytes

b. ¿Con qué objetivo se fijó esa longitud mínima?

Los 46 bytes + 18 bytes (header) son la ventana de colisión. El estándar define 2500 metros a una velocidad de 10 Mbits. Se necesitan transmitir 512 bits (64 bytes) para llenar el medio. Si se manda un mensaje más corto, la venta permite que otra estación NO me colisione sin darme cuenta. (Se puede leer en Redes de computadoras, p 270 del pdf).

c. ¿Qué longitud tiene una dirección MAC? ¿Qué campos la componen?

Resuelta más arriba.

d. ¿Qué es el protocolo 802.1Q y qué funcionalidad introduce?

Es un protocolo relacionado a las VLANs. Los bridges necesitan saber a qué VLAN pertenece una trama para poder reenviarla. El estándar 802.1q introduce un nuevo campo con una etiqueta VLAN. Los bridges y conmutadores utilizan esa nueva etiqueta. Contiene un identificador de VLAN, el cual es usado por el bridge como un índice en una tabla para averiguar a cuáles puertos enviar la trama.

e. ¿En qué puerto entregará el switch una trama con dirección

destino desconocida?

Se transmite a todos los puertos, excepto aquel por donde vino la trama.

3) Wireless LAN**a. ¿En qué se diferencian los modos DCF y PCF?**

DCF utiliza CSMA/CA refinado mediante un mecanismo basado en distintos IFS con distintas prioridades (aquellos más cortos tienen más prioridad). SIFS se usa para los

PCF consiste en un sondeo realizado por un elemento central (coordinador puntual). El coordinador usa PIFS cuando emite un sondeo. Dado que PIFS es menor que DIFS, el coordinador puntual puede adueñarse del medio y bloquear todo el tráfico asíncrono mientras emite un sondeo y recibe las respuestas.

b. ¿Qué es el NAV y qué función cumple?

Para reducir las ambigüedades con respecto a qué estación va a transmitir, se define la detección del canal como un proceso físico y virtual. En la detección física se verifica si el medio tiene una señal válida. En la detección virtual cada estación mantiene un registro lógico del momento en que se usa el canal rastreando el NAV. Cada trama lleva un campo NAV que indica cuánto tiempo tardará en completarse la secuencia a la que pertenece esa trama. Las otras estaciones que escuchen la trama saben que el canal estará ocupado durante el período indicado por el NAV, sin importar si pueden o no detectar una señal física.

c. ¿Qué función cumple el campo "duración" en la trama 802.11?

Ese campo es utilizado por las estaciones para administrar el NAV

4) IP**a. ¿Cuántas direcciones Clase A existen? ¿Cuántos host permite direccionar una Clase A?**

La máscara de clase A es 255.0.0.0 (/8). Esto significa que hay 24 bits asignados para los hosts y 8 para las direcciones de red. El primer bit está fijo en 0 y la dirección 127 está reservada. Entonces el rango posible (en la práctica) es de 0 a 126, en la teoría es de 0 a 127 (128 redes)

Cantidad de direcciones por red = $2^{24} = 16.777.216$

Cantidad de hosts = *Cantidad de direcciones por red* - 2 = 16.777.214

b. ¿Puede la dirección 172.16.255.3 ser una dirección de broadcast? ¿De qué red?

La analizamos a nivel bit:

10101100.00010000.11111111.00000011

La dirección de broadcast de una red es aquella que tiene todos 1s en la parte de hosts. Los últimos dos bits son 11, entonces el resto de los bits corresponden a la dirección:

10101100.00010000.11111111.000000|00 = 172.16.255.0

c. ¿Cuántas subredes se obtienen al aplicar una máscara de 13 bits a una red Clase A?

$13 - 8 = 5 \text{ bits} \Rightarrow 2^5 = 32 \text{ subredes posibles}$

d. ¿Cuál es la nueva máscara resultante?

Máscara de Clase A = 255.0.0.0

Máscara de /13 = 255.248.0.0

e. ¿Quién se encarga de la fragmentación en IP? ¿Y quién del reensamblado?

La fragmentación puede ser realizada por el emisor inicial o los routers que están entre el emisor y el receptor. El reensamblado es realizado por el destino.

1) Redes LAN

a. ¿En qué difieren los formatos de trama Ethernet y 802.3? ¿Cómo determina el receptor de una trama 802.3 a qué capa superior

entregar el PDU? Resuelto más arriba.

b. ¿Cómo está compuesta una dirección MAC? ¿Cuál es la dirección de broadcast? Resuelto más arriba.

c. ¿Cómo realiza Ethernet el control de errores?

Al final de la trama Ethernet, se tiene un campo FCS (Frame Check Sequence). Ethernet usa el mecanismo CRC32 para verificar la integridad de las tramas transmitidas.

d. Spanning Tree: ¿Cómo se realiza la elección del bridge Raíz "Root"?

Los bridges intercambian mensajes BPDUs cada 2 segundos. El BPDU contiene el BID (Bridge ID) del root bridge que conocen hasta el momento y su propio BID. Al comienzo, cada bridge se tiene como root bridge, o sea, indican "Yo soy el root". Al recibir BPDU con un BID menor que el suyo, deja de anunciar como root y anuncia el otro BID como tal. El root se termina eligiendo mediante el menor BID. El BID está conformado por el Bridge Priority y la MAC Address.

2) **Wireless LAN**

a. ¿Qué elementos componen una red wireless?

1. Access Point. Los clientes se asocian a un AP que está conectado a la otra red. Los clientes envían y reciben paquetes a través del AP.
2. Terminal. Equipo conectado a la red.
3. Sistema de distribución (DS). Varios AP pueden estar conectados mediante una red alámbrica. Esa red es el DS.

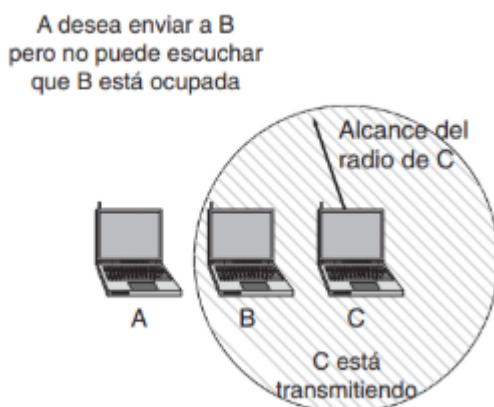
b. ¿Cuáles son las normas y en qué banda operan?

802.11 Wireless LAN Standards

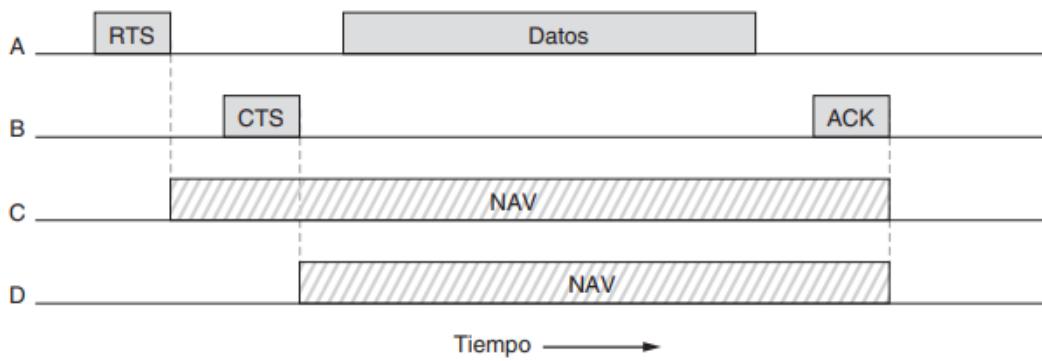
	802.11a	B	G	N	AC
Velocidad (Mbps)	54 Mbps	11	54	Hasta 600	433 /867 /1.69 Max 3.39 Gbps
Frecuencia de operación (GHz)	5	2.4	2.4	5 & 2.4	5 & 2.4
Modulación	QPSK, 16QAM, 64QAM	DSSS	OFDM, DSSS	OFDM	OFDM

c. ¿En qué consiste el problema del nodo oculto? ¿Cómo lo resuelve 802.11?

El problema del nodo oculto ocurre cuando una estación no puede detectar a un posible competidor en el medio debido a que está muy lejos.



Se soluciona mediante el uso de NAV con RTS/CTS. La terminal A manda un RTS, la terminal B responde con un CTS. A sabe que puede enviar datos y las demás terminales saben que alguien va a mandar datos, así que actualiza su NAV y se queda en silencio hasta que termine la transmisión.



3) IP

- ¿Qué es el Default Gateway? ¿Qué es el Default Route y cómo se relacionan?** TODO
- ¿Cuáles son las direcciones Clase D, cuántas son y para qué se utilizan?**

Son las direcciones IP reservadas para multicast (direcciones de grupo). Van de 224.0.0.0 a 239.255.255.255. Los primeros 4 bits corresponden a 1110. Si hay 4 bits fijos, quedan 28 bits para la dirección => $2^{28} = 268.435.456$

- ¿Qué campos de la cabecera intervienen en el mecanismo de fragmentación?** Repetida
 - ¿Qué mensajes intervienen en la operación del ARP? ¿A quién/es van dirigidos?** Repetida.
-

Segundo Parcial

1)

1) Analizando la siguiente captura:

ETH [00 05 9a 3c 7a 00 00 11 22 33 44 55 08 00 45 28 ...<z... "3DU..E(00 34 0a d1 40 00 6d 06 4e 47 34 6d 0c 12 ac 15 .4...@.m.NG4m.... c7 ef 01 bb)ca a4 5e 7c 6e e7 05 f9 81 58 80 121^|n...X.. 20 00 7a 07 00 00 02 04 05 14 01 03 03 08 01 01 ..z..... 04 02] Header length

Responda:

TCP

- a. ¿Quién envía el segmento?
- b. ¿Cuál será el siguiente segmento a intercambiar y quién lo enviará?
- c. ¿Contiene opciones?
- d. ¿Cuál es el ISN del cliente?
- e. ¿Cuál es el ISN del servidor?

Nos pide solo TCP. Los primeros 14 bytes son de Ethernet. Los siguientes 20 bytes son de IP. Es decir, los primeros 34 pares de hexa no nos importan para este ejercicio.

Puerto Origen = 01 bb = 443 (HTTPS) (Server)

Puerto Destino = ca a4 = 51876

SEQ = 5e 7c 6e e7 =

ACK = 05 f9 81 58 =

Header Length = 8 (palabras de 32 bits) =>

Reservado = 0

Flags = 12 = 000 ACK=1 00 SYN=1 0

Window = 20 00

Checksum = 7a 07

URG Pointer = 00 00

Options =

- a. El puerto 443, el server.
- b. Se está confirmando el segmento 05 f9 81 58, el cliente enviaría desde ese segmento.
- c. Sí. El header length es de 8. Si no tuviera opciones, debería ser de 5 (palabras de 32 bits)
- d. ACK=1 y SYN=1 => CONNECTION ACCEPTED. El server está aceptando la conexión. El cliente tuvo que haber enviado su ISN = X. El server está respondiendo con ACK = X + 1 y SEQ = ISN_Server = Y. Entonces ISN_CLIENTE = ACK - 1
- e. ISN_SERVER = SEQ

2) DNS: ¿qué es un resource record? ¿Cuáles conoce?

Un resource record es una entrada en la base de datos del DNS.

- **Host Record**: asocia estáticamente un nombre de Host con una dirección IP.
Comprende la mayor parte del archivo y lista todos los Hosts dentro de la zona
`www IN A 200.69.225.145`
- **MX Mail Exchange**: asocia un dominio de email con la dirección de los servidores de correo
`@ IN MX [10] mailhost`
`@ IN MX [20] mail1.infovia.com.ar`
- **CNAME Canonical Name**: permiten asociar más de un nombre de Host a una única dirección IP (alias)
`ftp CNAME Rhino`

3) ICMP: ¿Qué mensajes de reporte de error conoce? ¿Qué produce que se generen? Repetida

4) IPv6: ¿En qué consisten la compresión y supresión de ceros?

Compresión: donde sólo hay ceros, se reemplaza con ::

Supresión: en un grupo se pueden suprimir los 0s de la izquierda

Representación Hexadecimal, agrupado de a 16 bits, separados por ":"

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

Notación con supresión de ceros:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

Notación con compresión de ceros:

Por ejemplo, la dirección local **FE80:0:0:0:2AA:FF:FE9A:4CA2**

Se representa como: **FE80::2AA:FF:FE9A:4CA2**

5) ¿Qué características tiene una función de HASH?

Una función HASH debe cumplir:

1. Consistencia. Misma entrada, misma salida.
2. Aleatoriedad. Debe impedir adivinar el mensaje original.

3. Unicidad. Debe ser casi imposible encontrar dos mensajes con el mismo *digest* (resultado de la función hash).
4. One way. No debe ser posible obtener el mensaje usando el *digest*.

1)

1) Análisis de trama

0000	00 23 69 ca 9c a2 00 1a 73 67 8d 26 08 00 45 00
0010	00 44 09 b4 00 00 80 11 ad 3a c0 a8 01 69 c0 a8
0020	01 01 ed 70 00 35 00 30 d4 9d aa 46 01 00 00 01
0030	00 00 00 00 00 00 05 63 68 65 63 6b 0c 73 61 6e
0040	61 73 65 63 75 72 69 74 79 03 63 6f 6d 00 00 01
0050	00 01

Hallar la siguiente información en el formato que corresponde:

- a) Dir MAC fuente y destino
- b) Dir IP fuente y destino
- c) Puerto fuente y destino

2) WAN

- a) Describir los campos de la trama HDLC

8 bits	8	8 o 16	Variable	16 o 32	8
Delimitador	Dirección	Control	Información	FCS	Delimitador

Los campos **delimitador** corresponden a la secuencia 01111110. Se usan para sincronizarse con el comienzo y fin de la trama.

El campo **dirección** identifica a la estación secundaria.

En el campo **control** se implementan los mecanismos de control de flujo y control de enlace. La trama puede ser de **información, supervisión, y no numerada**.

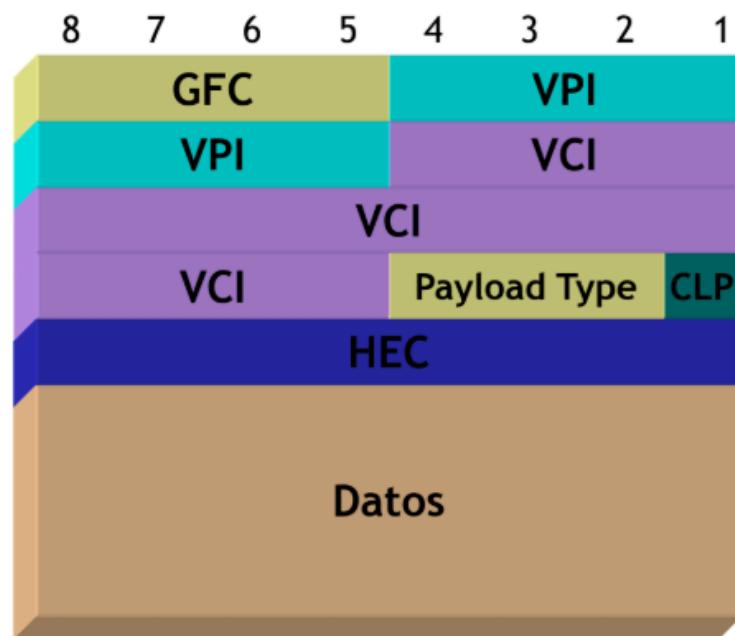
En **FCS** se usa CRC16 o CRC32 para la detección de errores.

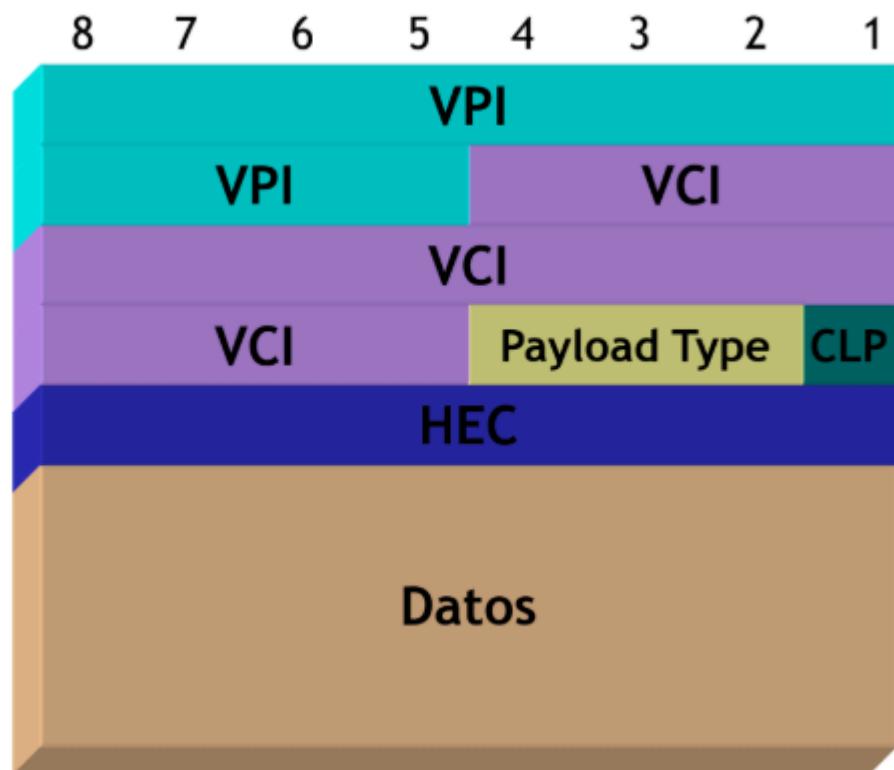
b) Mencionar el concepto de PAD en X.25 y los protocolos asociados al mismo ???

3) WAN

a) Describir el formato de las celdas ATM

Formato de Celda - UNI





b) Mencionar el significado del CAR, CIR y SLA

CAR (Committed Access Rate). Es la garantía mínima ofrecida por el servicio. Se asegura que esa capacidad va a estar disponible siempre, aun en caso de congestión.

CIR (Committed Information Rate). Es una velocidad en bps que acuerda la red para dar soporte a una conexión. Si un dato se transmite a una velocidad mayor al CIR, puede ser rechazado cuando se produce una congestión.

SLA (Service Level Agreement). Es un contrato entre un proveedor de servicios y un cliente que define los niveles de servicio garantizados (acá se contempla el CIR y el CAR)

4) WAN

a) Describir cómo se gestionan las congestiones en Frame Relay

Frame Relay realiza medidas de prevención y notificación de la congestión. Para la prevención se utilizan los bits FECN y BECN. FECN es la notificación hacia adelante (es decir, en el sentido del frame) y BECN es en el sentido contrario. BECN indica que las tramas que

transmita el usuario a través de esta conexión lógica pueden encontrar recursos congestionados. y FECN indica que la trama, sobre su conexión lógica, ha encontrado recursos congestionados.

En la prevención entra en juego el CIR (Committed Information Rate). Todo dato que se transmite a una velocidad mayor al CIR se coloca con DE=1 y puede ser descartado.

b) Mencionar el rango de velocidades en que se usa Frame Relay

Velocidades de $N \times 64$ hasta 34 Mbps ($N=1, 2, 3, 4, \dots$). Es decir, acepta velocidades múltiplo de 64 Kbps (redes telefónicas de 64 Kbps).

5) Seguridad

a) Definir las encriptaciones simétrica y asimétrica. REPETIDA

b) Mencionar los protocolos de seguridad aplicables en cada capa

IPsec -> Capa de Red

TLS -> Capa de transporte

Firewall -> Capa de aplicación

1)

1) Analizando la siguiente captura:

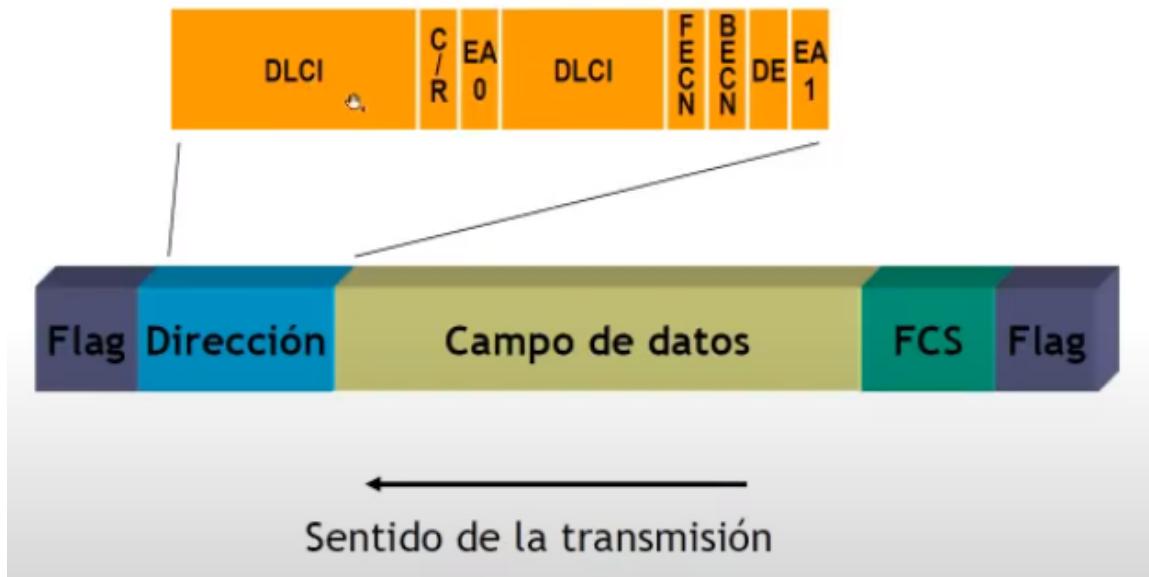
0000 90 e2|ba 21|3e 21 d8 fc|93 33 5b cb|08|00 45|00 ...!>!...3[...E.
0010 00|28 6e f0 40 00 80 06 3e b1 0a 5d 09 0b 28 65 .(n.@...>...])..(e
0020 1f 62 f6 70 01 bb 14 b3 70 44 bc d6 31 72 50 10 .b.p....pD..lrP.
0030 00 40 f6 f9 00 00 .@....

Indique el contenido de los siguientes campos para el PRÓXIMO segmento intercambiado en esta conexión:

TCP

- a. Puerto Origen
- b. Puerto Destino
- c. Secuencia
- d. Confirmación (Acknowledge)
- e. Flags (UAPRSF)

2) Frame Relay, describa el formato de la trama detallando especialmente el contenido del campo "Dirección"



- **DLCI.** Identificador de conexión del enlace de datos. Misma función que el número de circuito virtual en X.25 (permitir la multiplexación de varias conexiones lógicas a través de un único canal). Tiene sentido local.
- **C/R.** Comando/respuesta (uso por la aplicación).
- **EA0/EA1.** Bit de extensión del campo de dirección (ubicado al final de cada byte)
 - EA=0 → hay otro byte para campo de dirección; éste no es el último byte.
 - EA = 1 → éste es el último byte del campo de dirección.
- **F-FECN.** Notificación de congestión explícita hacia adelante.
 - F = 1 → hay congestión hacia adelante.
 - F = 0 → no hay congestión hacia adelante.
- **B-BECN.** Notificación de congestión explícita hacia atrás
 - B = 1 → hay congestión hacia atrás.
 - B = 0 → no hay congestión hacia atrás
- **DE.** Elegido para descarte.
 - DE = 1 → si hay congestión en la red, el frame se descartará.
 - DE = 0 → el frame no está elegido para descarte, no se descartará.

3) ¿Qué características tiene el tráfico implementado por las AAL1 y AAL2 en ATM?

4) Explique el uso de los 6 flags de TCP

- URG: 1 si está en uso el *apuntador urgente*.
- ACK: 1 si el *número de confirmación de recepción* es válido.

- PSH: 1 si los datos se deben transmitir de inmediato.
- RST: se usa para restablecer de manera repentina una conexión que se ha confundido debido a una falla de host o alguna otra razón; y para rechazar un segmento no válido o un intento de abrir una conexión.
- SYN: se usa para establecer conexiones.
 - $SYN = 1$ y $ACK = 0 \Rightarrow CONNECTION\ REQUEST$
 - $SYN = 1$ y $ACK = 1 \Rightarrow CONNECTION\ ACCEPTED$
- FIN: se usa para liberar una conexión y especifica que el emisor no tiene más datos que transmitir.

5) **¿Qué servicio ofrece el protocolo TLS? ¿Qué método de encriptación utiliza? ¿Qué es una Autoridad Certificante (Root CA)?**

6) **¿Cómo realiza TCP el control de flujo? Explique qué campos intervienen.**

El protocolo básico que utilizan las entidades TCP es el protocolo de ventana deslizante (basado en créditos) con un tamaño dinámico de ventana. Cuando un emisor transmite un segmento, también inicia un temporizador. Cuando llega el segmento al destino, la entidad TCP receptora devuelve un segmento (con datos si existen, de otro modo sin ellos) que contiene un número de confirmación de recepción igual al siguiente número de secuencia que espera recibir, junto con el tamaño de la ventana remanente. Si el temporizador del emisor expira antes de recibir la confirmación de recepción, el emisor transmite de nuevo el segmento. Intervienen el tamaño de ventana, el número de secuencia y el número de confirmación.

1) La suite IPSec contempla dos protocolos y dos modos de operación. ¿Cuáles son? Repetida

2) Frame Relay. Explique los mecanismos implementados con los bits DE y FECN.

FECN (notificación de congestión hacia adelante) es utilizado para la prevención de la congestión. Que sea hacia adelante significa que es en el mismo sentido que el del frame. El bit es seteado por el nodo (POP) y lo detectan los CPEs.

DE se setea cuando el usuario envía datos a una velocidad mayor a la contratada (CIR). Esos frames con el DE=1 no se descartan directamente, sino que se descartan en caso de congestión.

3) ¿Para qué se utilizan las opciones AAL1 y AAL2 en ATM? ¿En qué se diferencian? REPETIDA

4) **¿Cómo se realiza el cierre de la conexión en TCP? ¿y en UDP?**

Cada usuario TCP debe emitir una primitiva Close. Se setea el bit FIN en el último segmento que envía. Si un usuario emite un Abort, se produce un cierre abrupto. Se descartan todos los datos del buffer y se envía un RST al otro extremo.

En UDP no se debe realizar el cierre de la conexión, ya que el protocolo no es orientado a conexión, es decir, no establece una conexión y, por lo tanto, no mantiene un estado de la misma.

5) **¿Qué provoca la retransmisión de un segmento TCP? ¿Cómo se detecta la necesidad de retransmitir?** REPETIDA (RT0, etc)

6) **¿Qué características debe cumplir una función de "Hash"?** Repetida

1)

Source	Destination	Protocol	Info
172.21.105.100	172.16.132.73	TCP	49615-80 [SYN] Seq=0 Win=8192 Len=0
172.21.105.1	172.21.105.100	ICMP	Redirect (Redirect for t
172.16.132.73	172.21.105.100	TCP	80-49615 [SYN, ACK] Seq=0 Ack=1 Win=
172.21.105.100	172.16.132.73	TCP	49615-80 [ACK] Seq=1 Ack=1 Win=66560
172.21.105.100	172.16.132.73	HTTP	GET /SI/tikiwiki/tiki-jsplugin.php?1
172.16.132.73	172.21.105.100	TCP	80-49615 [ACK] Seq=1 Ack=616 Win=504
172.16.132.73	172.21.105.100	TCP	[TCP segment of a reassembled PDU]
172.16.132.73	172.21.105.100	TCP	[TCP segment of a reassembled PDU]
172.21.105.100	172.16.132.73	---	-----

- ¿Cuántos bytes ocupa la petición HTTP GET?
- ¿De qué tamaño es cada uno de los fragmentos en que fue dividida la respuesta?
- ¿Qué opciones TCP se intercambian? Explique la utilidad de cada una.
- ¿Quién de los dos otorgará un crédito mayor y por qué?

- Se ve que manda el número de SEQ=1 y el server responde con ACK=616. El cliente indica que está mandando a partir del byte 1 y el servidor confirma hasta el byte 616 => La petición ocupa 615 bytes.
- Se enviaron 3 segmentos TCP (cada uno con su cabecera IP). Si asumimos que el MSS=200 B, entonces cada segmento envió 200 B

- de datos. Los primeros dos segmentos serían de 240B (200 + encabezados) y el último de 45 B (15 + 40)
- c. Se debe haber intercambiado el MSS para indicar el tamaño máximo de segmento.
 - d. El cliente ya que manda una ventana de 66560 (el server de 8192)

2) ¿Cuántos y cuáles son los campos de la cabecera UDP?

Puerto de Origen (16 bits)	Puerto de destino (16 bits)
Longitud Total (16 bits)	Checksum (16 bits)
Data	

3) ¿Cómo realizan IP, TCP y UDP la detección de errores? ¿Y la corrección?

UDP tiene un campo checksum en su cabecera. Si se detecta un error, se descarta el datagrama.

TCP también detecta errores mediante un checksum en la cabecera y aquellos segmentos con errores deben retransmitirse. No tiene confirmación negativa (RJN), sino que la ausencia de confirmación hace que el RTO expire y se debe reenviar el segmento.

4) IPv6 describa las características de una dirección IPv6 y compárela con una IPv4.

IPv6: Dirección de 128 bits. Se representan como grupos de 4 valores hexa. Se puede usar notación de supresión y compresión de 0s. No hay dirección de broadcast (se usan direcciones multicast especiales para eso). Los primeros 64 bits

48 bits	16 bits	64 bits
Global Routing Prefix	Subnet ID	Interface ID

IPv4. Direcciones de 32 bits. Se representan como 4 grupos de valores decimales (192.168.0.1). Hay dirección de broadcast (todas los bits del host en 1).

5) Describa el establecimiento y cierre de una conexión TCP. ¿Cómo lo hace UDP?

UDP no es orientado a la conexión. Simplemente se envía el datagrama. No es fiable, es decir, no se garantiza la entrega.

En TCP el establecimiento de la conexión se realiza mediante un handshake de tres pasos. El cliente envía un header TCP con el número de secuencia inicial (ISN); el server responde con un ACK = ISN + 1 y con su propio número de secuencia inicial; el cliente recibe esa respuesta y envía un ACK = ISN_SERVER + 1 y también puede enviar sus datos. Respecto a los flags: SYN=1 y ACK=0 => CONNECTION REQUESTED; SYN = 1 y ACK = 1 => CONNECTION ESTABLISHED.

El cierre de conexión se realiza enviando el flag FIN = 1

6) DHCP: ¿Qué efectos tiene una asignación de tiempo (lease) demasiado corto? ¿Y demasiado largo?

Si el lease es muy largo, el host al que se le asignó esa IP puede estar inactivo por mucho tiempo reteniendo esa IP. Si el tiempo es muy corto, el host debe realizar más peticiones de renovación del lease.