

Nombre:

Apellidos:

Notas:

- Duración examen: 120 min.
- Este examen constituye el 60% de la nota final. "Es necesario aprobar el examen escrito para aprobar la asignatura".

(2.5p) Test

1. La suma de verificación, o checksum, se implementa en:
 - a. La capa de Red
 - b. La capa de Transporte
 - c. Las dos respuestas anteriores son correctas
 - d. Ninguna de las respuestas anteriores es correcta
2. El puerto 49151...
 - a. Es un puerto bien conocido
 - b. Es un puerto registrado
 - c. Es un puerto dinámico o privado a emplear en el servidor
 - d. Es un puerto dinámico o privado a emplear en el cliente
3. La solicitud de conexión y desconexión entre un servidor y un cliente a nivel de capa de transporte...
 - a. Ambas pueden realizarlas cualquiera de los dos
 - b. La solicitud de conexión debe realizar el cliente y cualquiera puede solicitar la desconexión
 - c. La solicitud conexión debe realizarla el servidor y cualquiera puede solicitar la desconexión
 - d. Ambas deben ser realizadas por el cliente
4. El protocolo TCP...
 - a. Debe incluir número de secuencia y puede incluir checksum
 - b. Debe incluir número de secuencia y fiabilidad de entrega
 - c. Es un protocolo orientado a conexión que puede incluir detección de errores
 - d. Es un protocolo "Best-effort"
5. Un host que quiere enviar un determinado paquete sólo puede enviarlo directamente a ese equipo si está en su red, o a la puerta de enlace.
 - a. Verdadero
 - b. Falso
6. Comprimir al máximo la dirección IPv6: 2001:1265:0000:0000:0AE4:0000:005b:06B0

2001:1265::AE4:0:5b:6B0

7. Las aplicaciones...

- a. **Escriben datos en el buffer de transporte cuando quieren y leen cuando y cuanto quieren**
- b. Escriben datos en el buffer de transporte cuando pueden y leen cuando pueden todo el contenido del buffer
- c. Escriben datos en el buffer de transporte cuando quieren y leen cuando pueden todo el contenido del buffer
- d. Escriben datos en el buffer de transporte cuando pueden y leen cuando y cuanto quieren

8. El objetivo de la capa de transporte es

- a. preparar la información para su transmisión y controlar el acceso a los medios físicos
- b. transportar datos entre dispositivos que no están conectados localmente en el mismo dominio de difusión,
- c. **Se encarga del transporte de los datos extremo a extremo (host origen a host destino)**
- d. Comunicar la única aplicación que se ejecuta en origen con todas las aplicaciones en destino

9. Los paquetes IPv4...

- a. **Se procesan en todos los dispositivos, si bien sólo se desencapsulan sólo en el destino**
- b. Se desencapsulan en todos los hosts, volviendo a encapsular si es necesario
- c. Es un protocolo orientado a conexión del tipo best-effort
- d. Llevan en su cabecera las direcciones de origen y destino del salto en cuestión

**10. La dirección IP 202.158.4.9 con máscara 255.255.255.239 ¿puede ser empleada en un host?
En caso negativo indicar por qué.**

Máscara imposible Maskara ezinezkoa da 255.255.255.11101111

11. La dirección IP 158.227.1.0/23 ...

- a. Es una dirección de clase B
- b. **Es una dirección sin clase**
- c. Es una dirección de (sub)red, y por tanto no puede asignarse a un host
- d. Es una dirección /24 subneteada

12. La dirección de broadcast...

- a. **Sólo es válida como dirección destino, y se puede emplear la dirección 255.255.255.255 si se quiere realizar a la red en la que se trabaja**
- b. Es asignable a un host
- c. Remota es 255.255.255.255
- d. en IPv6 es un caso especial de Anycast

13. El objetivo de la capa de red es

- a. Preparar la información para su transmisión y controlar el acceso a los medios físicos
- b. Transportar datos entre dispositivos que no están conectados localmente en el mismo dominio de difusión,**
- c. Se encarga del transporte de los datos extremo a extremo (host origen a host destino)
- d. Llevar la información al destino sin que pase por nodos intermedios

14. El protocolo de enrutamiento...

- a. IGP más conocido es el BGP
- b. EGP más conocido es el RIP
- c. Debe ser único para la comunicación interna en todo el AS**
- d. Pueden existir varios para la comunicación interna en un mismo AS

15. Los algoritmos de protocolos de enrutamiento

- a. *Distance vector* comunican a sus vecinos sólo el siguiente nodo por el que el paquete debe pasar, siendo uno de los más conocidos el Bellman-Ford**
- b. *Link state* no conocen la topología entera de la red
- c. *Path vector* sólo comunican los costes de la ruta

16. Las redes Tier 2...

- a. Forman el backbone de internet
- b. No emplean ruta por defecto
- c. Se conectan a uno o unos pocos Tier 1**
- d. No pueden interconectarse con otros Tier 2

17. Las conexiones Peering...

- a. Se realizan siempre a través de un enlace público IXP
- b. Son conexiones entre diferentes Tier y el proveedor publica todas las rutas de las que dispone
- c. Son conexiones para el tráfico sin coste entre operadores del mismo nivel y cada operador publica sólo sus rutas y no otras rutas que tenga con otros**
- d. Por definición, las redes Tier 1 son las únicas que no utilizan conexiones de peering.

18. En la técnica tunneling de IPv6

- a. Se encapsula un paquete IPv6 dentro de un paquete IPv4 para transferirse por una red basada en IPv4, y se transfiere así hasta el destino
- b. Se encapsula un paquete IPv6 dentro de un paquete IPv4 para transferirse por una red basada en IPv4, transfiriéndose el paquete IPv6 cuando la siguiente red es IPv6**
- c. Se traduce un paquete IPv6 a IPv4
- d. Se implementan ambos protocolos en los nodos

19. Calcular el bit de paridad cruzada de la siguiente trama:

1	0	1	0	0	0	0
1	0	0	0	0	0	1
1	0	0	0	1	1	1

Bit de paridad cruzada: **0**

20. La función de la capa de enlace es

- a. Se encarga del transporte de los datos extremo a extremo (host origen a host destino)
- b. Transportar datos entre dispositivos que no están conectados localmente en el mismo dominio de difusión,
- c. **preparar la información para su transmisión y controlar el acceso a los medios físicos**
- d. Conocer y gestionar la conexión con todos los dispositivos conectados en la red

(7.5p) Ejercicios

1. (2.5p) Un cliente (C) HTTPS solicita la descarga de una página HTML de 1200 bytes de un servidor web (S). Los tamaños de ventana de ambos se encuentran limitados (600 bytes para el servidor), el tamaño máximo de segmento (TMS) en ambos es de 300 bytes (no incluye la cabecera TCP). Representa el intercambio de segmentos entre cliente y servidor, sabiendo que:

- a) (1p) La solicitud de conexión se muestra en la siguiente trama. El número de secuencia inicial para el servidor es 4000.

```

0000  e0 0e e4 92 8d 90 00 e1 8c d7 11 f3 08 00 45 00 .....E.
0010  00 34 88 4b 40 00 80 06 e4 48 c0 a8 00 13 68 7e .4.K@....H....h~
0020  64 f6 d2 9e 01 bb 00 00 07 d0 00 00 00 00 80 02 d.....
0030  02 58 60 c8 00 00 02 04 05 b4 01 03 03 08 01 01 ..`.....
0040  04 02 ..
  
```

Nº secuencia = 00 00 07 d0 → 2000

Window = 02 58 → 600 bytes

- b) (1p) A continuación, el cliente envía la petición al servidor (300 bytes) y el servidor responde con la página HTML solicitada

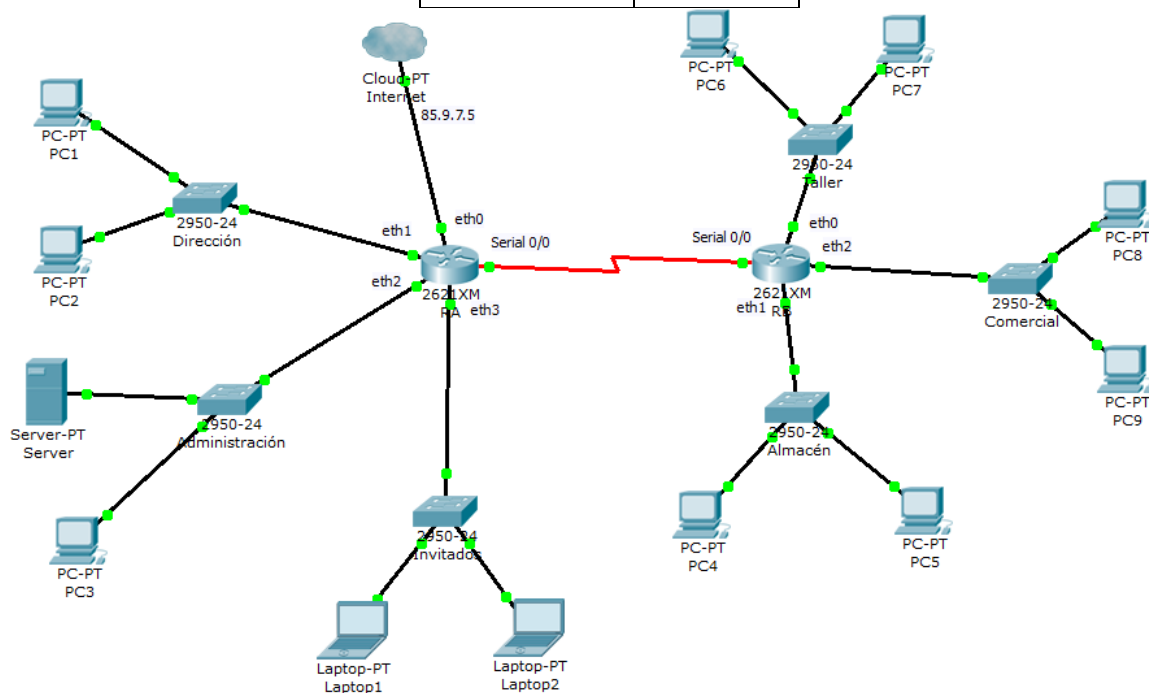
- c) (0.5p) Por último, el servidor solicita la desconexión

Sentido	Nº Secuencia	Nº ack	Código (Flags)	Datos	
C→S	2000	-	SYN	-	
S→C	4000	2001	SYN,ACK	-	TWH
C→S	2001	4001	ACK	-	
C→S	2001	4001	PSH, ACK	300	
S→C	4001	2301	ACK	300	
S→C	4301	2301	ACK	300	
C→S	2301	4601	ACK	-	Transferencia
S→C	4601	2301	ACK	300	
S→C	4901	2301	PSH, ACK	300	
C→S	2301	5201	ACK	-	
S→C	5201	2301	FIN, ACK	-	Desconexión

C→S	2301	5202	ACK	-
C→S	2301	5202	FIN, ACK	-
S→C	5202	2302	ACK	-

2. (3p) Una determinada empresa quiere establecer la red de trabajo a partir del bloque de direcciones en la que actualmente trabaja el servidor, con dirección 192.168.51.2/23. Las necesidades departamentales son las siguientes:

Red	Nº equipos
Dirección	12
Administración	12
Comercial	102
Taller	118
Almacén	31
Invitados	28



La empresa dispone de dos edificios, el primero con las oficinas de Dirección, Administración y sala de invitados; y el segundo con el departamento comercial, el taller y el almacén. Cada edificio dispone de un router, y estos se encuentran conectados mediante conexión Serial. El router que da servicio a la subred de Dirección dispone de salida a Internet. Se quiere mantener independiente el tráfico interno de cada uno de los departamentos.

NOTA: El número de equipos incluye el número de hosts y routers

NOTA 2: Las interfaces de los routers RA y RB de cada una de las subredes tienen como dirección IP las primeras direcciones disponibles de la red.

a) (0,5p) ¿Es posible direccionar la red mediante FLSM? Justificar la respuesta

No. El número de equipos en la subred de mayor tamaño supera el espacio disponible en la misma

6 subredes necesarias \rightarrow 3 bits de SubnetID \rightarrow 8 subredes disponibles

$32-23-3=6$ bits HostID $\rightarrow 2^6=64$ direcciones disponibles $< 118 + 2 =$ Direcciones Taller

b) (1p) Direccionar la red

b.1. (0,5p) Calculo direcciones Red

Dirección a subnetear (Red): Dirección IP & Subnet Mask

$192.168.51.2 \& 255.255.254.0 = 192.168.50.0$

Red	Nº equipos	Nº direcciones necesarias	Bits HostID
Dirección	12	14	4
Administración	12	14	4
Comercial	102	104	7
Taller	118	120	7
Almacén	31	33	6
Invitados	28	30	5
Enlace	2	4	2
Total		319	

$315 < 2^9 = 512$ En principio, es posible

Taller > Almacén > Invitados > Dirección > Administración

Taller / Comercial

SubnetID=Bits Totales-Mask-HostID= $32-23-7=2$

$192.168.0011001S.SHHHHHHH /23$

$.00110010.000000000 \rightarrow 192.168.50.0/25$ Taller

$.00110010.100000000 \rightarrow 192.168.50.128/25$ Comercial

$.00110011.000000000 \rightarrow 192.168.51.0/25$ Libre (a subnetear siguiente)

$.00110011.100000000 \rightarrow 192.168.51.128/25$ Libre

Almacén

SubnetID=Bits Totales-Mask-HostID= $32-25-6=1$

$192.168.00110011.0SHHHHHH /25$

$.00110011.000000000 \rightarrow 192.168.51.0/26$ Almacén

.00110011.01000000 → 192.168.51.64/26 Libre (a subnetear siguiente)

Invitados

SubnetID=Bits Totales-Mask-HostID=32-26-5=1

192.168.00110011.01SHHHHH /26

.00110011.01000000 → 192.168.51.64/27 Invitados

.00110011.01100000 → 192.168.51.96/27 Libre (a subnetear siguiente)

Dirección/Administración

SubnetID=Bits Totales-Mask-HostID=32-27-4=1

192.168.00110011.011SHHHH /27

.00110011.01100000 → 192.168.51.96/28 Dirección

.00110011.01110000 → 192.168.51.112/28 Administración

Enlace entre routers

SubnetID=Bits Totales-Mask-HostID=32-25-2=5

192.168.00110011.1SSSSSHH /25

.00110011.10000000 → 192.168.51.128/30 Enlace

b.2. (0,5p) Completar la tabla de direccionamiento

Red	Dir. Red	Dir. Broadcast	Rango IP asignable a HOST	Núm IPs asignables	Dir. Router	Primera IP asignada a HOST	Última IP asignada a HOST
Dirección	192.168.51.96/28	192.168.51.111/28	97-110	$2^4-2=14$.97	.98	.108
Administración	192.168.51.112/28	192.168.51.127/28	113-126	$2^4-2=14$.113	.114	.124
Comercial	192.168.50.128/25	192.168.50.255/25	129-254	$2^7-2=126$.129	.130	.230
Taller	192.168.50.0/25	192.168.50.127/25	1-126	$2^7-2=126$.1	.2	.118
Almacén	192.168.51.0/26	192.168.51.63/26	1-62	$2^4-6=62$.1	.2	.31
Invitados	192.168.51.64/27	192.168.51.95/28	65-94	$2^4-5=30$.65	.66	.92
Enlace	192.168.51.128/30	192.168.51.131/30	129-130	$2^2-2=2$.129 y .130	-	-

c) (1.5p) Completar la tabla de enrutamiento de ambos router

c.1. (0.75p) Tabla completa

Router A

Red	SM	GW	Interface	Metrica
0.0.0.0	/0	85.9.7.5	Eth0	-
51.64	/27	-	Eth3	0
51.96	/28	-	Eth1	0
51.112	/28	-	Eth2	0
51.128	/30	-	Serial0/0	0
50.0	/25	51.129 o 51.130	Serial0/0	1
50.128	/25	51.129 o 51.130	Serial0/0	1
51.0	/26	51.129 o 51.130	Serial0/0	1

Router B

Red	SM	GW	Interface	Metrica
0.0.0.0	/0	51.129 o 51.130	Serial0/0	-
50.0	/25	-	Eth0	0
50.128	/25	-	Eth2	0
51.0	/26	-	Eth1	0
51.128	/30	-	Serial0/0	0
51.64	/27	51.129 o 51.130	Serial0/0	1
51.96	/28	51.129 o 51.130	Serial0/0	1
51.112	/28	51.129 o 51.130	Serial0/0	1

c.2. (0.75p) Tabla mínima (con rutas sumarizadas)

Router A

Red	SM	GW	Interface	Metrica
0.0.0.0	/0	85.9.7.5	Eth0	-
51.64	/27	-	Eth3	0
51.96	/28	-	Eth1	0
51.112	/28	-	Eth2	0
51.128	/30	-	Serial0/0	0
50.0	/24	51.129 o 51.130	Serial0/0	1
51.0	/26	51.129 o 51.130	Serial0/0	1

Router B

Red	SM	GW	Interface	Metrica
0.0.0.0	/0	51.129 o 51.130	Serial0/0	-
50.0	/25	-	Eth0	0
50.128	/25	-	Eth2	0
51.0	/26	-	Eth1	0
51.128	/30	-	Serial0/0	0

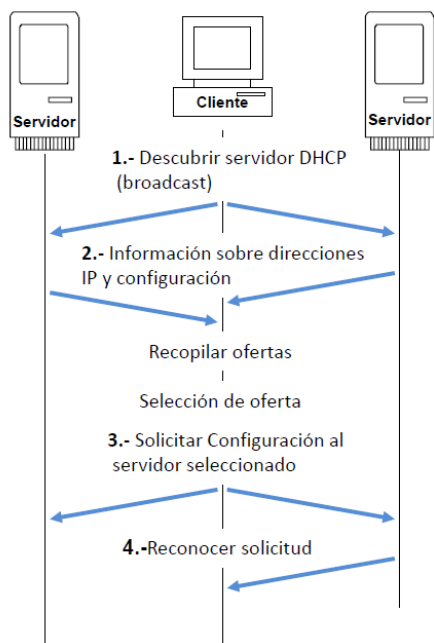
3. (1p) Si se conecta una red privada de clase C, con 1000 dispositivos que no operen a la vez, al router R con acceso a internet

a) ¿Qué protocolo se debe utilizar para el direccionamiento automático? Describir su funcionamiento y el proceso de asignación.

DHCP en Modo Automático



DIRECCIONES DINÁMICAS - DHCP



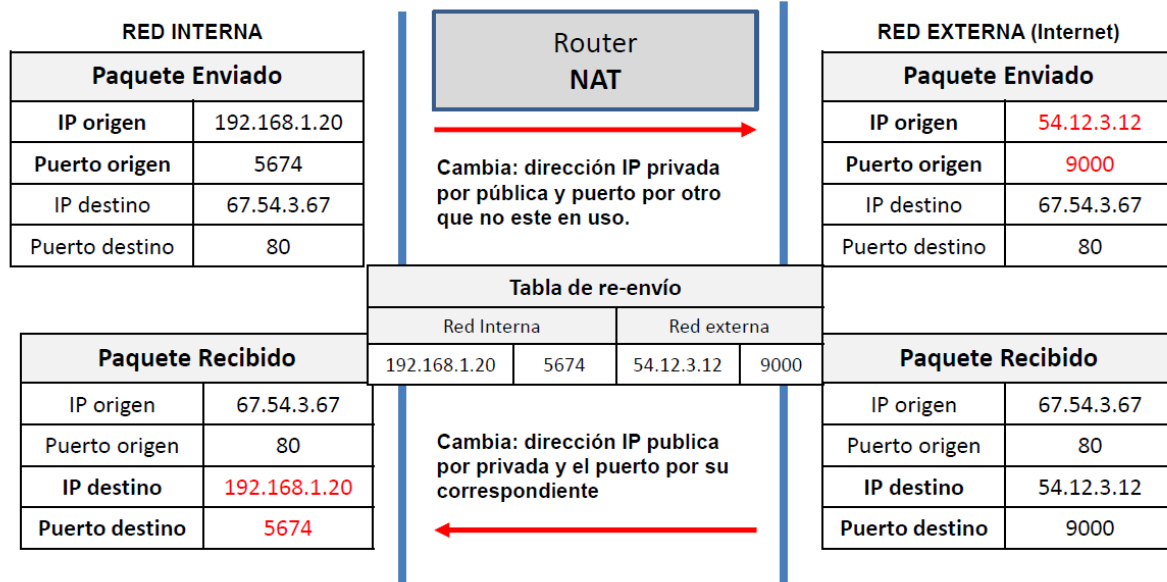
METODO DE ASIGNACION EN DHCP

- El cliente hace un **broadcast** de un mensaje **DHCP DISCOVER (1)** en su subred física.
- Cada servidor DHCP puede responder con un mensaje **DHCP OFFER (2)** que incluye una dirección de red disponible y otras opciones de configuración.
- El cliente **recibe** uno o más mensaje **DHCP OFFER** de uno o más servidores. Elige uno basándose en los parámetros de configuración ofertados y hace un **broadcast** de un mensaje **DHCP REQUEST** que incluye la opción identificadora del servidor para indicar qué mensaje ha seleccionado.
- Los servidores reciben el **broadcast** de **DHCP REQUEST (3)** del cliente. Los servidores no seleccionados utilizan el mensaje como notificación de que el cliente ha declinado su oferta.
- El servidor seleccionado responde con un mensaje **DHCP ACK(4)** que contiene los parámetros de configuración para el cliente.
- El cliente recibe el mensaje **DHCP ACK** con los parámetros de configuración. Si el cliente detecta un problema con los parámetros en el mensaje **DHCP ACK**, envía un mensaje **DHCP DECLINE** al servidor y reinicia el proceso de configuración.
- Puede elegir renunciar a su arrendamiento enviando un mensaje **DHCP PRELEASE** al servidor. El cliente especifica el arrendamiento al que renuncia incluyendo sus direcciones hardware y de red

b) ¿Qué protocolo se debe utilizar para la comunicación con Internet? Describirlo brevemente



DIRECCIONES TRADUCCIÓN DE DIRECCIONES NAT



Los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red. Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

4. (1p) En la red del ejercicio 2, un paquete de 5008 bytes (incluye cabecera IP mínima) se envía desde el ordenador con IP 192.168.50.100 con destino IP 192.168.51.100. Detallar:

Nota: Las direcciones MAC de los equipos se referenciarán como "MAC_{nombre_equipo, interface}", por ejemplo, la MAC del PCDirección será MAC_{PCDirección,eth0}.

- a) (0.25p) El camino seguido y el proceso de discriminación por cada dispositivo de la red con funcionalidad en la capa de red (sin cálculos, teóricamente)

Host Taller → RB → RA → Host Dirección

El host con IP 192.168.50.100 en la red Taller calculará la dirección red destino mediante un and lógico de la IP destino y su máscara, contrastará la IP de red destino con su tabla de enrutamiento, al no encontrarla la enviará a puerta de enlace (Router B).

Router B calculará la dirección red destino mediante un and lógico de la IP destino y su máscara, contrastará la IP de red destino con su tabla de enrutamiento, enviándolo por el camino por defecto a Router A.

Router A calculará la dirección red destino mediante un and lógico de la IP destino y su máscara, contrastará la IP de red destino con su tabla de enrutamiento, enviándolo directamente a Host Dirección.

LOS SWITCH NO TIENEN FUNCIONALIDAD EN LA CAPA DE RED

b) (0.25p) Las direcciones IP y MAC que aparecerán en las cabeceras en cada salto/segmento

Host Taller → RB → RA → Host Dirección

En el segmento de Host Taller:eth0 a RB:eth0

IP_{origen}: 192.168.50.100 MAC_{origen}: MAC_{PCDir,eth0}

IP_{destino}: 192.168.51.100 MAC_{destino}: MAC_{RB,eth0}

En el segmento de RB:serial0/0 a RA:serial0/0

IP_{origen}: 192.168.50.100 MAC_{origen}: MAC_{RB,serial0/0}

IP_{destino}: 192.168.51.100 MAC_{destino}: MAC_{RA,serial0/0}

En el segmento de RA:eth1 a Host Dirección:eth0

IP_{origen}: 192.168.50.100 MAC_{origen}: MAC_{RA,eth1}

IP_{destino}: 192.168.51.100 MAC_{destino}: MAC_{PCDir,eth0}

c) (0.5p) Cómo llega la información al destino (Suponer ID=1000, NF=0, MTU_{eth}=1500, MTU_{serial}=576)

5008-20=4088 bytes datos

En el segmento de Host Taller:eth0 a RB:eth0

MTU=1500=1480 bytes datos + 20 bytes cabecera → 1480/8=185

4088/1480 → 3 paquetes

Fragmento	ID	Flag NF	Flag MF	Desplazamiento	Longitud
1	1000	0	1	0	1480+20=1500
2	1000	0	1	1480/8=185	1480+20=1500
3	1000	0	0	2·1480/8=370	1480+20=1500
3	1000	0	0	3·1480/8=555	548+20=568

En el segmento de RB:serial0/0 a RA:serial0/0

MTU=576=556 bytes datos + 20 bytes cabecera → 556/8=69.5 (no entero) → 69·8=552 byte datos máximo

1480/556 → 3 paquetes

Fragmento	ID	Flag NF	Flag MF	Desplazamiento	Longitud
1	1000	0	1	0	$552+20=572$
2	1000	0	1	$552/8=69$	$552+20=572$
3	1000	0	1	$2 \cdot 552/8=138$	$376+20=396$

Fragmento	ID	Flag NF	Flag MF	Desplazamiento	Longitud
4	1000	0	1	$1480/8=185$	$552+20=572$
5	1000	0	1	$185+552/8=254$	$552+20=572$
6	1000	0	1	$254+552/8=323$	$376+20=396$

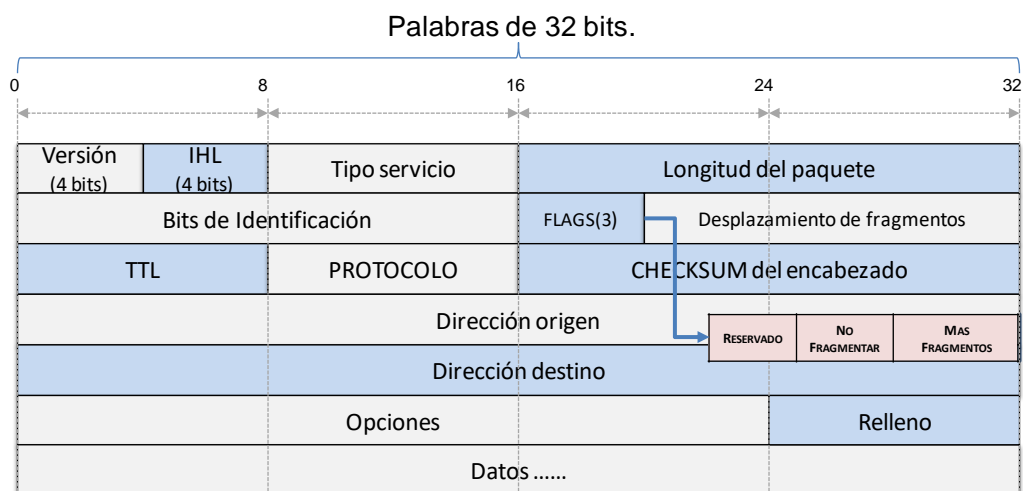
Fragmento	ID	Flag NF	Flag MF	Desplazamiento	Longitud
7	1000	0	1	$1480/8=370$	$552+20=572$
8	1000	0	1	$370+552/8=439$	$552+20=572$
9	1000	0	1	$439+552/8=508$	$376+20=396$

Fragmento	ID	Flag NF	Flag MF	Desplazamiento	Longitud
10	1000	0	1	$2 \cdot 1480/8=370$	$548+20=568$

- Formato de la trama Ethernet

Dirección Destino (6 bytes)	Dirección Origen (6 bytes)	Tipo (2 bytes)	Datos	CRC
--------------------------------	-------------------------------	-------------------	-------	-----

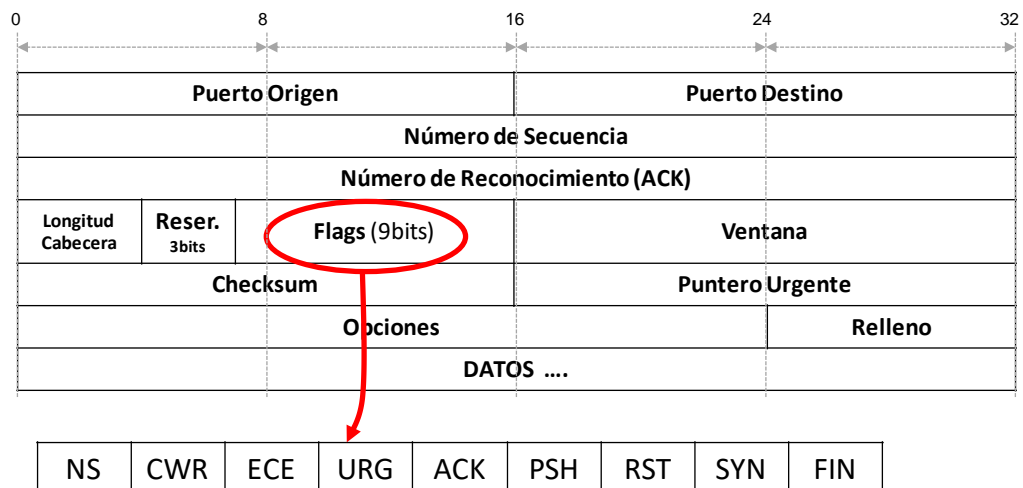
- Formato de la cabecera de IPv4



IHL: longitud de la cabecera en palabras de 32 bits

Longitud del paquete: longitud en bytes

- Formato de la cabecera TCP



- Formato de la cabecera UDP

