Arquitectura de redes I **Test de clase 1 de octubre de 2012 16:00 – 16:45**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

GRUPO: _____

Tiempo: Tres cuartos de hora
Sin libros ni apuntes
Calificación:
Respuesta correcta: +3
Respuesta errónea: -1

---

1. **¿Cuál de los siguientes campos NO se emplea en el proceso de demultiplexión?**
   a. El número de puerto de TCP o UDP.
   b. El número de protocolo de IP.
   c. El tipo de trama de Ethernet.
   d. La dirección de DNS del equipo.
2. **Se desea transmitir tráfico de datos por un cable tipo par trenzado. ¿Qué nivel es el encargado de corregir los errores de transmisión?**
   a. El nivel de red
   b. El nivel de sesión
   c. El nivel de enlace
   d. Ninguna de las anteriores.
3. **¿Qué se puede aseverar acerca de la dirección IP 150.256.56.1?**
   a. Se trata de un router.
   b. Se trata de un identificador de subred.
   c. Se trata de una dirección de broadcast de subred.
   d. No es una dirección válida.
4. **Al utilizar el comando tracert en un sistema se obtiene la siguiente salida:**

```
C:>tracert www.ii.uam.es
Tracing route to afrodita.ii.uam.es [150.244.56.51]
over a maximum of 30 hops:
1   *    *    *    Request timed out.
2   *    *    *    Request timed out.
3   *    *    *    Request timed out.
```

   Indicar cuál de las siguientes afirmaciones es cierta:

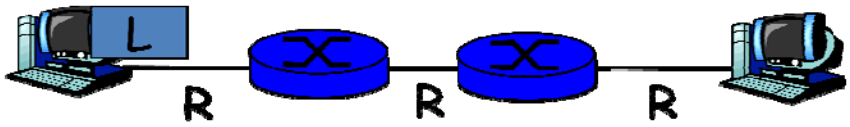
   a. La dirección del sistema www.ii.uam.es es 150.244.56.51
   b. Hay un problema en el sistema, el comando tracert no funciona
   c. Hay un error, se han confundido los nombres www y afrodita
   d. Ninguna de las anteriores
5. **Indicar cuál es el motivo por el que en el proceso de encapsulado, cada nivel de comunicaciones añade una cabecera**
   a. Para introducir la información del usuario
   b. Porque aumenta el ancho de banda
   c. Para enviar la información del protocolo
   d. Ninguna de las anteriores

6. **El correo electrónico (e-mail) es una aplicación basada en:**
    a. Arquitectura cliente/servidor
    b. Arquitectura P2P
    c. Arquitectura híbrida
    d. Ninguna de las anteriores
7. **La norma 802.11 b/g se refiere a:**
    a. Redes basada en coaxial
    b. Redes de área local tipo wireless
    c. Conexiones basadas en fibra óptica
    d. Ninguna de las anteriores
8. **¿Cómo consigue el comando *tracert* obtener los routers intermedios a un destino?**
    a. Mediante el acceso a una base de datos centralizada.
    b. Mediante el acceso a una base de datos distribuida.
    c. Mediante el aumento progresivo del TTL.
    d. Ninguna de las anteriores
9. **¿Qué medio físico es el más adecuado para transmitir a una velocidad de 100 Gbps?**
    a. Par trenzado
    b. Cable Coaxial .
    c. Fibra óptica .
    d. Ninguna de las anteriores.
10. **La característica fundamental de la conmutación de circuitos es:**
    a. Se usa para transmitir datos debido a que no tiene apenas “jitter”
    b. Reserva los recursos de comunicaciones durante el tiempo que dura la conexión
    c. El más económico que la conmutación de paquetes y más fiable
    d. Ninguna de las anteriores
11. **La multiplexación TDM utilizada en conmutación de circuitos consiste en:**

    a. Repartir el ancho de banda disponible modulando las señales con diferentes frecuencias
    b. Repartir la información en paquetes que se envían sucesivamente por el medio de transmisión
    c. Reservar frecuencias para transmitir canales de usuario en un medio de transmisión por radio
    d. Ninguna de las anteriores
12. **¿Cuánto se tarda transmitir un paquete completo de 640.000 bits (640k) si se utiliza una red basada en conmutación de circuitos si el ancho de banda de los enlaces es 1,536 Mbps (1536kbps), el enlace está compartido usando TDM con 24 ranuras/segundo y hace falta 500ms para establecer el circuito?**

    a. 10,5 s
    b. 10 s.
    c. 11 s
    d. Ninguna de las anteriores

13. **Se quiere transmitir un paquete de tamaño L = 1.000 bits (1kb) usando la red que se indica en la figura, cuyos enlaces tienen un ancho de banda de R=500 bps. ¿Cuánto se tarda en recibir el paquete completo en el destino, contando desde el momento en que se empieza a transmitir y despreciando los tiempos de propagación por los enlaces entre nodos?**



a. 4s.
b. 5s.
c. 6s.
d. Ninguna de las anteriores

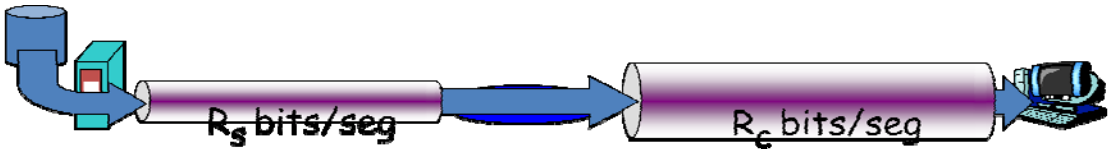
14. **En las redes de conmutación de paquetes, los nodos de conmutación tienen memoria dedicada a almacenar paquetes (colas). Indicar cuál es uno de los motivos para usar dicha memoria**

a. Almacenar el paquete entero antes de reenviarlo
b. Amentar el rendimiento de la red
c. Implantar los protocolos de comunicaciones
d. Ninguna de las anteriores

15. **Un medio de transmisión tiene una velocidad de propagación de 400.000 km/s ($4x10^8$ m/s) Indicar cuál de las siguientes afirmaciones es cierta.**

a. Es imposible que haya un medio de transmisión con esa velocidad de propagación.
b. Debe ser una fibra óptica monomodo para que tenga un ancho de banda tan alto
c. Debe ser un enlace en la parte troncal de una red de conmutación de circuitos
d. Ninguna de las anteriores.

16. **Se transmite información usando la red de la figura, en la que los anchos de banda instantáneos de los enlaces son diferentes $R_S < R_C$**



Indicar cuál es el ancho de banda medio extremo a extremo que se obtendría.

a. Como mucho R_C
b. Como mucho R_S
c. Un valor intermedio entre R_C y R_S
d. El producto de R_C y R_S

Arquitectura de redes I **Test de clase 30 de octubre de 2012 16:00 – 16:45**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

GRUPO: _____

Tiempo: Tres cuartos de hora
Sin libros ni apuntes
Calificación:
Respuesta correcta: +3
Respuesta errónea: -1

---

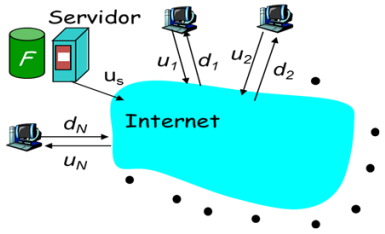
1. **Desde una máquina de la UAM se hace una consulta al servidor de nombres de la Universidad sobre la dirección www.google.com. ¿Cuántas preguntas DNS se mandarán desde el servidor de nombres de la UAM?**
   a) Mínimo 0 y máximo 2
   b) Mínimo 1 y máximo 2
   c) Mínimo 1 y máximo 3
   d) Mínimo 0 y máximo 3
2. **¿Qué protocolos se manejan desde la máquina de un usuario que está usando una aplicación webmail para procesar su correo electrónico desde un navegador web?**
   a) Necesariamente HTTP, SMTP y POP3
   b) Necesariamente HTTP y SMTP pero no POP3
   c) Necesariamente HTTP y POP3 pero no SMTP
   d) Necesariamente HTTP pero no SMTP ni POP3
3. **Se coloca un servidor de correo en cada una de las sedes en que se divide una empresa, con nombres smtp.administracion.empresa.es, smtp.delegacion.empresa.es, smtp.fabrica.empresa.es y smtp.almacen.empresa.es. En el DNS se configuran las siguientes entradas:**

   $ORIGIN administracion.empresa.es
   IN MX 10 smtp.administracion.empresa.es
   IN MX 20 smtp.delegacion.empresa.es

   $ORIGIN almacen.empresa.es
   IN MX 10 smtp.almacen.empresa.es
   IN MX 20 smtp.fabrica.empresa.es

   Si un usuario que tiene su cuenta de correo en smtp.administracion.empresa.es desea enviar un correo a encargado@almacen.empresa.es, se conectará por defecto a través de SMTP a:
   a) smtp.administracion.empresa.es
   b) smtp.almacen.empresa.es
   c) smtp.fabrica.empresa.es
   d) smtp.delegacion.empresa.es
4. **El diseño del protocolo Telnet se caracteriza porque los comandos y los datos se transmiten por la misma conexión TCP. En relación con las implicaciones de dicho diseño, indicar cuál de las siguientes afirmaciones es cierta:**
   a) La transmisión de comandos y datos por la misma conexión puede provocar confusiones entre ambos en caso de error
   b) La consecuencia de dicho diseño es que telnet sólo funciona en sistemas monoprocesador
   c) La consecuencia de este diseño es que el sistema operativo tiene que utilizar la tabla de procesos para distinguir el destino de los datagramas
   d) La ventaja fundamental de esta aproximación es que las cabeceras de los datagramas de TCP pueden ser mucho más pequeñas.
5. **En una sesión FTP, la conexión de control se abre**
   a) Exactamente una vez
   b) Exactamente dos veces
   c) Tantas como descargas se realicen
   d) Ninguna de las anteriores
6. **En SMTP, ¿qué comando identifica el ordenador cliente?**
   a) HELO
   b) MAIL FROM
   c) RCPT TO
   d) SEND FROM
7. **Indicar cuál de las siguientes afirmaciones es cierta con respecto a los tres componentes de un mensaje SMTP: Envoltorio, cabeceras y cuerpo**
   a) El envoltorio y las cabeceras no tiene que cumplir ninguna norma especial, cada agente de transferencia de mensajes puede utilizar el formato que quiera, siempre que los datos estén en ASCII
   b) El envoltorio consiste en los comandos que intercambian los agentes de transferencia de mensajes, por lo que es imprescindible que éstos sigan el estándar SMTP
   c) Las cabeceras de los mensajes sirven para completar la información del envoltorio cuando se producen errores
   d) Las cabeceras de los mensajes sirven para intercambiar información entre el agente de transferencia de mensajes de un sistema y el agente de usuario de otro sistema

8. **El campo de cabecera Last-Modified de HTTP:**
   a) Lo envía el cliente al servidor para pedir las actualizaciones de una página respecto a una fecha
   b) Lo envía el servidor al cliente para que éste la incluya en su caché y evite posteriores descargas si no se ha modificado la página
   c) Sólo se utiliza en sistemas Proxy-Caché
   d) Lo envía el servidor al cliente sólo cuando el cliente incluye el campo de cabecera If-Modified-Since
9. **La llamada accept() del API de sockets (BSD) se utiliza para:**
   a) Que un servidor (típicamente) saque una petición de conexión de la cola y cree un nuevo socket
   b) Indicar que el API ha aceptado a una aplicación y ésta puede utilizar las llamadas BSD
   c) Que un cliente envía un segmento de SYN a un servidor
   d) Ninguna de las anteriores
10. **El campo OPCODE de la cabecera DNS sirve:**
   a) Para indicar qué opciones hay que utilizar
   b) Para distinguir entre preguntas directas e inversas
   c) Relleno de bytes. Su uso es opcional
   d) Ninguna de las anteriores
11. **Se pretende estimar cuál es el tiempo necesario para distribuir un fichero F de longitud de 10MB desde un servidor conectado a Internet a cien (100) clientes utilizando un protocolo P2P sobre una arquitectura tal como se muestra en la figura:**



Los datos de la capacidad de los enlaces son:
us = 1Gbps
ui = 1Mbps
di = 10 Mbps
El tiempo estimado de distribución completa del fichero será:
   a) 0,09 segundos
   b) 0,73 segundos
   c) 0,8 segundos
   d) Ninguna de las anteriores
12. **A la hora de implementar un servidor de FTP, lo más adecuado es emplear:**
   a) Datagram sockets con programación secuencial.
   b) Datagram sockets con programación concurrente.
   c) Stream sockets con programación secuencial.
   d) Stream sockets con programación concurrente.
13. **¿Cuál es la secuencia típica de llamadas al API de sockets en la inicialización de un servidor TCP?**
   a) socket – listen – bind – accept
   b) socket – bind – listen – accept
   c) socket – bind – listen – connect
   d) socket – listen – bind – close

14. **Un sistema quiere hacer una pregunta DNS inversa para saber el nombre de un sistema cuya dirección IP es 150.244.28.254. Para ello, envía un paquete DNS con una pregunta PTR con el nombre:**
   a) 150.244.28.254.in-addr.arpa
   b) 150.244.28.254.PTR.in-addr.arpa
   c) 150.244.28.254.in-arrd.PTR
   d) Ninguna de las anteriores

15. **En el FQDN www.eps.uam.es, ¿cuál es el dominio de nivel superior (TLD)?**
   a) es
   b) uam
   c) eps
   d) www
16. **En una empresa se detecta que las descargas desde un servidor externo de páginas web tienen un tiempo de transmisión de diez (10) segundos. Para reducirlo, se instala un proxy desde el que las descargas tardan un (1) segundo. Para comprobar la efectividad, se muestrean un total de 415 descargas, de las cuales 395 son desde el proxy. ¿Cuál es el tiempo medio de descarga de la muestra en segundos?**
   a) 9,56
   b) 1,43
   c) 11
   d) Ninguna de las anteriores

Arquitectura de redes I **Test de clase 27 de noviembre de 2012 16:10 – 16:55**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

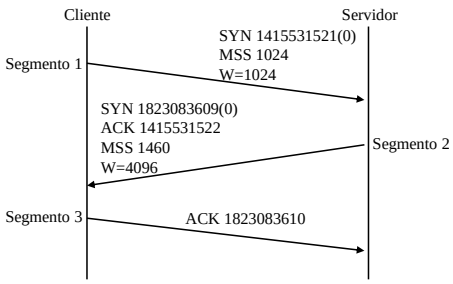
GRUPO: _____

Tiempo: Tres cuartos de hora
Sin libros ni apuntes
Calificación:
Respuesta correcta: +3
Respuesta errónea: -1

---

1. **Se tiene una conexión a Internet a 20Mbps. Si el RTT estimado es de 250 ms y la ventana ofrecida por el otro extremo es de 17.520 ¿Cuál será aproximadamente la velocidad media a la que se puede transmitir en estas condiciones?**
   a) 53,9 kbps
   b) 17,5 kbps
   c) 20 Mbps
   d) Ninguna de las anteriores
2. **El nivel TCP de un sistema conectado a Internet recibe un paquete TCP con el *flag* SYN activado. ¿En qué estado se encuentra inmediatamente después de recibirlo?**
   a) TIME_WAIT
   b) SYN_SENT
   c) No se puede saber con exactitud
   d) Ninguna de las anteriores
3. **Un sistema recibe un paquete UDP y comprueba que el *checksum* es correcto. Esto implica:**
   a) Que es seguro que no ha habido errores de transmisión
   b) Que es seguro que si hay errores de transmisión, no afectan a los datos
   c) Que es seguro que en la cabecera no hay errores
   d) Ninguna de las anteriores
4. **Se recibe un segmento TCP con la siguiente información: ack=100, Window=23.400, Seq= 345 el sistema que lo recibe envía un paquete con Seq= 23.100, len=400. Indicar cuál de las siguientes afirmaciones es cierta en relación con este segundo segmento:**
   a) El segmento es erróneo al no cumplir la ventana ofrecida
   b) El segmento es correcto al cumplir la ventana ofrecida
   c) Hace falta más información para saber si el segmento es correcto o no
   d) Ninguna de las anteriores
5. **Un sistema tiene como valor estimado de RTT *EstimatedRTT* = 200ms. En un determinado momento recibe un segmento de asentimiento y mide el valor del RTT como *SampleRTT*= 123ms. Si está utilizando la estimación basada en la media con el valor típico de α indicar cuál es la nueva estimación del valor del RTT:**
   a) 200 ms
   b) 123 ms
   c) 223 ms
   d) Ninguna de las anteriores

6. **Dado el siguiente intercambio de segmentos TCP, indicar cuál sería el número de secuencia del primer segmento enviado desde el servidor al cliente:**



a) 1823083609
b) 1415531521
c) 1415531522
d) Ninguna de las anteriores

7. **Un sistema recibe tres segmentos seguidos con el mismo número de asentimiento. Indicar cuál de las siguientes afirmaciones es cierta:**
   a) Es seguro que se trata de una petición de retransmisión de un segmento (*fast retransmit*)
   b) Depende del resto de información de los segmentos en que sea un *fast retransmit* o no
   c) Es la indicación de que hay que reenviar inmediatamente el último segmento enviado
   d) Ninguna de las anteriores
8. **El arranque lento de TCP consiste en:**
   a) Se comienza con una ventana de congestión de valor igual al *threshold* y se va incrementando linealmente
   b) Se comienza con una ventana de congestión grande y se va disminuyendo si se pierden paquetes
   c) Se comienza con una ventana de congestión igual a uno y se incrementa exponencialmente
   d) Ninguna de las anteriores

CAPTURA: Las siguientes cuestiones se refieren a la Captura adjunta

9. **¿A qué se debe que la ventana ofrecida en la trama 30 sea de 32.841?**
   a) A que el servidor se ha quedado sin memoria e indica al cliente que no envíe más paquetes
   b) A que el cliente ha enviado un paquete de tamaño mayor que el MSS y se tarda cierto tiempo en procesarlo
   c) A que el servidor indica que se han consumido 739 bytes de la ventana previa
   d) Ninguna de las anteriores
10. **¿Qué valor debe tener LONGITUD en la trama 31?**
   a) 776
   b) 777
   c) 740
   d) Ninguna de las anteriores
11. **Se sabe que se ha enviado un comando GET. Indicar en qué trama debería estar dicho comando**
   a) 30
   b) 31
   c) 32
   d) Ninguna de las anteriores
12. **Indicar cuál es el valor de ASENTIMIENTO en la trama 33**
   a) 741
   b) 777
   c) 778
   d) Ninguna de las anteriores
13. **Después de enviar la trama 32, el servidor queda en el estado:**
   a) FIN_SENT
   b) FIN_WAIT_1
   c) COLSING
   d) Ninguna de las anteriores
14. **¿Cuántos flujos hay capturados en la trama?**
   a) uno
   b) dos
   c) Hace falta más información
   d) Ninguna de las anteriores
15. **¿Qué valor tiene LONGITUD DE CABECERA en la trama 26?**
   a) 20
   b) 32
   c) 24
   d) Ninguna de las anteriores
16. **¿Cuál es el valor de MSS solicitado por el servidor?**
   a) 8.192
   b) 49.682
   c) No está reflejado en la traza
   d) Ninguna de las anteriores

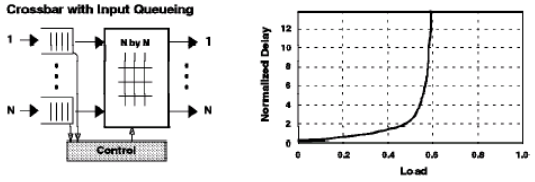
Arquitectura de redes I **Test de clase 18 de diciembre de 2012 16:15 – 17:00**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

GRUPO: _____

Tiempo: Tres cuartos de hora
Sin libros ni apuntes
Calificación:
Respuesta correcta: +3
Respuesta errónea: -1

---

1. **El servicio CBR de ATM se caracteriza por:**
   a) Ofrecer un tasa de bit constante y garantizar temporización
   b) Ofrecer un tasa de bit contante pero sin garantizar temporización
   c) Ofrecer una tasa de bit variable garantizando la temporización
   d) Ninguna de las anteriores
2. **En el esquema siguiente se presenta la arquitectura de un nodo de conmutación y su comportamiento con respecto a la carga de entrada. En la escala de la gráfica 1.0 es la capacidad máxima de conmutación del *Crossbar*.**



Indicar cuál de las siguientes afirmaciones es cierta:
   a) Es un claro ejemplo de saturación de un *Crossbar* debido a que la complejidad es $O(n^2)$
   b) El sistema de control está colapsado debido al exceso de carga
   c) La gráfica representa un ejemplo del efecto del HOL en el rendimiento
   d) Ninguna de las anteriores
3. **El campo de 16 bits de identificación de la cabecera IP tiene como propósito:**
   a) Ordenar los datagramas en el destino o en un *router* intermedio
   b) Detectar pérdidas de datagramas en el destino
   c) Comprobar que los datagramas forman parte de un flujo
   d) Ninguna de las anteriores
4. **El campo *Time to Live* (TTL) de la cabecera IP se mide en:**
   a) Segundos
   b) Décimas de segundos
   c) Milisegundos
   d) Ninguna de las anteriores
5. **El nivel IP de un sistema debe reencaminar datagramas que tiene 1490 Bytes de datos por un medio físico con una MTU de 1500 Bytes. Considerar que la cabecera IP no tiene opciones. La probabilidad de que un datagrama llegue al destino es de un 90%. Indicar cuál es la probabilidad de que lleguen correctamente tres datagramas como el descrito:**
   a) 72,9%
   b) 90%
   c) 53,1%
   d) Ninguna de las anteriores
6. **En un sistema se ejecuta el comando *netstat –r* y se obtiene la siguiente tabla de rutas:**

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	16.23.140.1	16.23.140.138	20
16.23.132.0	255.255.252.0	On-link	16.23.132.139	276
16.23.132.139	255.255.255.255	On-link	16.23.132.139	276
16.23.135.255	255.255.255.255	On-link	16.23.132.139	276
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	16.23.132.139	276
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	16.23.132.139	276

Se recibe un datagrama con dirección de destino 16.23.133.4 Indicar por qué interfaz se envía:
   a) 16.23.140.138
   b) 16.23.132.139
   c) 127.0.0.1
   d) Ninguna de las anteriores

7. **Siguiendo con el ejercicio anterior, se recibe ahora un datagrama con dirección de destino 15.23.132.139. Indican por cuál de las interfaces se envía:**
   a) 16.23.140.138
   b) 16.23.132.139
   c) 127.0.0.1
   d) Ninguna de las anteriores

8. **Se tienen un sistema cuya dirección de red es 10.15.155.32 /19 La dirección 10.15.129.7/19**
   a) Pertenece a la misma red y subred
   b) Pertenece a otra red y/o subred
   c) No puede saberse si pertenece a la misma red y subred
   d) Ninguna de las anteriores

9. **Indicar cuál es el motivo por el que en los mensajes de DHCP es necesario incluir un *transaction ID:***
   a) Por motivos de contabilidad
   b) Para utilizar TCP
   c) Para relacionar preguntas y respuestas
   d) Ninguna de las anteriores

10. **Un *router* que usa NAT tiene la siguiente tabla de traducción de direcciones:**

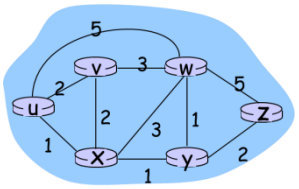
NAT translation table	
WAN side addr	**LAN side addr**
138.76.29.7, 5001	**10.0.0.1, 3345**

Indicar cuál de las siguientes afirmaciones es cierta:
   a) Los paquetes que se envían hacia Internet tienen como dirección de destino 138.76.29.7 y puerto destino 5001
   b) Los paquetes que se envían hacia Internet tienen como dirección de destiño 10.0.0.1 y puerto destino 3345
   c) Los paquetes que se reciben desde internet tienen como dirección origen 138.76.29.7 y puerto origen 5001
   d) Ninguna de las anteriores

11. **La versión 6 de IP (IPv6) supone varias modificaciones respecto a la versión 4 (IPv4) Indicar cuál de las siguientes afirmaciones es cierta:**
   a) No se pueden encapsular paquetes IPv6 dentro de paquetes IPv4
   b) El rango de direcciones IPv6 es mayor que el rango de direcciones de IPv4
   c) IPv6 no soporta el concepto de *multicast*
   d) Ninguna de las anteriores

12. **Para poder aplicar el algoritmo de Dijkstra en un *router* es necesario:**
   a) Usar previamente el algoritmo Vector Distancia
   b) Esperar un tiempo a que los costes de los enlaces no varíen
   c) Tener la descripción completa de la topología de la red
   d) Ninguna de las anteriores

13. **Se aplica el algoritmo de Dijkstra en el nodo z de la red cuya topología se indica en la figura:**



Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(u),p(u)
0	z	∞	5,z	∞	2,z	∞
1	zy	XX	3,y	3,y		∞

La tabla describe el paso 1 del algoritmo. Indicar el valor de XX:
   a) 8,w
   b) 5,y
   c) ∞
   d) Ninguna de las anteriores

14. **Siguiendo con la pregunta anterior, ¿Cuál sería el siguiente nodo en incluirse en el conjunto N' ?**
   a) El nodo v
   b) El nodo u
   c) El nodo y
   d) Ninguna de las anteriores

15. **Indicar cuál es la utilidad del mecanismo de "poisoned reverse":**
   a) Permite que un nodo indique a otro que se cambie el algoritmo al de estado de enlace en la red
   b) Permite evitar una situación "cuenta al infinito" cuando hay un cambio en la métrica de un enlace.
   c) Permite identificar que se ha entrado en el estado de "cuenta al infinito" con lo que debe esperarse tiempos muy largos de convergencia.
   d) Ninguna de las anteriores.

16. **Si se requiere considerar varias rutas a un destino se deberá utilizar**
   a) OSPF
   b) RIP
   c) Cualquiera de los dos, RIP o OSPF lo soportan
   d) Ninguna de las anteriores

Arquitectura de redes I Modelo 1 Examen Final 12 de Enero de 2013 10:00

APELLIDOS (MAYÚSCULAS)_____

NOMBRE (MAYÚSCULAS): _____

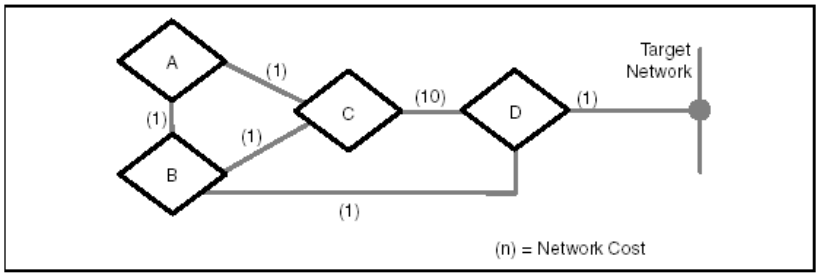
GRUPO: _____

Tiempo: Dos horas
Sin libros ni apuntes, 36 preguntas.
Calificación: todas las preguntas tienen el mismo peso en la nota:
Respuesta correcta: +3
Respuesta errónea: -1
El alumno entregará el examen junto con la hoja de lectura óptica.

CUESTIONES

1. **¿En qué red se encuentra es sistema con dirección IP 16.120.34.7 si la máscara de red es 255.255.240.0?**
   a) 16.120.32.7
   b) 16.120.32.0
   c) 16.120.34.0
   d) Ninguna de las anteriores
2. **¿Qué campo de la cabecera IP refleja el instante de tiempo en que se creó el datagrama?**
   a) Longitud de la cabecera.
   b) Longitud del datagrama.
   c) TTL.
   d) Ninguna de las anteriores
3. **¿Cuál de los siguientes valores de DF y MF indican que el datagrama está fragmentado?**
   a) DF=0, MF=1.
   b) DF=1, MF=0.
   c) DF=0, MF=0.
   d) Ninguna de las anteriores
4. **Los mensajes de error de ICMP se caracterizan por:**
   a) Siempre llegan al destino al ser mensajes de error.
   b) Son interpretados por todos los *routers* que los redirigen al destino
   c) Son respondidos siempre por el sistema que los recibe
   d) Ninguna de las anteriores
5. **¿Cuál de las siguientes afirmaciones es correcta respecto de algoritmos de encaminamiento?**
   a) El algoritmo de vector distancia se basa en el algoritmo de Dijkstra
   b) En estado de enlaces es importante evitar el conteo al infinito.
   c) En vector de distancia se usa la técnica de inundación.
   d) Ninguna de las anteriores.
6. **Respecto de los protocolos de encaminamiento existentes:**
   a) BGP tiene el problema de cuenta al infinito.
   b) RIP tiene el problema de cuenta al infinito
   c) OSPF tiene el problema de cuenta al infinito.
   d) Ninguna de las anteriores.
7. **¿Por qué UDP es más eficiente que TCP?**
   a) Porque UDP no es orientado a conexión.
   b) Porque TCP tiene un tamaño de paquete mayor
   c) Porque el checksum es opcional.
   d) Ninguna de las anteriores
8. **¿Cuánto vale el número de secuencia inicial o ISN de UDP?**
   a) Siempre 0.
   b) Siempre 1.
   c) Un valor aleatorio.
   d) Ninguna de las anteriores
9. **¿Cuál de los siguientes mecanismos de TCP está pensado para evitar que un emisor rápido desborde a los routers de la red?**
   a) La ventana de congestión.
   b) La ventana del receptor.
   c) La recuperación rápida.
   d) Ninguna de las anteriores

10. **¿Cuál de los siguientes temporizadores de TCP es el que se emplea para asegurar que la red queda limpia de segmentos antes de iniciar la siguiente conexión?**
    a) 2MLS.
    b) RTO.
    c) Persist.
    d) Ninguna de las anteriores
11. **¿Cuántas conexiones TCP se abren en una sesión FTP:**
    a) Una como máximo
    b) Dos como mínimo
    c) Exactamente dos
    d) Ninguna de las anteriores
12. **¿Cuál de las siguientes afirmaciones de HTTP es falsa?**
    a) HTTP utiliza cabeceras MIME para indicar el tipo de archivo que se descarga.
    b) HTTP implementa cabeceras que facilitan la cache de archivos.
    c) HTTP utiliza URLs para identificar archivos en la red.
    d) HTTP utiliza una conexión de control y otra distinta para la de descarga de archivos.
13. **¿Qué máscara es necesario utilizar para que los sistemas con direcciones IP 172.16.0.0 a 172.31.255.255 estén en la misma red?**
    a) 255.192.0.0
    b) 255.224.0.0
    c) 255.240.0.0
    d) Ninguna de las anteriores
14. **Un ordenador envía un datagrama UDP por una ruta con alta tasa de errores. Si en un punto de la ruta el datagrama sufre errores que afectan a los datos (suponer que el datagrama no se descarta por congestión en la red):**
    a) El destino descartará el datagrama UDP en cualquier caso.
    b) El destino descartará el datagrama sólo si el checksum de UDP es distinto de cero.
    c) El datagrama será descartado por el router dónde se produzca el error.
    d) Ninguna de las anteriores
15. **En un sistema se tiene un servidor iterativo que utiliza el protocolo udp y el puerto 85 y que está recibiendo datagramas de un cliente que se ejecuta en un sistema remoto y que utiliza el puerto 10340. Indicar cuál de las siguientes afirmaciones es cierta:**
    a) El servidor iterativo solo puede esperar datagramas que lleguen a una y solo una dirección de destino
    b) El servidor iterativo tiene que utilizar un puerto cuyo identificador sea menor que 100
    c) El cliente no puede asumir fiabilidad en la transmisión de los paquetes UDP hacia el servidor
    d) Ninguna de las anteriores
16. **El servidor SMTP del dominio eps.uam.es recibe de un cliente de correo electrónico interno de la Escuela un mensaje dirigido a e12345@estudiante.uam.es. Para reenviarlo a su destino, necesitará obtener del DNS:**
    a) El RR de tipo A del nombre de dominio estudiante.uam.es
    b) El RR de tipo MX del nombre de dominio estudiante.uam.es
    c) El RR de tipo MX del nombre de dominio eps.uam.es
    d) Ninguna de las anteriores
17. **Se tiene la siguiente topología de routers en la cual se quiere utilizar el algoritmo del vector distancia para hacer converger las tablas de enrutamiento:**



En un momento dado, el enlace entre el router B y el D falla. Cuando el router B se da cuenta, empieza a enviar mensajes utilizando el algoritmo mencionado. La siguiente tabla refleja esquemáticamente la información que tienen los routers A, B, C y D sobre la distancia que tiene la ruta para alcanzar la red "Target Network".

Time													
D:	Direct	1	Direct	1	Direct	1	Direct	1	....	Direct	1	Direct	1
B:	Unreachable		C	4	C	5	C	6		C	11	C	12
C:	B	3	A	4	A	5	A	6		A	11	D	11
A:	B	3	C	4	C	5	C	6	....	C	11	C	12

Indicar cuál de las siguientes afirmaciones es cierta:

a) El algoritmo basado en el vector distancia no puede tener este comportamiento, hay algún error
b) Es un ejemplo de que "las buenas noticias vuelan"
c) Es un ejemplo de que "las malas noticias van despacio"
d) Ninguna de las anteriores

18. Los routers utilizan habitualmente un algoritmo denominado Random Early Detect (RED) para mejorar el comportamiento frente a situaciones de congestión en una red IP. Dicho algoritmo se basa en que cuando la ocupación de la cola de salida de un router supera un determinado umbral (inferior a la ocupación máxima), el router descarta aleatoriamente paquetes. Con esto se consigue:

a) Que los sistemas finales reduzcan su ritmo de envío, al reducirse el tamaño de la ventana de congestión CWD por detectarse la pérdida de un segmento.
b) Que los sistemas finales se envíen mensajes ICMP para que reduzcan su velocidad de transferencia.
c) Que los sistemas finales busquen una ruta alternativa que pierda menos paquetes.
d) Ninguna de las anteriores

19. La pila TCP de un servidor tiene una conexión en estado LISTEN en el puerto 23. La conexión pasará al estado SYN_RCVD tras recibir un segmento con los siguientes valores:

a) SYN=1, ACK=1, puerto origen=23, puerto destino= 1234.
b) SYN=1, ACK=0, puerto origen=1234, puerto destino= 23.
c) SYN=1, ACK=0, puerto origen=23, puerto destino 1234.
d) Ninguna de las anteriores

20. Un sistema cliente se conecta a un servidor remoto utilizando TCP/IP para descargar un fichero de 10Mbytes. La velocidad neta que se obtiene es de 1.0 Kbytes/segundo. Para obtener mayor eficiencia, se duplica la ventana ofrecida por el nivel TCP en el sistema cliente sin cambiar ningún otro parámetro y la velocidad que se obtiene es de 1.2 Kbytes/segundo. Indicar cuál de las siguientes afirmaciones es cierta:

a) Es imposible el resultado anterior, al duplicar la ventana debería duplicarse aproximadamente la velocidad neta
b) El tamaño de la ventana no tiene nada que ver con la velocidad neta de transmisión, por lo que no puede tener influencia nunca en la velocidad de transmisión
c) El comportamiento se explica porque al aumentar el tamaño de ventana, ésta ha dejado de ser un freno para utilizar toda la capacidad de la pipa y por tanto se ha alcanzado la máxima velocidad neta
d) Ninguna de las anteriores

21. El campo de cabecera Last-Modified de HTTP:

a) Lo envía el cliente al servidor para pedir las actualizaciones de una página respecto a una fecha.
b) Lo envía el servidor al cliente para que éste la incluya en su caché y evite posteriores descargas si no se ha modificado la página.
c) Lo envía el servidor al cliente sólo cuando el cliente incluye el campo de cabecera If-Modified-Since.
d) Ninguna de las anteriores

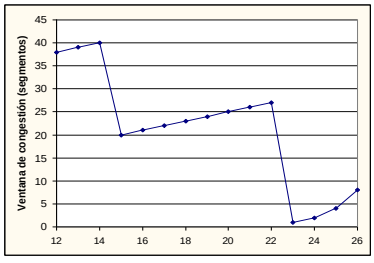
22. El motivo de usar un campo de tiempo de vida (TTL) en la cabecera IP v4 es:

a) Para llevar control del tiempo que tarda en llegar un datagrama al destino
b) Para informar al temporizador Keepalive
c) Para evitar que un datagrama se quede en un bucle de reencaminamientos infinito
d) Ninguna de las anteriores

23. El campo OPCODE de la cabecera DNS sirve:

a) Para indica qué opciones hay que utilizar
b) Para distinguir entre preguntas directas e inversas
c) Relleno de bytes. Su uso es opcional
d) Ninguna de las anteriores

24. La figura representa el tamaño de la ventana de congestión (CWD) de una conexión TCP en función del tiempo:



En el instante 22, la pila TCP del emisor detecta la pérdida de un segmento debido probablemente a:

a) Se ha cumplido el tiempo RTO en la recepción de ACK
b) Recepción de un segmento fuera de secuencia
c) Se ha cumplido el tiempo 2MSL en la recepción de ACK
d) Ninguna de las anteriores

TRAZA Responder a las siguientes preguntas referidas a la TRAZA del apéndice.

25. ¿En qué subred se encuentra el servidor de FTP? (suponer el valor de la máscara /16)

a) En una subred de la misma organización distinta a la subred del cliente.
b) En una subred de otra organización.
c) Con los datos aportados no puede saberse.
d) Ninguna de las anteriores

26. ¿Cuántas conexiones TCP hay establecidas al enviarse la trama 6?

a) una
b) dos
c) No puede saberse
d) Ninguna de las anteriores

27. ¿Cuál de los siguientes servidores no proporcionaría una respuesta autorizada para el dominio ii.uam.es?

a) chico.rediris.es
b) ns.uam.es
c) ns0.uam.es
d) Ninguna de las anteriores

28. ¿Por qué en la trama 8 se asiente con el número 1?

a) Porque siempre se asiente sumando 1 al número de secuencia recibido.
b) Porque el segmento anterior llevaba un byte de datos.
c) Se trata de un error al decodificar el segmento, puesto que el asentimiento debería ser 0.
d) Ninguna de las anteriores

29. ¿En qué estado se encuentra la conexión TCP en el servidor tras la trama 8?

a) SYN_RCVD
b) SYN_SENT
c) ESTABLISHED
d) Ninguna de las anteriores

30. ¿Qué mecanismo de representación se utiliza para enviar los datos en respuesta a la solicitud de la trama 25?

a) EBCDIC.
b) HTML.
c) Binario (Image).
d) Ninguna de las anteriores.

31. ¿Qué valor tiene el número de puerto descrito en la captura como "PUERTO" (trama 26)?

a) 1141
b) 4121
c) 30980
d) Ninguna de las anteriores

32. ¿Qué valor debe tener el número de secuencia "SECUENCIA" (tramas 28, 29)?

a) 273
b) 272
c) 46
d) Ninguna de las anteriores

33. ¿De qué tipo son los mensajes de las tramas 29 y 31?

a) Comando realizado.
b) Errores pasajeros.
c) Errores permanentes.
d) Ninguna de las anteriores

34. ¿Por qué no se establece la conexión de datos correctamente?

a) El cliente debe tener activado un mecanismo de filtrado de paquetes (cortafuegos) y no admite conexiones entrantes.
b) El cliente se encuentra detrás de un router que hace NAT, con lo que la conexión entrante se dirige a un socket que no está disponible.
c) El servidor se encuentra detrás de un router que hace NAPT, y la conexión saliente no se corresponde con ningún puerto registrado.
d) Ninguna de las anteriores

35. ¿Cuál de las siguientes alternativas solucionaría el problema en cualquier sesión posterior de FTP?

a) Utilizar el comando PASV por parte del cliente.
b) Registrar el puerto 20 en el router que hace NAPT.
c) Admitir conexiones salientes del puerto 20 del servidor.
d) Admitir conexiones entrantes al mismo puerto número: "PUERTO" (trama 26) en el cliente.

36. ¿Para qué envía el servidor un segmento de reset (trama 32)?

a) Es para cerrar la conexión de control que permanecía abierta y sin actividad del cliente.
b) Es para provocar un asentimiento del cliente, siguiendo el algoritmo de keepalive.
c) Es para cerrar la conexión de datos que se abrió de forma incorrecta.
d) Ninguna de las anteriores

FIN DEL EXAMEN

Arquitectura de Redes I Todos los modelos
Examen Final 12 de enero de 2013

TRAZA

La captura se ha realizado en la maquina CLIENTE.

```
Trama 1 (42 bytes), Arrival Time: Sep 14, 2007 10:00:54.333066000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
   Hardware type: Ethernet (0x0001)
   Protocol type: IP (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (0x0001)
   Sender MAC address: 00:19:21:45:b0:8a
   Sender IP address: 140.24.56.169
   Target MAC address: 00:00:00:00:00:00
   Target IP address: 140.24.56.1
```

```
Trama 2 (60 bytes), Arrival Time: Sep 14, 2007 10:00:54.333411000
Ethernet II, Src: 00:09:7b:e5:d4:40, Dst: 00:19:21:45:b0:8a
Address Resolution Protocol (reply)
   Hardware type: Ethernet (0x0001)
   Protocol type: IP (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (0x0002)
   Sender MAC address: 00:09:7b:e5:d4:40
   Sender IP address: 140.24.56.1
   Target MAC address: 00:19:21:45:b0:8a
   Target IP address: 140.24.56.169
```

```
Trama 3 (76 bytes), Arrival Time: Sep 14, 2007 10:00:54.333451000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:09:7b:e5:d4:40
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.58.100
User Datagram Protocol, Src Port: 1034, Dst Port: 53
Domain Name System (query)
   Transaction ID: 0x3478
   Flags: 0x0100 (Standard query)
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
   Queries
      efetepe.ii.uam.es: type A, class IN
```

Trama 4 (239 bytes), Arrival Time: Sep 14, 2007 10:00:54.335268000
Ethernet II, Src: 00:09:7b:e5:d4:40, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.58.100, Dst: 140.24.56.169
User Datagram Protocol, Src Port: 53, Dst Port: 1034
Domain Name System (response)
  Transaction ID: 0x3478
  Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 5
  Additional RRs: 3
  Queries
    efetepe.ii.uam.es: type A, class IN
  Answers
    efetepe.ii.uam.es: type A, class IN, addr 140.24.57.113
  Authoritative nameservers
    uam.es: type NS, class IN, ns ns2.uam.es
    uam.es: type NS, class IN, ns sun.rediris.es
    uam.es: type NS, class IN, ns chico.rediris.es
    uam.es: type NS, class IN, ns ns.uam.es
    uam.es: type NS, class IN, ns ns0.uam.es
  Additional records
    ns.uam.es: type A, class IN, addr 140.24.58.200
    ns0.uam.es: type A, class IN, addr 140.24.58.226
    ns2.uam.es: type A, class IN, addr 140.24.58.100

Trama 5 (42 bytes), Arrival Time: Sep 14, 2007 10:00:54.363611000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:19:21:45:b0:8a
  Sender IP address: 140.24.56.169
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 140.24.57.113

Trama 6 (60 bytes), Arrival Time: Sep 14, 2007 10:00:54.363755000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Address Resolution Protocol (reply)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (0x0002)
  Sender MAC address: 00:18:8b:18:6b:ae
  Sender IP address: 140.24.57.113
  Target MAC address: 00:19:21:45:b0:8a
  Target IP address: 140.24.56.169

Trama 7 (62 bytes), Arrival Time: Sep 14, 2007 10:00:54.363784000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 0, Len: 0
  Hdr Len: 28 bytes, Flags: 0x02 (SYN), Window size: 65535, Checksum: 0xc84e
  Options: (8 bytes)
    Maximum segment size: 1460 bytes
    NOP
    NOP
    SACK permitted

Trama 8 (62 bytes), Arrival Time: Sep 14, 2007 10:00:54.363954000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 0, Ack: 1, Len: 0
  Hdr Len: 28 bytes, Flags: 0x12 (SYN, ACK), Window size: 17520, Checksum: 0x6455
  Options: (8 bytes)
    Maximum segment size: 1460 bytes
    NOP
    NOP
    SACK permitted

Trama 9 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.363991000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65535, Checksum: 0xd589

Trama 10 (96 bytes), Arrival Time: Sep 14, 2007 10:00:54.366899000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 1, Ack: 1, Len: 42
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17520, Checksum: 0x2c28
File Transfer Protocol (FTP)
  220-FileZilla Server version 0.9.23 beta\r\n

Trama 11 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.552466000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 43, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65493, Checksum: 0xd589

Trama 12 (160 bytes), Arrival Time: Sep 14, 2007 10:00:54.552673000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 43, Ack: 1, Len: 106
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17520, Checksum: 0x177a
File Transfer Protocol (FTP)
  220-written by Tim Kosse (Tim.Kosse@gmx.de)\r\n
  220 Please visit http://sourceforge.net/projects/filezilla/\r\n

Trama 13 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.753621000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 149, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65387, Checksum: 0xd589

Trama 14 (66 bytes), Arrival Time: Sep 14, 2007 10:00:56.170722000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 149, Len: 12
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65387, Checksum: 0x3684
File Transfer Protocol (FTP)
  USER jorge\r\n

Trama 15 (60 bytes), Arrival Time: Sep 14, 2007 10:00:56.337523000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 149, Ack: 13, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17508, Checksum: 0x9085

Trama 16 (87 bytes), Arrival Time: Sep 14, 2007 10:00:59.640578000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
    Src Port: 21, Dst Port: 1143, Seq: 149, Ack: 13, Len: 33
    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17508, Checksum: 0x8819
File Transfer Protocol (FTP)
    331 Password required for jorge\r\n

Trama 17 (54 bytes), Arrival Time: Sep 14, 2007 10:00:59.782589000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
    Src Port: 1143, Dst Port: 21, Seq: 13, Ack: 182, Len: 0
    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65354, Checksum: 0xd57d

Trama 18 (68 bytes), Arrival Time: Sep 14, 2007 10:01:01.387513000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
    Src Port: 1143, Dst Port: 21, Seq: 13, Ack: 182, Len: 14
    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65354, Checksum: 0xb71a
File Transfer Protocol (FTP)
    PASS enrique\r\n

Trama 19 (60 bytes), Arrival Time: Sep 14, 2007 10:01:01.567693000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
    Src Port: 21, Dst Port: 1143, Seq: 182, Ack: 27, Len: 0
    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17494, Checksum: 0x9064

Trama 20 (69 bytes), Arrival Time: Sep 14, 2007 10:01:05.643223000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
    Src Port: 21, Dst Port: 1143, Seq: 182, Ack: 27, Len: 15
    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17494, Checksum: 0x7c42
File Transfer Protocol (FTP)
    230 Logged on\r\n

Trama 21 (54 bytes), Arrival Time: Sep 14, 2007 10:01:05.817346000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
    Src Port: 1143, Dst Port: 21, Seq: 27, Ack: 197, Len: 0
    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65339, Checksum: 0xd56f

Trama 22 (81 bytes), Arrival Time: Sep 14, 2007 10:01:08.866831000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
    Src Port: 1143, Dst Port: 21, Seq: 27, Ack: 197, Len: 27
    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65339, Checksum: 0x0fb2
File Transfer Protocol (FTP)
    PORT 150,244,56,169,4,121\r\n

Trama 23 (60 bytes), Arrival Time: Sep 14, 2007 10:01:09.010690000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
    Src Port: 21, Dst Port: 1143, Seq: 197, Ack: 54, Len: 0
    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17467, Checksum: 0x9055

Trama 24 (83 bytes), Arrival Time: Sep 14, 2007 10:01:13.639891000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
    Src Port: 21, Dst Port: 1143, Seq: 197, Ack: 54, Len: 29
    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17467, Checksum: 0xb633
File Transfer Protocol (FTP)
    200 Port command successful\r\n

Trama 25 (60 bytes), Arrival Time: Sep 14, 2007 10:01:13.670615000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 54, Ack: 226, Len: 6
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65310, Checksum: 0x269c
File Transfer Protocol (FTP)
  LIST\r\n

Trama 26 (62 bytes), Arrival Time: Sep 14, 2007 10:01:13.671578000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 20, Dst Port: **PUERTO**, Seq: 0, Len: 0
  Hdr Len: 28 bytes, Flags: 0x02 (SYN), Window size: 65535, Checksum: 0xb774
  Options: (8 bytes)
    Maximum segment size: 1460 bytes
    NOP
    NOP
    SACK permitted

Trama 27 (100 bytes), Arrival Time: Sep 14, 2007 10:01:13.671803000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 226, Ack: 60, Len: 46
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0x02ca
File Transfer Protocol (FTP)
  150 Opening data channel for directory list.\r\n

Trama 28 (54 bytes), Arrival Time: Sep 14, 2007 10:01:13.863690000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 60, Ack: **SECUENCIA**, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65264, Checksum: 0xd54e

Trama 29 (87 bytes), Arrival Time: Sep 14, 2007 10:01:24.640290000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: **SECUENCIA**, Ack: 60, Len: 33
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0xf5e7
File Transfer Protocol (FTP)
  425 Can't open data connection.\r\n

Trama 30 (54 bytes), Arrival Time: Sep 14, 2007 10:01:24.826833000
Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae
Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113
Transmission Control Protocol
  Src Port: 1143, Dst Port: 21, Seq: 60, Ack: 305, Len: 0
  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65231, Checksum: 0xd54e

Trama 31 (114 bytes), Arrival Time: Sep 14, 2007 10:05:06.633776000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 305, Ack: 60, Len: 60
  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0x23f0
File Transfer Protocol (FTP)
  421 No-transfer-time exceeded. Closing control connection.\r\n

Trama 32 (60 bytes), Arrival Time: Sep 14, 2007 10:05:06.633921000
Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a
Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169
Transmission Control Protocol
  Src Port: 21, Dst Port: 1143, Seq: 365, Ack: 60, Len: 0
  Hdr Len: 20 bytes, Flags: 0x14 (RST, ACK), Window size: 0, Checksum: 0xd3de

FIN DE LA TRAZA

Esta hoja puede ser conservada por el alumno para referencia:

1 a b c d	16 a b c d	31 a b c d
2 a b c d	17 a b c d	32 a b c d
3 a b c d	18 a b c d	33 a b c d
4 a b c d	19 a b c d	34 a b c d
5 a b c d	20 a b c d	35 a b c d
6 a b c d	21 a b c d	36 a b c d
7 a b c d	22 a b c d	
8 a b c d	23 a b c d	
9 a b c d	24 a b c d	
10 a b c d	25 a b c d	
11 a b c d	26 a b c d	
12 a b c d	27 a b c d	
13 a b c d	28 a b c d	
14 a b c d	29 a b c d	
15 a b c d	30 a b c d	

Arquitectura de redes I **Examen 14 de junio de 2013 15:00 – 17:30**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

GRUPO: _____

Tiempo: Dos horas y media
Sin libros ni apuntes
Calificación: Respuesta correcta: +3
Respuesta errónea: -1

---

1. ¿Cómo sabe un servidor SMTP cuál es la longitud de los correos que recibe?
   a) Mediante el campo Content-length de la cabecera.
   b) Porque terminan con " \r\n.\r\n ".
   c) Porque el cliente cierra la conexión TCP cuando ha terminado de enviar el correo.
   d) Porque el cliente manda el comando QUIT.

2. El dominio .com.es es:
   a) Un dominio de nivel superior geográfico (ccTLD).
   b) Un dominio de nivel superior genérico (gTLD).
   c) Un dominio de tercer nivel.
   d) Ninguna de las anteriores

3. ¿Cuál de las siguientes afirmaciones de HTTP es falsa?
   a) HTTP utiliza cabeceras para indicar el tipo de archivo que se descarga.
   b) HTTP implementa cabeceras que facilitan la cache de archivos.
   c) HTTP utiliza URLs para identificar archivos en la red.
   d) HTTP utiliza una conexión de control y otra distinta para la de descarga de archivos.

4. Para desarrollar un servidor de FTP, lo más adecuado es emplear:
   a) Datagram sockets con un solo proceso.
   b) Datagram sockets con varios procesos.
   c) Stream sockets con un solo proceso.
   d) Stream sockets con varios procesos.

5. En un mensaje de DNS:
   a) El formato de las respuestas, registros de autoridad y registros adicionales es el mismo, y distinto al de las preguntas.
   b) El formato de las preguntas, respuestas, registros de autoridad y registros adicionales es el mismo.
   c) El formato de los registros de autoridad y registros adicionales es el mismo, pero distinto al de las preguntas y al de las respuestas.
   d) Los formatos de las preguntas, respuestas, registros de autoridad y registros adicionales son todos diferentes

6. En la arquitectura de SMTP, ¿con qué se corresponde un cliente de correo electrónico?
   a) Con un agente de transferencia de mensajes (MTA).
   b) Con un agente de usuario.
   c) Con un buzón de correo (mailbox).
   d) Ninguna de las anteriores.

7. Desde un ordenador conectado a una red doméstica, se quiere resolver el nombre de dominio www.uam.es. Típicamente, ¿a cuántos servidores DNS consultará dicho ordenador?
   a) Tres: un raíz, uno con autoridad sobre .es, y uno con autoridad sobre .uam.es.
   b) Uno, el asignado por el proveedor de servicios de Internet (ISP).
   c) Uno si el nombre está cacheado en el servidor DNS asignado por el ISP, y si no es así, tres.
   d) Depende de si servidor asignado por el proveedor de servicios de Internet (ISP) admite consultas inversas.

8. ¿Puede ocurrir que un navegador web muestre un archivo JPEG como si fuera texto HTML, en vez de pintarlo como imagen?
   a) Sí, pero sólo si la extensión del archivo es incorrecta, esto es .htm en vez de .jpg
   b) Si puede ocurrir cuando, por cualquier motivo, la cabecera Content-Type sea errónea.
   c) No, en HTTP 1.1 no puede ocurrir, pero sí en HTTP 1.0 debido a que no implementa protecciones.
   d) No, nunca puede ocurrir.

9. ¿Es seguro usar FTP a través de una conexión WiFi no cifrada para descargar un archivo desde un repositorio confidencial?
   a) No, porque FTP no usa cifrado ni en la transmisión de datos ni en la autenticación.
   b) No, porque FTP no usa cifrado en la transmisión. Sin embargo, si el archivo se cifra si podría ser seguro, porque en FTP la autenticación sí que está cifrada.
   c) Sí, usando el comando CRYP de FTP que permite cifrar la conexión.
   d) Sí, pero sólo si se usa el modo pasivo (comando PASV) para la descarga del archivo, puesto que la vulnerabilidad surge cuando se abre un socket en el cliente.

10. ¿Cómo puede saber un cliente HTTP la longitud de los archivos que solicita mediante un comando GET?
   a) Puede saberlo si recibe el campo File-Length de la cabecera de la respuesta HTTP.
   b) No puede saberlo de antemano, el cliente debe siempre recibir datos hasta que el servidor cierra la conexión TCP.
   c) Puede saberlo si recibe el campo Content-Length de la cabecera de la respuesta HTTP.
   d) Está siempre en los cuatro primeros bytes del archivo que se recibe.

11. Un usuario está utilizando para acceder a su correo. una aplicación webmail disponible comercialmente y que está conectada a un servidor externo a través de un cortafuegos que solo deja pasar paquetes con destino al puerto 80 ¿Qué protocolo o protocolos se estarán empleando en el ordenador de dicho usuario para que funcione dicha aplicación?
   a) HTTP.
   b) HTTP y SMTP.
   c) HTTP, SMTP y POP3.
   d) IMAP4.

12. **Dos sistemas conectados al mismo segmento de red está utilizando HTTP para conectarse a un servidor de páginas en Internet. En el Browser se introduce la siguiente dirección en ambos sistemas:**

Uno de los sistemas da error y el otro no. Sin embargo, cuando se introduce la siguiente información:

Ambos sistemas se conectan correctamente al servidor de páginas correspondiente. Indicar cuál de los siguientes motivos podría provocar este comportamiento:

a) Uno de los sistemas no tiene el protocolo HTTP correctamente configurado por lo que la direccion IP que se obtiene es errónea.
b) Al hacer la consulta al servidor DNS uno de los sistemas añade automáticamente el dominio ii.uam.es al nombre del destino y el otro no.
c) El servidor de páginas "sistema1" no tiene el protocolo HTTP correctamente configurado
d) Ninguna de las anteriores.

13. **Desde una máquina de la UAM se hace una consulta al servidor de nombres de la Universidad sobre la dirección www.google.com. ¿Cuántas preguntas DNS como mínimo se mandarán desde el servidor de nombres de la UAM?**
a) 0
b) 1
c) 2
d) Ninguna de las anteriores

14. **En un proyecto se debe hacer un servidor HTTP lo más ligero posible porque va a ser ejecutado en una máquina con unas prestaciones muy limitadas. Sólo se le pide la funcionalidad básica de servir páginas web y no se van a enviar datos al servidor. ¿Qué comandos HTTP se deberían implementar?**
a) GET
b) GET y POST
c) GET y PUT
d) GET, HEAD y POST

15. **Desde un sistema conectado a Internet, usando el comando telnet, se abre un socket al puerto 25 de otro sistema remoto, que tiene un servidor esperando en dicho puerto:**

C:\>telnet cis.ply.edu 25

A continuación se envía lo siguiente

GET /~ross/ HTTP/1.1
Host: cis.poly.edu

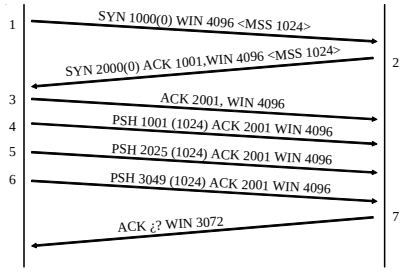
¿Qué es lo más probable que ocurra?
a) El servidor devolverá una página html que se representará en pantalla como una página web.
b) El servidor devolverá una página html, pero lo que se representa en pantalla es el código sin interpretar.
c) El servidor devolverá una página html, pero no es seguro que corresponda con la que se pide.
d) Ninguna de las anteriores

16. **¿Cuál es el tamaño máximo de la ventana en TCP?**
a) 64 KB
b) 256 B
c) 64 Ksegmentos
d) Ninguna de las anteriores

17. **En el diagrama de estados de TCP, indicar cuál de las siguientes respuestas no es objetivo del estado de TIME_WAIT**
a) Poder retransmitir el ACK final del cierre de conexión si es que se hubiera perdido
b) Evitar mezcla de paquetes entre dos conexiones
c) Esperar un cierto tiempo antes de que el socket se pueda reutilizar
d) Gestionar el cierre simultáneo de TCP

18. **¿Cuál de las siguientes afirmaciones acerca del checksum de UDP es falsa?**
a) Es opcional, si está a cero es que no se usa
b) Implementa una detección de errores en los datos
c) Implementa además una detección de errores en ciertos campos de la cabecera IP
d) Usa un CRC con el polinomio generador x^15 + x + 1

19. **Dado el siguiente diagrama de secuencia en una conexión TCP**

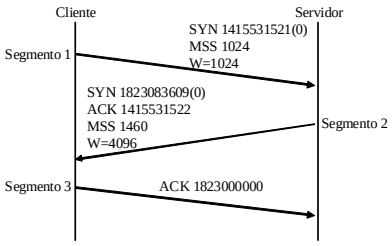


¿Cuánto debe valer el último ACK (segmento 7) si suponemos que todos los segmentos han llegado sin errores?

a) 4073
b) 4074
c) 3050
d) Ninguna de las anteriores

20. **Sobre un enlace de 1 Mbit/s una conexión TCP envía segmentos de L bytes, y la ventana de congestión del receptor está fijada en 6 de estos segmentos. El tiempo que transcurre desde el envío de un segmento hasta que se recibe el ACK para dicho segmento es de 210 ms. Despreciando las cabeceras ¿cuál es el valor mínimo de L para el que se obtiene envío continuo?**
    a) 35000 bytes
    b) 210000 bytes
    c) 26250 bytes
    d) 4375 bytes

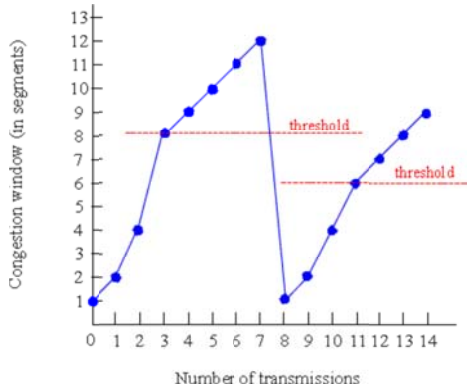
21. **Dado el siguiente intercambio de segmentos TCP, indicar cuál de las siguientes afirmaciones es cierta:**



a) Se ha establecido la conexión entre ambos extremos, por lo que puede empezar la transmisión de datos
b) Faltaría recibir en el cliente un ACK del servidor para completar la conexión
c) El protocolo de conexión no está terminado aún, pero puede completarse si se transmite(n) el (los) segmento(s) adecuado(s)
d) Ninguna de las anteriores

22. **Se realiza una conexión TCP. Se estima que el sistema tiene una velocidad de transmisión máxima para los segmentos de TCP de 50.000 Bytes por segundo. Si se consigue una velocidad de transmisión de segmentos de 10.000 Bytes/segundo al aplicar una ventana en el receptor de 5.000 bytes, indicar cuál sería el RTT de la conexión:**
    a) 100 ms.
    b) 0,5 s.
    c) 0,25 s.
    d) Ninguna de las anteriores

23. **La siguiente figura representa la evolución de la ventana de congestión en un sistema:**



Indicar qué está pasando:
a) El sistema ha detectado congestión al transmitir el segmento 3 y el segmento 12
b) El sistema ha detectado congestión al transmitir los segmentos 4 y 9
c) El sistema ha detectado congestión al transmitir el segmento 7 y el 11
d) Ninguna de las anteriores

CAPTURA: Las siguientes cuestiones se refieren a la Captura adjunta

24. **¿A qué se debe que la ventana de recepción del servidor se mantenga siempre en 17520?**
    a) A que el cliente no envía datos.
    b) A que el buffer de recepción del servidor se libera siempre antes de enviar un segmento.
    c) Es el reflejo del fenómeno de arranque lento.
    d) Es el reflejo del fenómeno de recuperación rápida.

25. **¿Qué valor debe tener el número de secuencia descrito en la captura como "SECUENCIA"?**
    a) 285
    b) 286
    c) 261
    d) 262
26. **¿Qué valor tiene el número de puerto descrito en la captura como "PUERTO"?**
    a) 5001
    b) 4982
    c) 3136
    d) 3137
27. **¿Aprovecha el servidor el tamaño MSS anunciado por el cliente? ¿Por qué?**
    a) No se puede saber.
    b) Sí, porque siempre envía los paquetes con el tamaño máximo.
    c) No, porque el servidor se ve limitado por la ventana del cliente.
    d) No, porque ningún segmento llega al tamaño del MSS.
28. **¿Por qué en la trama 25 se asiente 44, si el último número de secuencia recibido por el servidor es 13 y dicho segmento contiene 30 octetos?**
    a) Porque el segmento asentido lleva activado el bit FIN.
    b) Porque el segmento asentido lleva activado el bit PSH.
    c) Porque siempre se asiente con el número de secuencia siguiente a la suma del número de secuencia anterior y el número de octetos.
    d) Porque ha habido un error en la transmisión.
29. **¿En qué estado queda el servidor al enviar la trama 27?**
    a) TIME_WAIT
    b) FIN_WAIT_1
    c) CLOSE_WAIT
    d) CLOSING
30. **¿En qué estado queda el cliente al recibir la trama 33?**
    a) FIN_WAIT_1
    b) CLOSE_WAIT
    c) TIME_WAIT
    d) CLOSING
31. **¿A qué se debe que la ventana de recepción del cliente comience con 64240 bytes y termine con 63942 bytes?**
    a) A que se utiliza como mecanismo de asentimiento de las tramas recibidas.
    b) A que el buffer de recepción del cliente no se ha liberado durante la conexión.
    c) Es el reflejo del fenómeno de arranque lento.
    d) Es el reflejo del fenómeno de recuperación rápida.

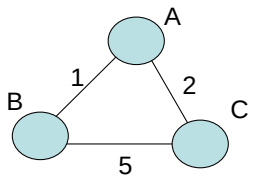
FINAL CAPTURA

---

32. **Se ha comprobado que un sistema de comunicaciones produce dos tipos de errores: los que afectan a un sólo bit y los que afectan a una serie de bits seguidos (ráfagas). Se ha decidido en IP que la protección de errores sea sólo para la cabecera. Indicar el motivo:**
    a) Porque es mucho más probable que los errores afecten a la cabecera que a los datos
    b) Porque es necesario para el cálculo de las rutas, que debe seguir el datagrama, al consultar la tabla de enrutamiento
    c) Porque un bit erróneo en la cabecera puede provocar que el datagrama se entregue en un destino erróneo
    d) Ninguna de las anteriores

33. **Para poder estudiar la utilización de los algoritmos de encaminamiento, se quiere dar pesos a los enlaces entres nodos y routers que indiquen la distancia para aplicar el algoritmo de Dijkstra (x es el peso del enlace a 100Mbps, y el del enlace a 9.6Kbps y z el de 10Mbps). Indicar de las siguientes alternativas cuál supondría un modelado más realista de la red:**
    a) x=1, y=10000, z=10
    b) x=100, y=0.96, z=10
    c) x=800, y=0.96, z=80
    d) x=10, y=10000, z=1
34. **Si se aplica el algoritmo de Dijkstra en un router A, lo que se obtendría sería:**
    a) La infomación necesaria para poder diseñar las máscaras de la red
    b) Un árbol con los caminos de distancia mínima desde A a los nodos de la red
    c) Medir los pesos correctos de los enlaces entre los nodos, que permitirá corregir las tablas de enrutamiento de A
    d) Ninguna de las anteriores
35. **Se pretende evaluar la implantación de un algoritmo basado en vector distancia (VD). Se contempla el incluir "poisoned reverse". Indicar cuál es su utilidad:**
    a) Permite que un nodo indique a otro que se cambie el algoritmo al de estado de enlace en la red
    b) Permite evitar una situación "cuenta al infinito" cuando hay un cambio en la métrica de un enlace.
    c) Permite identificar que se ha entrado en el estado de "cuenta al infinito" con lo que debe esperarse tiempos muy largos de convergencia.
    d) Ninguna de las anteriores.

36. Se modela una red según el grafo siguiente:



Si se aplica el algoritmo Vector Distancia en el nodo A, indicar cuál de las siguientes tablas sería la inicial en el nodo A:

Coste vía

Dest. (D^A)	B	C
B	1	∞
C	6	∞

TABLA 1

Coste vía

Dest. (D^A)	B	C
B	1	∞
C	6	2

TABLA 2

Coste vía

Dest. (D^A)	B	C
B	1	∞
C	∞	2

TABLA 3

a) La tabla 1
b) La tabla 2
c) La tabla 3
d) Ninguna

37. (Continuación de la pregunta anterior) Una vez que el algoritmo VD ha llegado a su situación estable, se produce un cambio en el enlace entre los routers B y C y el peso asociado al mismo queda como 3. El router C es el que detecta el cambio y lo empieza a propagar. Envía un primer mensaje a los nodos B y A para que actualicen las tablas de distancias. Después de la recepción de este primer mensaje, indicar cuál es el contenido de la tabla de distancias en el nodo B. (no considerar "poisoned reverse")

Coste vía

Dest. (D^B)	A	C
A	1	5
C	5	3

TABLA 1

Coste vía

Dest. (D^B)	A	C
A	1	∞
C	3	∞

TABLA 2

Coste vía

Dest. (D^B)	A	C
A	1	∞
C	3	3

TABLA 3

a) La tabla 1
b) La tabla 2
c) La tabla 3
d) Ninguna

38. El nivel IP de un sistema conectado a Internet está reconstruyendo un datagrama a partir de los fragmentos que se van recibiendo. En un determinado momento se tienen varios fragmentos almacenados en memoria, ninguno con el bit MF a cero. El temporizador de espera expira. Indicar cuál de las siguientes afirmaciones es cierta:

a) Sólo puede ocurrir que falte un único fragmento para completar el datagrama
b) Pueden faltar varios fragmentos por recibirse
c) Sólo puede ocurrir que se haya producido un error en alguno de los bits de MF
d) Ninguna de las anteriores

39. Un datagrama se fragmenta en tres paquetes más pequeños. ¿Cuál de las siguientes afirmaciones es cierta?

a) El bit DontFragment (DF) se pone a 1 en los tres paquetes.
b) El bit MoreFragments (MF) se pone a 0 en los tres paquetes.
c) El campo de identificación es el mismo para los tres paquetes.
d) Ninguna de las anteriores.

40. Un datagrama IP que contiene un segmento TCP es descartado por un router debido a que el campo TTL ha llegado a cero. El router genera un mensaje ICMP encapsulado dentro de un datagrama IP con las siguientes características:

a) El campo protocolo del datagrama IP tendrá el valor asignado a TCP.
b) La dirección IP destino será igual a la dirección origen del datagrama descartado.
c) La dirección IP origen será igual a la dirección destino del datagrama descartado.
d) Al utilizarse TCP, no se emplea ICMP para informar de errores.

41. Dadas la dirección IP 150.244.78.65 y la máscara de subred 255.255.255.224, ¿cuál es la dirección de la subred?

a) 150.244.78.0
b) 150.244.78.32
c) 150.244.78.64
d) 150.244.78.65

42. **Un sistema A está separado del servidor B por n routers. Para obtener la ruta desde A hasta B se utiliza la herramienta tracert. En este caso:**
    a) Se enviarán desde A mensajes ICMP echo request con destino B variando el TTL desde 1 a n
    b) Se enviarán desde A mensajes ICMP echo request con destino B variando el TTL desde 1 a n+1
    c) Se enviarán desde A mensajes ICMP echo request con destino a cada uno de los routers intermedios
    d) En respuesta a los mensajes enviados por A, los routers intermedios responderán con mensajes ICMP echo reply

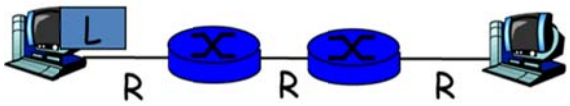
43. **El efecto de HOL se produce en los routers cuya arquitectura de colas es:**
    a) Colas de entrada
    b) Colas de salida
    c) En ambos casos, colas de entrada y de salida
    d) En ninguno de los dos casos, entrada o salida.

44. **El tamaño de una cabecera IP sin opciones es de**
    a) 10 Bytes
    b) 20 Bytes
    c) 40 Bytes
    d) Ninguna de las anteriores

45. **Si un nivel IP tiene que enviar un datagrama con 5000 Bytes de datos a través de un enlace con MTU de 1500 Bytes, ¿Cuántos fragmentos se envían, considerando que la cabecera IP no tiene opciones?**
    a) 2
    b) 3
    c) 5
    d) Ninguna de las anteriores

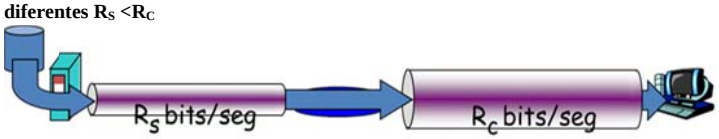
46. **Dada la dirección de red 200.23.16.0/23 indica cuál es la parte de subred:**
    a) 11001000 10010111 00010000
    b) 11001000 00010111 00010000
    c) 11001000 00010111 11010000
    d) Ninguna de las anteriores

47. **Se quiere transmitir un paquete de tamaño L = 1.000 bits (1kb) usando la red que se indica en la figura, cuyos enlaces tienen un ancho de banda de R=500 bps. ¿Cuánto se tarda en recibir el paquete completo en el destino, contando desde el momento en que se empieza a transmitir y despreciando los tiempos de propagación por los enlaces entre nodos?**



    a) 4s.
    b) 5s.
    c) 6s.
    d) Ninguna de las anteriores

48. **Se transmite información usando la red de la figura, en la que los anchos de banda instantáneos de los enlaces son diferentes $R_S < R_C$**



Indicar cuál es el ancho de banda medio extremo a extremo que se obtendría.

    a) Como mucho RC
    b) Como mucho RS
    c) Un valor intermedio entre RC y RS
    d) El producto de RC y RS