Arquitectura de redes I **Test de clase 3 de octubre de 2011 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:

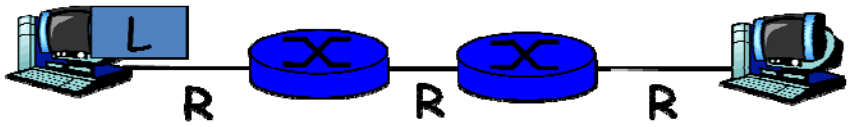
   a. La dirección del sistema www.ii.uam.es es 150.244.56.51
   b. Hay un problema en el sistema, el comando tracert no funciona
   c. Hay un error, se han confundido los nombres www y afrodita
   d. Ninguna de las anteriores
5. **Indicar cuál es el motivo por el que en el proceso de encapsulado, cada 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

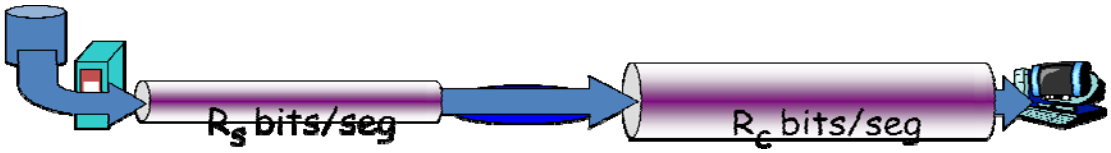
14. **En las redes de conmutación de paquetes, los nodos de conmutación tienen memoria dedicada a almacenar paquetes (colas). Indicar cuál es uno de los motivos para usar dicha memoria**

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 31 de octubre de 2011 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. ¿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 segundo nivel.
d) Un dominio invalido.

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.

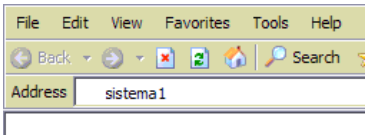
8. **¿Puede ocurrir que un navegador web muestre un archivo JPEG como si fuera texto HTML, en vez de pintarlo como imagen?**
   a) Sí, pero sólo si la extensión del archivo es incorrecta, esto es .htm en vez de .jpg
   b) Si puede ocurrir cuando, por cualquier motivo, la cabecera Content-Type sea errónea.
   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.

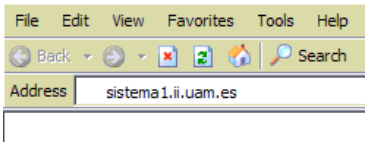
10. **¿Cómo puede saber un cliente HTTP la longitud de los archivos que solicita mediante un comando GET?**
    a) Puede saberlo si recibe el campo File-Length de la cabecera de la respuesta HTTP.
    b) No puede saberlo de antemano, el cliente debe siempre recibir datos hasta que el servidor cierra 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:

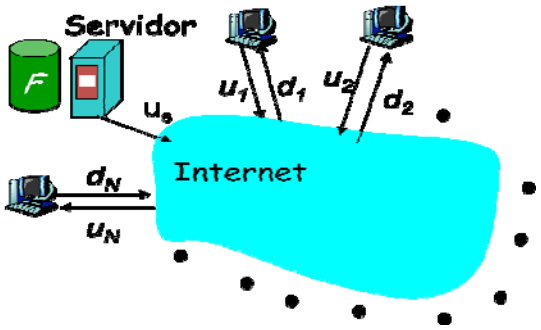


Ambos sistemas se conectan correctamente al servidor de páginas correspondiente. Indicar cuál de los siguientes motivos podría provocar este comportamiento:
   a) Uno de los sistemas no tiene el protocolo HTTP correctamente configurado por lo que la direccion IP que se obtiene es errónea.
   b) Al hacer 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. **Se pretende estimar cuál es el tiempo necesario para distribuir un fichero F de longitud de 1MB 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) 0,8 segundos
    b) 0,73 segundos
    c) 0,01 segundos
    d) Ninguna de las anteriores

F	N	Us	Ui	Di	F/Us	F/di	NF/(us+ SUM(ui))
8.000.000,00	100,00	1.000.000.000,00	1.000.000,00	10.000.000,00	0,01	0,80	0,73

16. **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

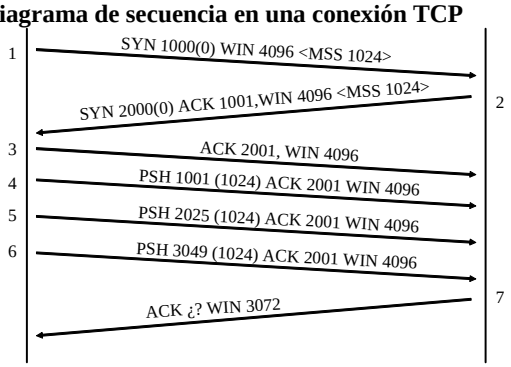
Arquitectura de redes I **Test de clase 5 de diciembre de 2011 16:00 – 16:45**
Modelo 1
NOMBRE Y APELLIDOS
(MAYÚSCULAS)_____

GRUPO: _____

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

---

1. **¿Cuál es el tamaño máximo de la ventana en TCP?**
   a) 64 KB
   b) 256 B
   c) 64 Ksegmentos
   d) Ninguna de las anteriores
2. **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
3. **¿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
4. **Dado el siguiente diagrama de secuencia en una conexión TCP**

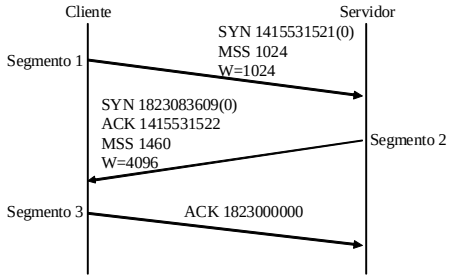


¿Cuánto debe valer el último ACK (segmento 7)?

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

5. **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

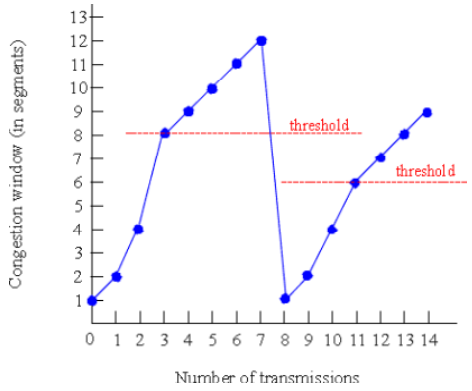
6. **Dado el siguiente intercambio de segmentos TCP, indicar cuál de las siguientes afirmaciones es cierta:**



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

7. **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

8. **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

9. **¿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.

10. **¿Qué valor debe tener el número de secuencia descrito en la captura como "SECUENCIA"?**
   a) 285
   b) 286
   c) 261
   d) 262

11. **¿Qué valor tiene el número de puerto descrito en la captura como "PUERTO"?**
   a) 5001
   b) 4982
   c) 3136
   d) 3137

12. **¿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.

13. **¿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.

14. **¿En qué estado queda el servidor al enviar la trama 27?**
   a) TIME_WAIT
   b) FIN_WAIT_1
   c) CLOSE_WAIT
   d) CLOSING

15. **¿En qué estado queda el cliente al recibir la trama 33?**
   a) FIN_WAIT_1
   b) CLOSE_WAIT
   c) TIME_WAIT
   d) CLOSING

16. **¿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.

Arquitectura de redes I
CAPTURA correspondiente al test de clase del 5 de Diciembre de 2011

Frame 1 (42 bytes on wire, 42 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: ff:ff:ff:ff:ff:ff Address Resolution Protocol Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: 0x0001 Sender MAC address: 00:02:3f:56:ba:b6 Sender IP address: 82.185.99.93 Target MAC address: 00:00:00:00:00:00 Target IP address: 82.185.96.1
Frame 2 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Address Resolution Protocol Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: 0x0002 Sender MAC address: 00:11:20:6a:a8:f8 Sender IP address: 82.185.96.1 Target MAC address: 00:02:3f:56:ba:b6 Target IP address: 82.185.99.93
Frame 3 (73 bytes on wire, 73 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 62.81.16.131 User Datagram Protocol, Src Port: 3009, Dst Port: domain (53) Domain Name System (query) Transaction ID: 0x0136 Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries ftp.fi.upm.es: type A, class IN

Frame 4 (289 bytes on wire, 289 bytes captured)
Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6
Internet Protocol, Src: 62.81.16.131, Dst: 82.185.99.93
User Datagram Protocol, Src Port: domain (53), Dst Port: 3009
Domain Name System (response)
  Transaction ID: 0x3601
  Flags: 0x8180 (Standard query response, No error)
  Questions: 1
  Answer RRs: 2
  Authority RRs: 5
  Additional RRs: 5
  Queries
    ftp.fi.upm.es: type A, class IN
  Answers
    ftp.fi.upm.es: type CNAME, class IN, cname asterix.fi.upm.es
    asterix.fi.upm.es: type A, class IN, addr 138.100.8.6
  Authoritative nameservers
    fi.upm.es: type NS, class IN, ns zape.fi.upm.es
    fi.upm.es: type NS, class IN, ns goofy.fi.upm.es
    fi.upm.es: type NS, class IN, ns asterix.fi.upm.es
    fi.upm.es: type NS, class IN, ns galileo.ccupm.upm.es
    fi.upm.es: type NS, class IN, ns ns.fi.upm.es
  Additional records
    ns.fi.upm.es: type A, class IN, addr 138.100.8.23
    ns.fi.upm.es: type A, class IN, addr 138.100.240.4
    ns.fi.upm.es: type A, class IN, addr 138.100.8.1
    ns.fi.upm.es: type A, class IN, addr 138.100.8.4
    galileo.ccupm.upm.es: type A, class IN, addr 138.100.4.4

Frame 5 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8
Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6
Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 0, Len: 0, Hdr Len: 28, Flags: 0x0002 (SYN), Window: 64240
  Options: (8 bytes)
    Maximum segment size: 1460 bytes
    NOP
    NOP
    SACK permitted

Frame 6 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6
Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 0, Ack: 1, Len: 0, Hdr Len: 24, Flags: 0x0012 (SYN, ACK), Window: 17520
  Options: (4 bytes)
    Maximum segment size: 1460 bytes

Frame 7 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8
Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6
Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 64240

Frame 8 (104 bytes on wire, 104 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 1, Ack: 1, Len: 50, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 220 ProFTPD 1.3.0 Server (asterix) [138.100.8.6]\r\n
Frame 9 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 1, Ack: 51, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 64190
Frame 10 (70 bytes on wire, 70 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 1, Ack: 51, Len: 16, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 64190 File Transfer Protocol (FTP) USER anonymous\r\n
Frame 11 (130 bytes on wire, 130 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 51, Ack: 17, Len: 76, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 331 Anonymous login ok, send your complete email address as your password.\r\n
Frame 12 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 17, Ack: 127, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 64114
Frame 13 (68 bytes on wire, 68 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 17, Ack: 127, Len: 14, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 64114 File Transfer Protocol (FTP) PASS usuario@fi.upm.es\r\n
Frame 14 (105 bytes on wire, 105 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 127, Ack: 31, Len: 51, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 230 Anonymous access granted, restrictions apply.\r\n
Frame 15 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 31, Ack: 178, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 64063

Frame 16 (80 bytes on wire, 80 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 31, Ack: 178, Len: 26, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 64063 File Transfer Protocol (FTP) PORT 82,185,99,93,19,137\r\n
Frame 17 (83 bytes on wire, 83 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 178, Ack: 57, Len: 29, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 200 PORT command successful\r\n
Frame 18 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 57, Ack: 207, Len: 6, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 64034 File Transfer Protocol (FTP) NLST[1]\r\n
Frame 19 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: PUERTO, Seq: 0, Len: 0, Hdr Len: 24, Flags: 0x0002 (SYN), Window: 17520 Options: (4 bytes) Maximum segment size: 1460 bytes
Frame 20 (58 bytes on wire, 58 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: PUERTO, Dst Port: ftp-data (20), Seq: 0, Ack: 1, Len: 0, Hdr Len: 24, Flags: 0x0012 (SYN, ACK), Window: 64240 Maximum segment size: 1460 bytes
Frame 21 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: PUERTO, Seq: 1, Ack: 1, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 17520
Frame 22 (108 bytes on wire, 108 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 207, Ack: 63, Len: 54, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 150 Opening ASCII mode data connection for file list\r\n
Frame 23 (66 bytes on wire, 66 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: PUERTO, Seq: 1, Ack: 1, Len: 12, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 FTP Data FTP Data: lost+found\r\n

[1] Comando similar a LIST

Frame 24 (84 bytes on wire, 84 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: PUERTO, Seq: 13, Ack: 1, Len: 30, Hdr Len: 20, Flags: 0x0019 (FIN, PSH, ACK), Window: 17520 FTP Data FTP Data: pub\r\nbin\r\netc\r\nlib\r\nincoming\r\n
Frame 25 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: PUERTO, Dst Port: ftp-data (20), Seq: 1, Ack: 44, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 64198
Frame 26 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: PUERTO, Dst Port: ftp-data (20), Seq: 1, Ack: 44, Len: 0, Hdr Len: 20, Flags: 0x0011 (FIN, ACK), Window: 64198
Frame 27 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: PUERTO, Seq: 44, Ack: 2, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 17520
Frame 28 (78 bytes on wire, 78 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 261, Ack: 63, Len: 24, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 226 Transfer complete.\r\n
Frame 29 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 63, Ack: SECUENCIA, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 63956
Frame 30 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 63, Ack: SECUENCIA, Len: 6, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 63956 File Transfer Protocol (FTP) QUIT\r\n
Frame 31 (68 bytes on wire, 68 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: SECUENCIA, Ack: 69, Len: 14, Hdr Len: 20, Flags: 0x0018 (PSH, ACK), Window: 17520 File Transfer Protocol (FTP) 221 Goodbye.\r\n
Frame 32 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 69, Ack: 299, Len: 0, Hdr Len: 20, Flags: 0x0011 (FIN, ACK), Window: 63942

Frame 33 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136, Seq: 299, Ack: 69, Len: 0, Hdr Len: 20, Flags: 0x0011 (FIN, ACK), Window: 17520
Frame 34 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:56:ba:b6, Dst: 00:11:20:6a:a8:f8 Internet Protocol, Src: 82.185.99.93, Dst: 138.100.8.6 Transmission Control Protocol, Src Port: 3136, Dst Port: ftp (21), Seq: 70, Ack: 300, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 63942
Frame 35 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 00:11:20:6a:a8:f8, Dst: 00:02:3f:56:ba:b6 Internet Protocol, Src: 138.100.8.6, Dst: 82.185.99.93 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3136 (3136), Seq: 299, Ack: 70, Len: 0, Hdr Len: 20, Flags: 0x0010 (ACK), Window: 17520

Arquitectura de redes I **Test de clase 19 de diciembre de 2011 17:00 – 17:45**
Modelo 1
NOMBRE Y APELLIDOS (MAYÚSCULAS)_____

GRUPO: _____

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

---

1. **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

2. **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

3. **Para poder estudiar con detalle lo que ocurre al aplicar el algoritmo de Dijkstra, se desarrolla un programa que lo ejecuta. El pseudo-código es el siguiente, utilizando la notación vista en teoría:**

```
1  Inicialización:
2   N = {A}
3   Para todos los nodos  v
4     Si  v es vecino directo de A
5       entonces D(v) = c(A,v)
6       Si no  D(v) = infinito
7
8   Repetir
9     Encontrar w no incluido en N tal que D(w) es un mínimo
10    Añadir  w a N
11    Actualizar D(v) para todos los v vecinos directos de w y no en N:
12
13  Hasta que todos los nodos estén en  N
```

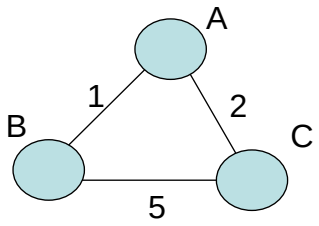
Indicar cuál es la línea 12 que falta:

   a) D(v) = min(D(v), D(w) + c(A,v))
   b) D(v) = min (D(w), D(w) + c(w,v))
   c) D(v) = min(D(v), D(w) + c(w,v))
   d) Ninguna de las anteriores

4. **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

5. **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.

6. **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

7. **(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")**

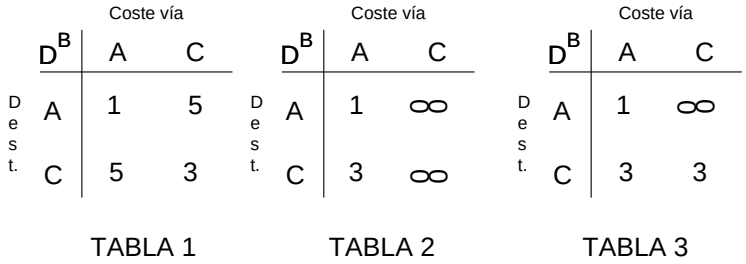


TABLA 1 TABLA 2 TABLA 3

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

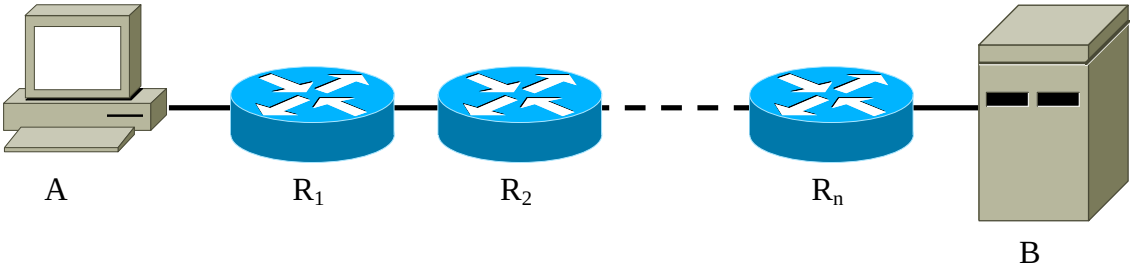
8. **El nivel IP de un sistema conectado a Internet está reconstruyendo un datagrama a partir de los fragmentos que se van recibiendo. En un determinado momento se tienen varios fragmentos almacenados en memoria, ninguno con el bit MF a cero. El temporizador de espera expira. Indicar cuál de las siguientes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

9. **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.

10. **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.

11. **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

12. Según se muestra en la figura, el 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

13. 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.

14. El tamaño de una cabacera IP sin opciones es de

a) 10 Bytes
b) 20 Bytes
c) 40 Bytes
d) Ninguna de las anteriores

15. 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

16. 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

Arquitectura de Redes I

Tutoría 12 de enero de 2012 16:00

CUESTIONES:

1. **Antes de empezar la transmisión de datos entre dos hosts se mide cuál es el path MTU entre ellos, que resulta ser de 1500. Se hace también un traceroute, y se averigua que hay 9 saltos (routers intermedios) entre ambos hosts. Se configura el stack TCP/IP de ambas máquinas para usar un MTU de 1500, y comienza una transmisión de datos usando HTTP. ¿Pueden llegar paquetes fragmentados a alguna de las máquinas?**
   a) Sí, porque el path MTU puede variar en cualquier momento.
   b) No, porque los routers aseguran que segmentos de una misma conexión TCP irán siempre por el mismo camino.
   c) Sí, pero sólo en el caso que los paquetes se dupliquen porque haya routers redundantes en el camino.
   d) No, los routers siempre reensamblan los fragmentos antes de entregarlos a su destino final.

2. **Para mejorar la fiabilidad de un sistema, se decide redundar el enlace que da servicio a la subred de servidores, y en vez de usar un mecanismo de encaminamiento dinámico se opta por mandar todos los paquetes por ambos enlaces, llegando siempre duplicados a esta subred de servidores.**
   a) Es una solución válida y no tendrá ningún efecto secundario.
   b) Es una solución válida pero aumentará la carga de la pila TCP/IP de los servidores.
   c) Es una solución válida, pero si cae uno de los enlaces el tiempo sin servicio será mayor que si se opta por una solución de encaminamiento dinámico basada en RIP.
   d) No es una solución válida, porque IP no soporta la existencia de paquetes duplicados.

3. **¿Cuántos ordenadores se pueden conectar a una red privada con dirección 10.0.0.32 y máscara 255.255.255.240, considerando que ya hay conectados a esa red 2 routers y 3 servidores?**
   a) 11.
   b) 9.
   c) La máscara no es válida para esa dirección de red.
   d) La dirección de red no es válida.

4. **El arranque lento de TCP impide que se puedan enviar datos a la máxima velocidad inmediatamente después de la apertura de una conexión. ¿Cómo se consigue superar este arranque lento para llegar a optimizar la velocidad de transmisión?**
   a) Recibiendo asentimientos desde el otro extremo.
   b) Midiendo el tiempo que tardan en llegar los asentimientos desde el otro extremo.
   c) Esperando a que expire el temporizador de arranque lento.
   d) Recibiendo un mensaje ICMP de un router intermedio.

5. **¿Para cuál de las siguientes aplicaciones NO es buena idea usar UDP?**
   a) Streaming de video en aplicaciones pay-per-view.
   b) Enviar un archivo voluminoso a varios destinos mediante multicast.
   c) Protocolo cliente/servidor que usa preguntas y respuestas cortas y que se emplea principalmente en un entorno de redes de área local.
   d) Protocolo cliente/servidor que usa respuestas largas y que se emplea principalmente para acceder a servidores lejanos conectados vía Internet.

6. **¿Puede ocurrir el problema del conteo al infinito en BGP?**
   a) Sí, porque usa un algoritmo de vector distancia.
   b) No, siempre que se use BGPv3, que usa un algoritmo de estado de enlace.
   c) Sí, porque los EGP por definición pueden tener este problema.
   d) No, porque usa un algoritmo de vector camino.

7. **¿Pueden varios servidores contestar a un mensaje DISCOVER de DHCP?**
    a) No, porque en una subred sólo puede haber un único servidor DHCP.
    b) No, porque el primer servidor contesta en difusión, y así los otros servidores ven también la respuesta y saben que no tienen que contestar.
    c) Sí, porque DHCP permite que haya varios servidores en una subred.
    d) Sí, porque es el mecanismo que permite que pueda funcionar el relaying de DHCP.

8. **¿Cómo sabe un cliente web como representar los archivos que recibe por HTTP?**
    a) Por la extensión del archivo.
    b) Por el tipo MIME.
    c) Mirando los primeros bytes del archivo.
    d) Mediante los tags HTML del documento que enlaza con el archivo recibido.

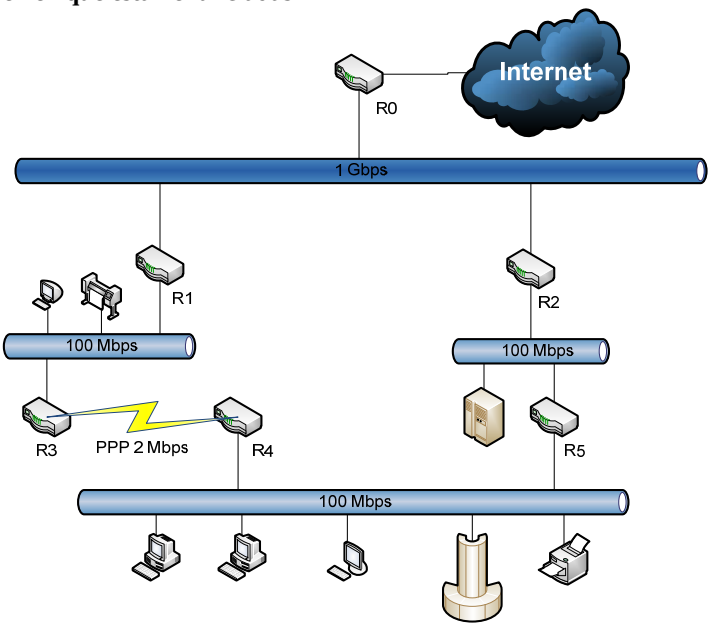
9. **¿Es posible poner un servidor HTTP en una red doméstica conectada a Internet a través de un router ADSL con funcionalidad NATP, y que tiene una única dirección IP pública asignada dinámicamente? Los usuarios del servidor web sólo conocen su FQDN.**
    a) Sí, siempre, sin ningún problema.
    b) Sí, pero para el nombre del dominio habrá que contratar un servicio DynDNS o similar.
    c) No, hay que cambiar el router por uno que tenga funcionalidad NAT.
    d) No, hay que contratar una dirección IP pública fija.

10. **¿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.

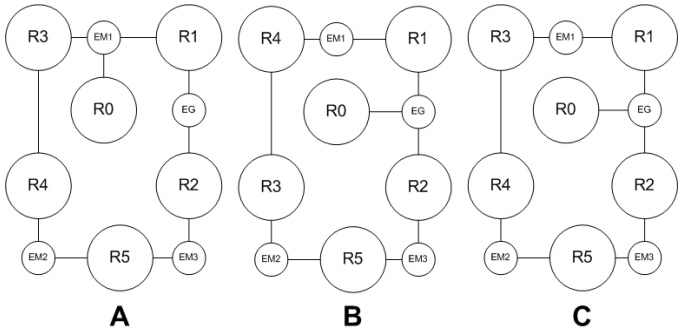
11. **¿Cuando se envía la opción MSS en la cabecera TCP?**
    a) Con el primer segmento de datos.
    b) Con el segmento de apertura de conexión (SYN activado).
    c) Con el segmento que asiente la apertura de conexión (segundo y tercer segmentos en el protocolo de 3 pasos, *three-way-handshake*).
    d) En cualquier momento de la transmisión si detecta un cambio en el path MTU.

PROBLEMA : Diseño de *routing*

Se quiere estudiar el *routing* en la topología de red indicada en la figura adjunta, para lo cual se requiere modelar la red como un grafo. Para responder cada pregunta tenga también en cuenta las condiciones planteadas en las preguntas anteriores. El orden de las preguntas es relevante, por lo que se deben contestar en el orden en que están enunciadas



12. Indicar cuál de los siguientes grafos serviría para modelar la red, siguiendo el convenio explicado para estado de enlace:



a) El grafo A.
b) El grafo B.
c) El grafo C.
d) Ninguno.

13. Para poder estudiar la utilización de los algoritmos de encaminamiento, se quiere dar pesos a los arcos del grafo que indiquen la distancia para aplicar el algoritmo de Dijkstra. Indicar, de las siguientes alternativas, cuál supondría un modelado más realista de la red, basándose en los retardos de transmisión:

a) c(R3, R4) =2, c(R*i*, EG) = 1000, c(R*j*, EM*k*) = 100.
b) c(R3, R4) =0.2, c(R*i*, EG) = 10, c(R*j*, EM*k*) = 1000.
c) c(R3, R4) =20, c(R*i*, EG) = 10, c(R*j*, EM*k*) = 1.
d) c(R3, R4) =500, c(R*i*, EG) = 1, c(R*j*, EM*k*) = 10.

14. **Si se aplica el algoritmo de Dijkstra al *router* R0, lo que se obtendría sería:**
    a) La información necesaria para poder diseñar las máscaras de la red.
    b) Un árbol con los caminos de distancia mínima desde R0 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 R0.
    d) Ninguna de las anteriores.

15. **Al final, se decide utilizar como pesos de los arcos una estimación de las cargas de tráfico correspondientes, que quedan como sigue:**

c(R3,R4)	**5**
c(R*i*,EG)	**7**
c(R*j*, EM*k*)	**2**

Si se aplica el algoritmo de Dijkstra desde el nodo R3 ¿Cuál sería la distancia a R2 una vez ejecutado el algoritmo completamente?
    a) 7.
    b) 15.
    c) 17.
    d) Ninguna de las anteriores.

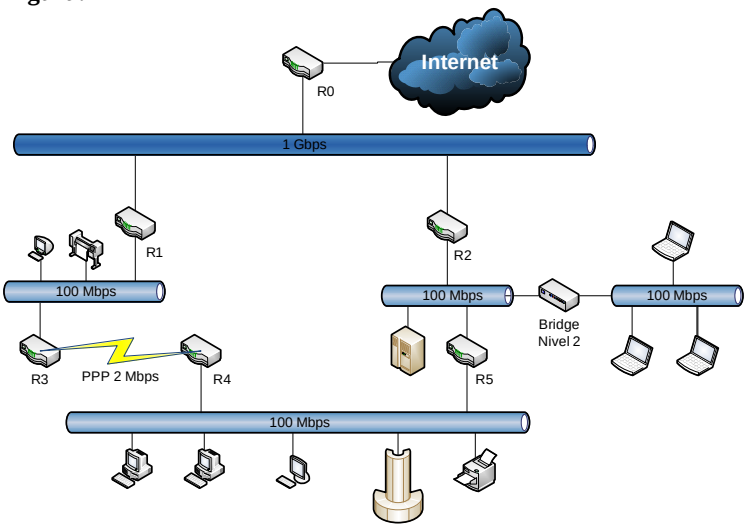
16. **¿Cómo se tiene consigue que la topología de la red esté almacenada en los nodos para poder aplicar el algoritmo de Dijkstra?**
    a) No hace falta saber la topología para aplicar el algoritmo de Dijkstra.
    b) Hay que configurarlo manualmente en cada uno de los nodos.
    c) Cada nodo envía a sus vecinos su vector de distancias al resto de la red.
    d) Ninguna de las anteriores.

17. **Se inicial el algoritmo de Dijkstra desde el nodo R3 y en un determinado momento de ejecución el conjunto N tiene los siguientes elementos:**
    N = {R3, EM1, R4}
    Indicar cuál de las siguientes afirmaciones es cierta:
    a) El algoritmo se está aplicando correctamente.
    b) Es incorrecto, no se está aplicando bien el algoritmo.
    c) Hace falta más información para saber si es correcto.
    d) Es imposible que el conjunto N tenga menos de 10 elementos.

18. **Se analiza también el posible protocolo IGP y se evalúa la posibilidad de utilizar RIP. Sin embargo, se teme que haya fragmentación debido a que la línea PPP entre los *routers* R3 y R4 es de sólo 2 Mbps. Indicar cuál de las siguientes observaciones es correcta:**
    a) Efectivamente, habrá fragmentación de los datagramas que lleven RIP encapsulado.
    b) Nunca habrá fragmentación si los bits TOS=0000.
    c) El que haya o no fragmentación de mensajes RIP dependerá sólo de que el bit de DF esté o no activado en la cabecera IP.
    d) No se puede saber, hace falta más información del nivel de enlace.

19. **¿Cuál sería la opción para implantar el *routing* basado en el estado de enlace?**
    a) OSPF.
    b) RIP.
    c) SMTP.
    d) SNMP.

20. Se pretende extender uno de los segmentos de la red utilizando un bridge de nivel 2 tal como se presenta en la figura:



¿Qué modificaciones habría que introducir en el grafo para aplicar el algoritmo de Dijkstra?

a) Un nuevo nodo idéntico a EM3.
b) Dos nuevos nodos idénticos a EM3.
c) Un nuevo nodo, parecido a EM3, pero con coste que refleje el retardo del bridge.
d) Ninguna de las anteriores.

21. Como alternativa a estado de enlaces, 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 en el que se basa el vector distancia.
b) Permite aliviar una situación de "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.

22. ¿En cuál de las siguientes situaciones es más probable que se dé un "conteo al infinito" en R1 y R2?

a) El valor de c(R0, EG) cambia a infinito.
b) El valor de c(R*j*, EM*k*) cambia a 100.
c) El valor de c(R1, EG) cambia a infinito.
d) Todos los valores de coste de los arcos se duplican.

23. Si se aplica en algoritmo de VD, ¿Cuál sería la tabla inicial del nodo R3?

Coste al destino vía

$D^{R3}()$	EM1	R4
R1	∞	∞
R2	∞	∞
R3	∞	∞
R4	∞	2
EM1	2	∞
EM2	∞	∞
EM3	∞	∞
EG	∞	∞

Destino

Tabla 1

Coste al destino vía

$D^{R3}()$	EM1	R3
R1	∞	∞
R2	∞	∞
R3	∞	∞
R4	∞	7
EM1	2	∞
EM2	∞	∞
EM3	∞	∞
EG	∞	∞

Destino

Tabla 2

Coste al destino vía

$D^{R3}()$	EM1	EM2
R1	∞	∞
R2	∞	∞
R3	∞	∞
R4	∞	5
EM1	2	∞
EM2	∞	∞
EM3	∞	∞
EG	∞	∞

Destino

Tabla 3

a) La tabla 1.
b) La tabla 2.
c) La tabla 3.
d) Ninguna de las anteriores.

24. Para conectar la topología anterior a otros sistemas se plantea la utilización de encaminamiento jerárquico. Indicar cuál sería la ventaja de su utilización:

a) Evita el problema de "cuenta al infinito".
b) Reduciría el tamaño de las tablas de encaminamiento.
c) Permitiría compatibilizar la arquitectura con DNS.
d) Optimizaría el número de saltos a cualquier destino.

CAPTURA: Responder a las siguientes preguntas en relación con la traza adjunta:

25. Según se puede observar del volcado de pantalla y del contenido de la traza, se trata de:

a) Una sesión de FTP para transferir un archivo de datos.
b) Una conexión remota TELNET para listar el contenido de un directorio.
c) Una simulación de envío de correo usando SMTP.
d) Ninguna de las anteriores.

26. El filtro que se ha utilizado para seleccionar los paquetes presentados es:

a) Sólo los paquetes ICMP.
b) Sólo los paquetes que tengan protocolo UDP o TCP.
c) Sólo los paquetes que tengan protocolo FTP de control.
d) Sólo los paquetes TELNET.

27. El valor de ASENT en la trama dos (2) es:

a) 0.
b) 1.
c) 2.
d) Ninguna de las anteriores.

28. Después de recibirse y procesarse la trama tres (3) en el destino, indicar cuál de las siguientes afirmaciones es cierta::

a) El sistema 15.201.57.23 podría enviar 8193 bytes de datos por el socket abierto sin necesidad de asentimiento.
b) El sistema 15.201.57.23 podría enviar 8192 bytes de datos por el socket abierto sin necesidad de asentimiento.
c) El sistema 16.38.10.126 ha abierto una ventana de 8191 bytes al otro extremo que la puede usar sin necesidad de asentimiento.
d) Ninguna de las anteriores.

29. ¿Cuál es el valor de LENGTH en la trama cuatro (4))?

a) 72.
b) 73.
c) 74.
d) Ninguna de las anteriores.

30. La trama cinco (5) tiene longitud cero (0) ¿Qué sentido tiene enviar una trama sin datos?:

a) Ninguno, es un error de protocolo.
b) Sirve para asentir los datos de la trama cuatro (4).
c) El único propósito es impedir que aparezca el síndrome de la "ventana tonta".
d) Ninguna de las anteriores.

31. La herramienta de traza indica que el tiempo que transcurre entre la trama cinco (5) y la trama seis (6) es significativamente mayor que el que transcurre entre las tramas anteriores. ¿Por qué puede ocurrir esto?

a) Puede haber una congestión en las comunicaciones que retrase la recepción de tramas.
b) El sistema donde se ejecuta el comando FTP está sobrecargado de manera transitoria debido al envío de los segmentos anteriores.
c) Es el tiempo que el usuario tarda en teclear el identificador: "anonymous".
d) Ninguna de las anteriores.

32. En la trama siete (7) se recibe un código de respuesta 331. ¿Qué significa este código?

a) Que el comando USER se ha realizado completamente y ya se puede empezar a transferir archivos.
b) Que el comando USER ha provocado un error transitorio que se arreglará si se ejecuta correctamente el siguiente comando .
c) Que el comando USER se ha realizado con éxito parcial, pues queda algo más por hacer.
d) Ninguna de las anteriores.

33. ¿Qué significa la cadena de caracteres "`access restrictions apply`" que se recibe con la trama diez(10) ?

a) Que el sistema cliente tiene restringidos los puertos a los que se puede conectar.
b) Que el sistema servidor de FTP está en la zona desmilitarizada (DMZ).
c) Que se va a realizar una apertura pasiva para evitar los cortafuegos (firewalls).
d) Ninguna de las anteriores.

34. ¿Qué puerto está indicando el comando PORT de la trama doce (12)?

a) 59.832.
b) 47.337.
c) 417.
d) Ninguna de las anteriores.

35. En la trama catorce (14) aparece claramente el envío del comando LIST, que es asentido correctamente por la trama quince (15). Sin embargo, no aparece en la traza por ningún sitio el listado del directorio que se puede ver en el volcado de pantalla. ¿Qué ha pasado?

a) Es un error, tendría que estar la trama con el contenido del directorio como parte de la misma conexión.
b) No aparece porque lo que se está listando es el directorio local del sistema cliente.
c) No aparece porque esta información se envía por otra conexión distinta a la que ha muestreado la herramienta de traza.
d) Ninguna de las anteriores.

36. ¿Es correcto el valor de asentimiento de `Ack=493` de la trama veinticuatro (24)?

a) Si, ya que es igual al número de secuencia más el tamaño de la trama que está asintiendo más uno.
b) No, tiene que ser la suma del número de secuencia más el tamaño de la trama que está asintiendo.
c) Es correcto. Lo que ocurre es que la herramienta no está presentando que la trama veintitrés (23) tiene el flag de FIN activado.
d) No, tiene que ser la suma del número de secuencia más el tamaño de la trama que está asintiendo menos 1.

37. ¿Qué hacen las últimas tramas de la traza?

a) Cierran la conexión definida por puerto 21 y dirección IP 15.201.57.23 en un extremo, y puerto 59830 dirección IP 16.38.10.126 en el otro, y protocolo TCP.
b) Cierran la conexión definida por puerto 21 y dirección IP 15.201.57.23 en un extremo, y puerto 20 dirección IP 16.38.10.126 en el otro, y protocolo TCP.
c) Cierran la conexión definida por puerto 21 y dirección IP 15.201.57.23 en un extremo, y puerto 59830 dirección IP 16.38.10.126 en el otro, y protocolo UDP.
d) Ninguna de las anteriores.

38. Si se asume que el ancho de banda de transmisión es el que indica el volcado de pantalla (237,20Kbytes/sec), y asumiendo una ventana ofrecida por el cliente de 8192 bytes. ¿Cuál sería el valor máximo de RTT (aproximado) para que la velocidad media de transmisión desde el servidor al cliente no estuviese limitada por dicha ventana (8192 bytes)?

a) 550 milisegundos
b) 5 segundos
c) 33 milisegundos
d) La ventana indicada nunca puede limitar la velocidad media de transmisión del servidor al cliente Depende de la ventana que ofrezca el servidor

39. Considerando la información completa de la traza, ¿Cuál es la dirección física del sistema 15.201.57.23?

a) **`00:11:bb:eb:9f:c2`**.
b) **`00:00:0c:07:ac:66`**.
c) A veces **`00:00:0c:07:ac:66`** y a veces **`00:11:bb:eb:9f:c2`**.
d) No puede saberse.

Arquitectura de redes I Tutoría 12 de enero de 2012 16:00

APÉNDICE

Datos correspondientes a la CAPTURA:

Volcado de pantalla:

```
C:\Users\jose>ftp www.co.com
Connected to www.cogtm.nsatc.net.
220 g4u1138.houston.co.com FTP server (co.com version wco02s_p1)
ready.
User (www.cogtm.nsatc.net:(none)): anonymous
331 Guest login ok, send your complete e-mail address as
password.
Password:
230 Guest login ok, access restrictions apply.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 8
drwxr-xr-x  16 32227      4436          1024 May  6 20:34 .
drwxr-xr-x  16 32227      4436          1024 May  6 20:34 ..
drwxr-xr-x   2 2          2               96 Nov 21  2008 bin
drwxrwxr-x   2 32226      4436          1024 May 12  2009 control
drwxrwxr-x   2 32227      4436            96 Sep 14  2007 dist
dr-xr-xr-x   4 0          3             1024 Sep 23  2003 etc
drwxr-xr-x   5 32227      4436            96 Mar  6  2009 ftp1
drwxr-xr-x   5 32227      4436            96 Mar  6  2009 ftp2
drwxr-xr-x   5 32227      4436            96 Mar  6  2009 ftp3
drwxr-xr-x   4 32227      4436            96 Apr  5  2009 ftp4
drwxr-xr-x   4 32227      4436            96 Sep 10  2009 ftp5
drwxr-xr-x   4 32227      4436            96 Sep 10  2009 ftp6
drwxrwxr-x   4 32227      4436            96 May  7 19:17 ftp7
drwxrwxr-x   4 32227      4436            96 May  7 19:17 ftp8
drwxr-xr-x   2 0          0               96 Mar  2  2009
lost+found
lrwxrwxr-x   1 32227      4436             8 Mar  6  2009 pub ->
ftp1/pub
lrwxrwxr-x   1 32227      4436             9 Mar  6  2009 save ->
ftp1/save
dr-xr-xr-x   4 2          2               96 Nov 21  2008 usr
226 Transfer complete.
ftp: 1186 bytes received in 0,01Seconds 237,20Kbytes/sec.
ftp> quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1593 bytes in 1 transfers.
221-Thank you for using the FTP service on
g4u1138.houston.co.com.
221 Goodbye.

C:\Users\jose>ftp www.co.com
```

Traza correspondiente:

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    16.38.10.126          15.201.57.23          TCP      59830 > ftp [SYN] Seq=0 Win=8192
Len=0 MSS=1460 WS=2

Frame 1 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 0, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
      2 0.139290    15.201.57.23          16.38.10.126          TCP      ftp > 59830 [SYN, ACK] Seq=0
Ack=ASENT Win=32768 Len=0 MSS=1380 WS=0

Frame 2 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 0, Ack:ASENT, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
      3 0.139361    16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=1 Ack=1
Win=8192 Len=0

Frame 3 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
      4 0.289330    15.201.57.23          16.38.10.126          FTP      Response: 220
g4u1138.houston.co.com FTP server (co.com version wco02s_p1) ready.

Frame 4 (127 bytes on wire, 127 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 1, Ack: 1, Len:LENGTH
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
      5 0.489365    16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=1 Ack=74
Win=8116 Len=0

Frame 5 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 1, Ack: 74, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
      6 11.807442   16.38.10.126          15.201.57.23          FTP      Request: USER anonymous

Frame 6 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 1, Ack: 74, Len: 16
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
      7 11.947994   15.201.57.23          16.38.10.126          FTP      Response: 331 Guest login ok,
send your complete e-mail address as password.

Frame 7 (122 bytes on wire, 122 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 74, Ack: 17, Len: 68
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
      8 12.142083   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=17 Ack=142
Win=8048 Len=0

Frame 8 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 17, Ack: 142, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
      9 24.904079   16.38.10.126          15.201.57.23          FTP      Request: PASS jose.tomas@co.com

Frame 9 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 17, Ack: 142, Len: 24
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     10 25.042723   15.201.57.23          16.38.10.126          FTP      Response: 230 Guest login ok,
access restrictions apply.

Frame 10 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 142, Ack: 41, Len: 48
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     11 25.237781   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=41 Ack=190
Win=8000 Len=0

Frame 11 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 41, Ack: 190, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     12 31.864992   16.38.10.126          15.201.57.23          FTP      Request: PORT
16,38,10,126,233,184

Frame 12 (81 bytes on wire, 81 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 41, Ack: 190, Len: 27
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     13 32.002171   15.201.57.23          16.38.10.126          FTP      Response: 200 PORT command
successful.

Frame 13 (84 bytes on wire, 84 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 190, Ack: 68, Len: 30
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     14 32.006899   16.38.10.126          15.201.57.23          FTP      Request: LIST

Frame 14 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 68, Ack: 220, Len: 6
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     15 32.209137   15.201.57.23          16.38.10.126          TCP      ftp > 59830 [ACK] Seq=220 Ack=74
Win=32768 Len=0

Frame 15 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 220, Ack: 74, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     16 32.329145   15.201.57.23          16.38.10.126          FTP      Response: 150 Opening ASCII mode
data connection for /bin/ls.

Frame 16 (107 bytes on wire, 107 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 220, Ack: 74, Len: 53
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     17 32.522193   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=74 Ack=273
Win=7920 Len=0

Frame 17 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 74, Ack: 273, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     18 32.658170   15.201.57.23          16.38.10.126          FTP      Response: 226 Transfer complete.

Frame 18 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 273, Ack: 74, Len: 24
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     19 32.852214   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=74 Ack=297
Win=7896 Len=0

Frame 19 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 74, Ack: 297, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     20 38.000494   16.38.10.126          15.201.57.23          FTP      Request: QUIT

Frame 20 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 74, Ack: 297, Len: 6
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     21 38.137497   15.201.57.23          16.38.10.126          FTP      Response: 221-You have
transferred 0 bytes in 0 files.

Frame 21 (100 bytes on wire, 100 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 297, Ack: 80, Len: 46
File Transfer Protocol (FTP)
```

```
No.     Time        Source                Destination           Protocol Info
     22 38.328587   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=80 Ack=343
Win=7848 Len=0

Frame 22 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 80, Ack: 343, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     23 38.465480   15.201.57.23          16.38.10.126          FTP      Response: 221-Total traffic for
this session was 1593 bytes in 1 transfers.

Frame 23 (203 bytes on wire, 203 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 343, Ack: 80, Len: 149
```

```
No.     Time        Source                Destination           Protocol Info
     24 38.465585   16.38.10.126          15.201.57.23          TCP      59830 > ftp [ACK] Seq=80 Ack=493
Win=7700 Len=0

Frame 24 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 80, Ack: 493, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     25 38.474484   16.38.10.126          15.201.57.23          TCP      59830 > ftp [FIN, ACK] Seq=80
Ack=493 Win=7700 Len=0

Frame 25 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CompnyP_d2:be:53 (18:a9:05:d2:be:53), Dst: All-HSRP-routers_66 (00:00:0c:07:ac:66)
Internet Protocol, Src: 16.38.10.126 (16.38.10.126), Dst: 15.201.57.23 (15.201.57.23)
Transmission Control Protocol, Src Port: 59830 (59830), Dst Port: ftp (21), Seq: 80, Ack: 493, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
     26 38.613509   15.201.57.23          16.38.10.126          TCP      ftp > 59830 [ACK] Seq=493 Ack=81
Win=32768 Len=0

Frame 26 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_eb:9f:c2 (00:11:bb:eb:9f:c2), Dst: CompnyP_d2:be:53 (18:a9:05:d2:be:53)
Internet Protocol, Src: 15.201.57.23 (15.201.57.23), Dst: 16.38.10.126 (16.38.10.126)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 59830 (59830), Seq: 493, Ack: 81, Len: 0
```

Arquitectura de redes I Modelo 1 Examen Final 14 de Enero de 2012 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. **¿Cuántas direcciones IP se pueden utilizar para asignarlas a equipos (hosts o routers) en una subred con máscara 255.255.255.224?**
   a) 222.
   b) 32.
   c) 31.
   d) 30.
2. **¿Qué campo de la cabecera IP mide octetos en múltiplos de ocho?**
   a) Longitud de la cabecera.
   b) Longitud del datagrama.
   c) Offset.
   d) TTL.
3. **¿Cuál de los siguientes casos no podría ocurrir en los bits de fragmentación de la cabecera IP?**
   a) DF=0, MF=0.
   b) DF=0, MF=1.
   c) DF=1, MF=0.
   d) DF=1, MF=1.
4. **Los tipos de mensajes ICMP que se utilizan en el comando ping sin opciones son:**
   a) Echo-request y echo-reply.
   b) Echo-request, time-exceeded y echo-reply.
   c) Echo-request, source-quench y echo-reply.
   d) Ping-request y pong-reply.
5. **¿Cuál de las siguientes afirmaciones es correcta respecto de algoritmos de encaminamiento?**
   a) El encaminamiento por inundación es el método que menos recursos utiliza.
   b) En estado de enlaces, cada nodo obtiene la topología completa de la red.
   c) En vector de distancia, cada nodo obtiene la topología completa de la red.
   d) Ninguna de las anteriores.
6. **Respecto de los protocolos de encaminamiento existentes:**
   a) RIP tiene el problema de cuenta al infinito.
   b) BGP tiene el problema de cuenta al infinito.
   c) OSPF tiene el problema de cuenta al infinito.
   d) Ninguna de las anteriores.
7. **Por qué no es UDP un protocolo orientado a conexión?**
   a) Porque IP no es orientado a conexión.
   b) Porque no numera los datagramas.
   c) Porque el checksum es opcional.
   d) UDP sí es un protocolo orientado a conexión.

- UDP no numera datagramas
- No usa ventana de recepción
- Keepalive no
- ISN

8. **¿Cuánto vale el número de secuencia inicial o ISN de TCP?**
   a) Siempre 0.
   b) Siempre 1.
   c) Un valor aleatorio.
   d) El ISN no es de TCP.
9. **¿Cuál de los siguientes mecanismos de TCP está pensado para evitar que un emisor rápido desborde a un receptor lento?**
   a) La ventana de congestión.
   b) La ventana del receptor.
   c) La recuperación rápida.
   d) La prevención de congestión.
10. **¿Cuál de los siguientes temporizadores de TCP es el que se emplea para mantener una conexión que no ha transmitido datos durante un largo periodo de tiempo?**
    a) 2MLS.
    b) RTO.
    c) Persist.
    d) Keepalive.
11. **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 segundo nivel.
    d) Un dominio invalido.
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.

PROBLEMA

La figura incluida en el apéndice muestra la topología de la red de una compañía. Se utilizan direcciones privadas en las subredes A, B, C, D, y los enlaces PPP, excepto los enlaces a Internet, que usan las direcciones públicas proporcionadas por el ISP. La red no tiene ningún proxy de ARP. Los datagramas IP no llevan opciones.

13. **El protocolo de encaminamiento de los routers se basa en el algoritmo de estado de enlaces. Los routers troncales anuncian los siguientes valores de los estados de sus enlaces, obtenidos como el retardo RTT en ms:**

R_A	
R_B	2.4
R_C	2.4
R_D	2.4
R_I	0.02
R_K	0.02

R_B	
R_A	2.4
R_C	12

R_C	
R_A	2.4
R_B	12
R_D	12

R_D	
R_A	2.4
R_C	12

¿Cuál sera el path MTU entre B_1 y C_1?
   a) 9000 bytes.
   b) 1500 bytes.
   c) 1400 bytes.
   d) 576 bytes.
14. **¿Qué ocurrirá si uno de los enlaces PPP entre los routers troncales fallase?**
    a) Existen suficientes enlaces redundantes. Seguiría habiendo conectividad entre todos los equipos de la red.
    b) Ningún ordenador en las subredes que se conectan a través de dicho enlace podrá comunicarse con el resto de la red.
    c) El algoritmo de estado de enlaces contará hasta el infinito.
    d) Ninguna de las anteriores.

15. **El ordenador B_1 envía un datagrama IP a C_1 con el TTL puesto a 2. ¿Qué nodo enviará de vuelta un mensaje ICMP de error a B_1?**
    a) R_B.
    b) R_C.
    c) R_A.
    d) Ninguno, el mensaje alcanzará su destino.
16. **El datagrama UDP de B_1 a C_1 contiene 5000 bytes de datos del nivel de aplicación. Si no se pierden paquetes, ¿cuántos fragmentos llegarán a C_1?**
    a) 4.
    b) 7.
    c) 11.
    d) Ninguna de las anteriores.
17. **Se han asignado direcciones consecutivas a los enlaces PPP entre los routers troncales para permitir reducir las entradas de las tablas de rutas de R_I y R_K. ¿Cuál será la mascara que agrupe dichas subredes (enlaces PPP entre los routers troncales) utilizando el mínimo número de direcciones IP? Considere que las direcciones se han asignado correctamente para permitir este agrupamiento. Suponga la misma métrica a todos los enlaces.**
    a) 255.255.255.252.
    b) 255.255.255.248.
    c) 255.255.255.240.
    d) 255.255.255.224.
18. **Además de los routers del dibujo, la subred A tiene otros 12 ordenadores conectados a la misma, incluyendo entre estos a A_1, DNS y Mail. ¿Cuál será la mascara más adecuada que minimiza el número de direcciones IP en dicha subred?**
    a) 255.255.255.248.
    b) 255.255.255.240.
    c) 255.255.255.224.
    d) 255.255.255.192.
19. **El ordenador A_1 tiene configurada incorrectamente su mascara de red a 255.255.255.0. ¿Qué puede ocurrir?**
    a) Podrá recibir cualquier datagrama IP, pero es posible que no pueda enviar datagramas a algunos ordenadores de la red de la empresa.
    b) Podrá enviar cualquier datagrama IP, pero es posible que no pueda recibir datagramas de algunos ordenadores de la red de la empresa.
    c) No podrá enviar ni recibir datagrama IP alguno a/de cualquier ordenador de la red de la empresa.
    d) Podrá enviar y recibir cualquier datagrama IP a/de cualquier ordenador de la red de la empresa.
20. **El retardo RTT entre B_1 y R_B, así como entre C_1 y R_C, es aproximadamente 0.24 ms. Considerando además los retardos proporcionados por el protocolo de estado de enlaces (ver 8 preguntas hacia atrás), ¿cuál es el valor mínimo que se debe ofrecer de ventana TCP en una conexión entre B_1 y C_1 que permita envío continuo? Tenga en cuenta el ancho de banda más bajo en la ruta que se está utilizando entre B_1 y C_1.**
    a) 3120 bytes.
    b) 6600 bytes.
    c) 24960 bytes.
    d) 52800 bytes.
21. **B_1 realiza un descubrimiento del path MTU hasta C_1 para evitar fragmentación en los segmentos de TCP. Según esto, ¿cuál será el tamaño máximo de segmento que pueda haber en dicha conexión?**
    a) 1500 bytes.
    b) 1460 bytes.
    c) 1400 bytes.
    d) 1360 bytes.
22. **Se necesita estimar el RTT en la conexión entre B_1 y C_1. El esquema utilizado solo tiene en cuenta la forma más sencilla de Estimar el RTT (RFC 793), y no el de Jacobson. ¿Cuál será aproximadamente la estimación si el RTT permanece estable?**
    a) 10.6 ms.
    b) 21 ms.
    c) 25 ms.
    d) Ninguna de las anteriores.

23. **Se instala un software para hacer NAT/NATP en los routers de salida a Internet, tanto en R_I como R_K. El servidor de DNS únicamente contiene direcciones privadas, y el servidor de correo se utiliza tanto para enviar como para recibir mensajes de correo electrónico.**
    a) Se necesitará añadir dos reglas en los routers para que los sistemas externos puedan acceder a los servidores: una para permitir consultas externas al servidor de DNS y otra para permitir conexiones entrantes al servidor de SMTP.
    b) Se necesitará añadir solo una regla en los routers, para permitir conexiones entrants al servidor SMTP.
    c) Se necesitará añadir solo una regla en los routers, para permitir consultas externas al servidor de DNS.
    d) No se necesitará añadir ninguna regla en los routers.
24. **Se instala un servidor proxy-cache de web en la subred A, para permitir una navegación web más rápida. Sin embargo, los usuarios de toda la red no notan una mejora significativa en la velocidad de descarga. ¿Qué puede estar sucediendo?**
    a) El número de mensajes "304 Not Modified" recibidos en el servidor proxy-cache es muy pequeño.
    b) El número de mensajes "304 Not Modified" recibidos en los clientes web es muy pequeño.
    c) Un servidor proxy-cache no está pensando para mejorar la velocidad de descarga, sino para reducir la latencia de los paquetes.
    d) Se necesitaría haber añadido una regla en la tabla de NAPT

TRAZA

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

25. **¿En qué subred se encuentra el servidor de FTP?**
    a) En la misma subred que el cliente.
    b) En una subred de la misma organización distinta a la subred del cliente.
    c) En una subred de otra organización.
    d) Con los datos aportados no puede saberse.
26. **¿Cuál de las siguientes máscaras de subred podría estar usando la máquina cliente?**
    a) 255.255.252.0
    b) 255.255.254.0
    c) 255.255.255.0
    d) 255.255.255.128
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 el flag de SYN activado.
    c) Porque el segmento anterior llevaba un byte de datos.
    d) Se trata de un error al decodificar el segmento, puesto que el asentimiento debería ser 0.
29. **¿En qué estado se encuentra la conexión TCP en el servidor tras la trama 8?**
    a) LISTEN
    b) SYN_RCVD
    c) SYN_SENT
    d) ESTABLISHED
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) 1145
    b) 1141
    c) 4121
    d) 30980

32. **¿Qué valor debe tener el número de secuencia descrito en la captura como "SECUENCIA" (tramas 28, 29)?**
    a) 272
    b) 273
    c) 227
    d) 46
33. **¿De qué tipo son los mensajes de las tramas 29 y 31?**
    a) Inicio de una acción.
    b) Comando realizado.
    c) Errores pasajeros.
    d) Errores permanentes.
34. **¿Por qué no se establece la conexión de datos correctamente?**
    a) El servidor debe tener activado un mecanismo de filtrado de paquetes (cortafuegos) y no admite conexiones entrantes.
    b) El cliente debe tener activado un mecanismo de filtrado de paquetes (cortafuegos) y no admite conexiones entrantes.
    c) 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.
    d) El servidor se encuentra detrás de un router que hace NAPT, y la conexión saliente no se corresponde con ningún puerto registrado.
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 la forma habitual de semi-cierre de conexiones en TCP.
    b) Es para cerrar la conexión de datos que se abrió de forma incorrecta.
    c) Es para cerrar la conexión de control que permanecía abierta y sin actividad del cliente.
    d) Es para provocar un asentimiento del cliente, siguiendo el algoritmo de keepalive.

FIN DEL EXAMEN

Arquitectura de Redes I Modelo 1

Examen Final 14 de Junio de 2012 15:00

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.

CAPTURA : Responder a las siguientes preguntas en relación con la traza adjunta:

---

1. **¿Cuántos segmentos de solicitud de conexión de TCP se han registrado?**
   a) Dos
   b) Tres
   c) Cuatro
   d) Ninguna de las anteriores

2. **El filtro que se ha utilizado para seleccionar los paquetes presentados es:**
   a) Sólo los paquetes ICMP
   b) Sólo los paquetes que tengan protocolo UDP o TCP
   c) Sólo los paquetes que tengan protocolo DNS
   d) Sólo los paquetes TCP

3. **La trama número cuatro (4) se corresponde con:**
   a) El cierre de una conexión TCP
   b) Un error en la herramienta de traza
   c) Que la aplicación desea abortar la conexión TCP
   d) Ninguna de las anteriores

4. **El valor de "ACK" en la trama ocho (8) es:**
   a) No puede saberse
   b) 0
   c) 1
   d) Ninguna de las anteriores

5. **¿En qué estado queda TCP en el sistema 88.30.180.33 después de enviar la trama ocho (8)?**
   a) SYN_SENT
   b) SYN_RCVD
   c) LISTEN
   d) Ninguna de las anteriores

6. **El valor de "LONGITUD" en la trama doce (12) es:**
   a) 1419
   b) 1493
   c) No puede saberse
   d) Ninguna de las anteriores

7. **En el momento de enviarse la trama diez (10) ¿Cuántas conexiones TCP abiertas hay en 88.30.180.33?**
    a) Tres
    b) Dos
    c) Una
    d) Ninguna de las anteriores

8. **La trama seis (6) se corresponde con una respuesta DNS a una petición que no está en la traza. Suponiendo que se hubiesen guardado los paquetes anteriores a esta traza. ¿Cómo se podría identificar la pregunta correspondiente?**
    a) Por los puertos UDP origen y destino, que deben ser los mismos
    b) Buscando el valor "0x879" en los mensajes DNS
    c) No hay manera de relacionar pregunta y respuesta en DNS
    d) Ninguna de las anteriores

9. **¿Por qué se reciben respuestas DNS desde dos direcciones IP diferentes?**
    a) Porque hay configurados un servidor primario y uno secundario
    b) Porque el cliente siempre solicita la información por duplicado
    c) Es imposible que se reciban respuestas DNS desde dos direcciones IP distintas, es un error de la herramienta de traza
    d) Ninguna de las anteriores

10. **A la vista de los mensajes DNS registrados ¿qué es lo más probable que esté haciendo el usuario?**
    a) Generar una copia de seguridad de los datos del disco duro en la red
    b) Se está intentando acceder a servidores de Internet que no existen
    c) Está intentando enviar un correo usando el protocolo SMTP
    d) Ninguna de las anteriores

11. **¿Cuántas preguntas DNS ha realizado como mínimo el sistema 88.30.180.33 antes de comenzar la traza?**
    a) Una
    b) Dos
    c) Tres
    d) Cuatro

12. **El valor de los flags de la cabecera TCP en la trama diez (10) es de 0x18. Este valor indica que la aplicación que ha generado el segmento solicita en relación con los datos contenidos en el mismo:**
    a) Que están cifrados a nivel de aplicación
    b) Que deben ser entregados cuanto antes a la aplicación
    c) Que no consumen toda la ventana disponible
    d) No significa nada a nivel de datos

CUESTIONES

13. **¿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
14. **¿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.
15. **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

16. **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

17. **¿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.

18. **¿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.

19. **¿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.

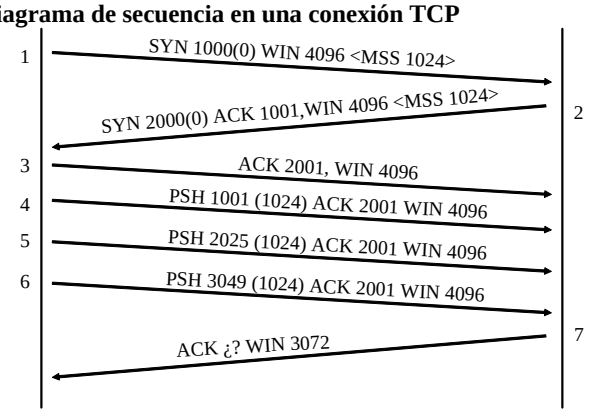
20. **Un usuario está utilizando para acceder a su correo. una aplicación webmail disponible comercialmente y que está conectada a un servidor externo a través de un cortafuegos que solo deja pasar paquetes con destino al puerto 80 ¿Qué protocolo o protocolos se estarán empleando en el ordenador de dicho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

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

22. **En el diagrama de estados de TCP, indicar cual 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

23. **¿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

24. Dado el siguiente diagrama de secuencia en una conexión TCP



¿Cuánto debe valer el último ACK (segmento 7)?

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

PROBLEMA

Las siguientes preguntas hacen referencia a la red que se presenta en la figura del anexo. Seguir el criterio de no asignar direcciones de subred o de nodo "todo a ceros" ni "todo a unos"

25. Dado el coste de adquirir direcciones IP públicas, se usará direccionamiento privado en la red, en particular un rango de direcciones IP privadas de clase C. Este rango se dividirá en subrangos de igual tamaño: Uno para el backbone, otro para la subred de servicios TI, otro para el departamento de producción, y finalmente, otro para el laboratorio. Considerando que en la red sólo hay las máquinas que aparecen en la figura, ¿Cuál de las siguientes afirmaciones es cierta?

a) Se puede usar el rango 192.168.200.0/24
b) Se puede usar el rango 10.0.0.0/16
c) La red tiene demasiadas máquinas como para que sea posible usar una única clase C
d) Ninguna de las anteriores

26. Se decide que la subred de backbone tenga la máscara 255.255.255.192 ¿Cuál sería entonces la máscara de red de estas subredes P1, P2 y Wireless?

a) 255.255.255.248
b) 255.255.255.240
c) 255.255.255.224
d) 255.255.255.192

27. Para hacer la conexión con Internet, el router R0 implementará NAT y NATP. Se contratará una única dirección IP pública para la salida de R0, y se desea dar hacia el exterior servicios de Web (localizado en el servidor S5), correo SMTP (localizado en el servidor S4) y FTP (localizado en el servidor P4). ¿Es esto posible?

a) Si, pero hay que configurar el NATP del router R0 adecuadamente
b) Si, pero siempre que los tres servicios se centralicen en un mismo servidor
c) No, sería necesario contratar 3 direcciones IP públicas adicionales, una por servicio
d) No, los servidores accesibles desde Internet nunca pueden usar direcciones privadas

28. En la sección de diseño se corren simulaciones complejas en el superordenador. Estas simulaciones generan volúmenes de datos grandes (50 GBytes) que se mandan por FTP a la máquina donde está trabajando el ingeniero de diseño. Para ello se ha planteado usar Gigabit Ethernet en todas las subredes del laboratorio. El retardo (RTT) desde el superordenador a una estación de diseño es pequeño, de 2 milisegundos , y se mantiene constante durante la conexión. No se observa pérdida de paquetes. Sin embargo, el envío de los datos tarda 100 minutos, mucho más de lo esperado. ¿A qué puede deberse esto?

a) A que el ancho de banda alcanzable por FTP es limitado
b) A que la MTU es demasiado grande
c) A que la ventana de TCP del receptor no es suficientemente grande
d) Ninguna de las anteriores

29. **Se contrata el dominio "empresa.es", y se decide usar los nombres "www.empresa.es", "smtp.empresa.es" y "ftp.empresa.es" para los tres servicios que se van a dar hacia Internet. Considerando que el servidor DNS que hay dentro de la red sólo tiene almacenadas las direcciones privadas de los nodos, indicar cual de las siguientes afirmaciones es correcta:**
    a) Puede usarse el servidor DNS que hay dentro de la red, configurando el NATP adecuadamente
    b) No se puede hacer, porque los nombres de dominio apuntan a direcciones privadas de los servidores
    c) Se puede hacer sólo si se contratan 4 direcciones IP públicas, una para cada servidor y otra para el router
    d) Se puede hacer con un servidor DNS externo y usando alias, pues los tres nombres de dominio apuntarán a la misma dirección IP pública

30. **¿Cuántas entradas tendrá en su tabla de encaminamiento el router R1 referidas a las redes del departamento de producción? Considerar que se pueden agrupar subredes y que la única información almacenada en cada entrada de la tabla es destino, máscara y gateway.**
    a) Con una es suficiente
    b) Dos: una para la red troncal de producción, y otra para sus subredes
    c) Tres: P1, P2 y Wireless
    d) Cuatro: P1, P2, Wireless y una adicional para la red troncal de producción

31. **La empresa tiene dos talleres en una localización remota, a los que hay que enviar los planos de producción, que son archivos grandes (10 GBytes). Para ello se decide contratar un enlace vía satélite, que es unidireccional. Además se añade un enlace telefónico bidireccional de 56 Kbps para cada taller. ¿Sería posible mandar los planos por FTP?**
    a) No, porque el enlace vía satélite es unidireccional y por tanto sólo puede encaminar paquetes UDP
    b) Si, pero habría que hacerlo exclusivamente por los enlaces telefónicos que son muy lentos
    c) Si, y se podría mejorar la velocidad si se utilizase en los talleres un router que fuese capaz de recibir los datagramas IP por el enlace satélite y enviarlos por el enlace telefónico
    d) FTP nunca podría funcionar con esta configuración, pero HTTP si, así que se podrían leer los planos por ejemplo en una página web

32. **Suponer que el enlace vía satélite se puede hacer bidireccional, con lo que los problemas de la pregunta anterior ya no tienen sentido. Considerar que cada uno de los talleres tiene dos direcciones IP, una privada para el enlace por satélite (Sat_1 y Sat_2) y otra pública para el telefónico. Para probar el funcionamiento de las comunicaciones, en el router R2 se configura la siguiente tabla de encaminamiento:**

Destination	Gateway	Flags	Interface
Loopback	Loopback	UH	lo0
Sat_1	R4	UGH	le0
Sat_2	R4	UGH	le0
Backbone	R2	U	le0
Producción	R2	U	le1
Default	R0	UG	le0

Indicar cuál de las siguientes respuestas es la correcta en relación con el tráfico que pasa por R2:

    a) Todo el tráfico hacia los talleres irá por los enlaces telefónicos, no pudiendo en ningún caso usarse el enlace por satélite
    b) Dependiendo de la dirección IP de destino de un datagrama dirigido a un taller, se usará el enlace telefónico o el enlace vía satélite
    c) Todo el tráfico hacia los talleres irá por el enlace vía satélite no pudiendo en ningún caso usarse el enlace por teléfono
    d) Ninguna de las anteriores

33. **Se acaba el presupuesto asignado para la dirección IP fija, y se plantea pasar a una conexión a Internet a través de ADSL de bajo coste, que tiene dirección IP pública asignada dinámicamente. ¿Es esto posible?**
    a) Si, todo seguiría funcionando igual sin cambiar la configuración de los equipos de la red.
    b) Si, el acceso a Internet desde la red interna seguiría funcionando, pero sería un problema continuar dando servicio de Web, SMTP y FTP hacia el exterior
    c) No porque ADSL no permite que haya subredes detrás del router de acceso
    d) Ninguna de las anteriores

34. **Se ha descubierto una vulnerabilidad en el superordenador de la red de cálculo (C2), en particular en el servidor HTTP que tiene para monitorizar su estado vía Web, por lo que es posible tomar posesión de la máquina a partir de una sesión Web. ¿Es preocupante esta vulnerabilidad?**
    a) Si, mucho, porque cualquiera desde Internet podría entrar directamente en el superordenador
    b) Es moderadamente preocupante, porque este ataque sólo se puede hacer desde máquinas de dentro de la red
    c) No, porque este ataque no puede ocurrir nunca con esta configuración de red
    d) Si, y la solución óptima es añadir una regla al firewall del router R0 para que tire todos los paquetes con destino el puerto 80

35. **Para mejorar la fiabilidad de la red, se decide añadir un par de routers más, respectivamente entre la subred de servicios TI y la subred troncal de producción, y entre las subredes troncales de producción y del laboratorio. Se pasa a usar RIP como protocolo de encaminamiento dinámico. ¿Qué pasa si cae el router R3?**
    a) Se produce el problema de conteo al infinito
    b) Se detecta rápidamente un nuevo camino alternativo a través de producción
    c) Se pierde la conexión con Internet pero no con el resto de la empresa
    d) En esta topología de red no se puede usar RIP

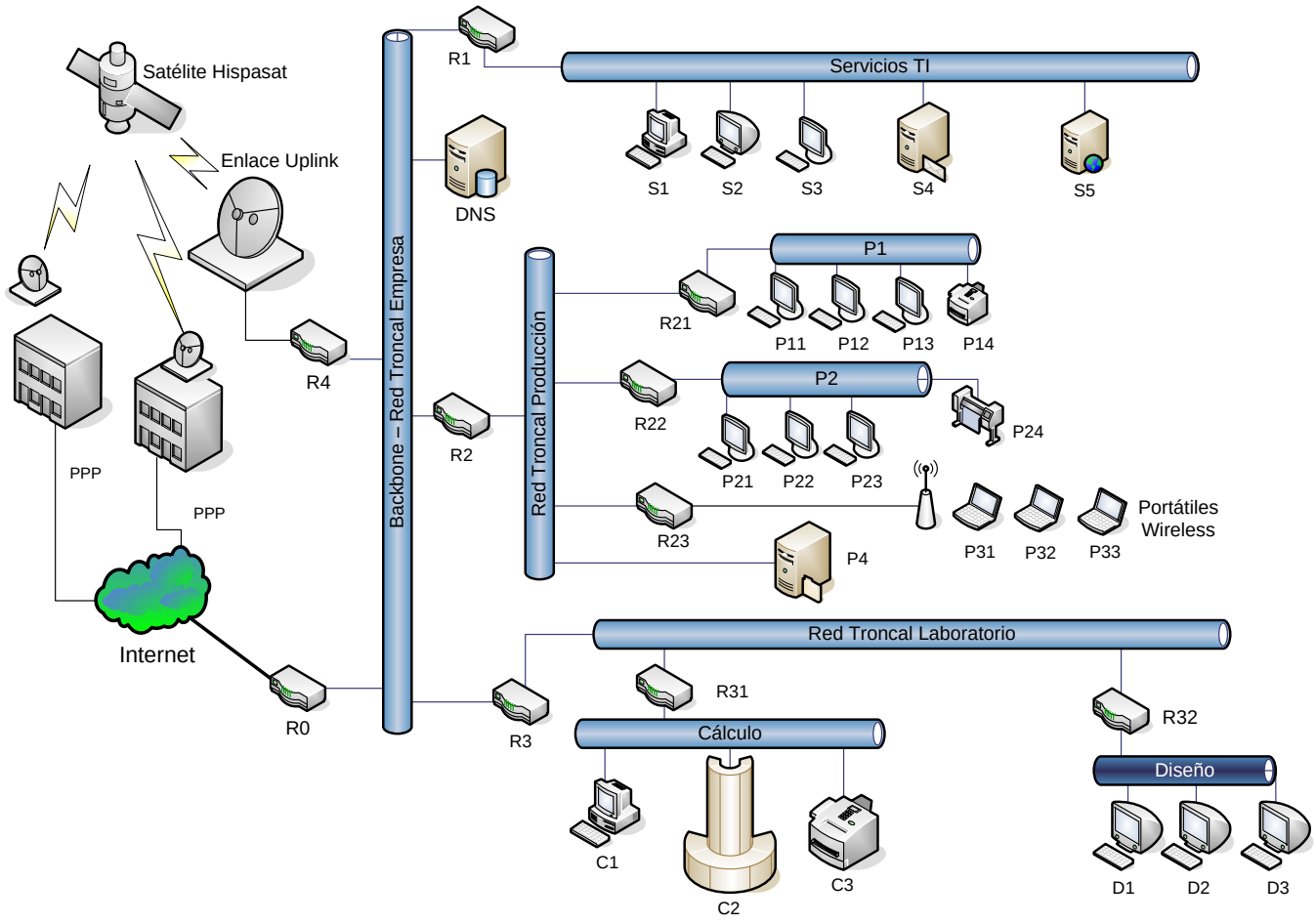
36. **Se ha observado que el tiempo de encaminamiento de los datagramas IP en los routers es aproximadamente independiente del tamaño de los datos. ¿Cuál de las siguientes alternativas mejoraría más el throughput de la red?**
    a) Aumentar la MTU hasta el máximo que sea posible
    b) Disminuir la MTU hasta alcanzar las prestaciones necesarias
    c) Reducir el MSS al mínimo posible
    d) Evitar el uso de opciones de escala de ventana en la cabecera TCP

Arquitectura de Redes I Todos los modelos

Examen Final 14 de Junio de 2012 15:00

APÉNDICE

Figura correspondiente al PROBLEMA:



Datos correspondientes a la CAPTURA :

1	No. Time Source Destination Protocol Info 1 0.000000 88.30.180.33 16.46.57.86 TCP jvserver > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1420 Frame 1 (62 bytes on wire, 62 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 16.46.57.86 (16.46.57.86) Transmission Control Protocol, Src Port: jvserver (1939), Dst Port: netbios-ssn (139), Seq: 0, Len: 0 Source port: jvserver (1939) Destination port: netbios-ssn (139) Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) Window size: 65535 Checksum: 0xa362 [correct] Options: (8 bytes)
2	No. Time Source Destination Protocol Info 2 1.404480 88.30.180.33 16.46.57.86 TCP jwclient > microsoft-ds [SYN] Seq=0 Win=65535 Len=0 MSS=1420 Frame 2 (62 bytes on wire, 62 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 16.46.57.86 (16.46.57.86) Transmission Control Protocol, Src Port: jwclient (1938), Dst Port: microsoft-ds (445), Seq: 0, Len: 0 Source port: jwclient (1938) Destination port: microsoft-ds (445) Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) Window size: 65535 Checksum: 0xb84e [correct] Options: (8 bytes)
3	No. Time Source Destination Protocol Info 3 6.019200 88.30.180.33 16.46.57.86 TCP jvserver > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1420 Frame 3 (62 bytes on wire, 62 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 16.46.57.86 (16.46.57.86) Transmission Control Protocol, Src Port: jvserver (1939), Dst Port: netbios-ssn (139), Seq: 0, Len: 0 Source port: jvserver (1939) Destination port: netbios-ssn (139) Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) Window size: 65535 Checksum: 0xa362 [correct] Options: (8 bytes)
4	No. Time Source Destination Protocol Info 4 8.284426 16.46.57.86 88.30.180.33 TCP http > jetcmeserver [FIN, ACK] Seq=1 Ack=1 Win=65320 Len=0 Frame 4 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 16.46.57.86 (16.46.57.86), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: http (80), Dst Port: jetcmeserver (1936), Seq: 1, Ack: 1, Len: 0 Source port: http (80) Destination port: jetcmeserver (1936) Sequence number: 1 (relative sequence number) Acknowledgement number: 1 (relative ack number) Header length: 20 bytes Flags: 0x11 (FIN, ACK) Window size: 65320 Checksum: 0x2ed4 [correct]
5	No. Time Source Destination Protocol Info 5 8.284426 88.30.180.33 16.46.57.86 TCP jetcmeserver > http [ACK] Seq=1 Ack=2 Win=65400 Len=0 Frame 5 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 16.46.57.86 (16.46.57.86) Transmission Control Protocol, Src Port: jetcmeserver (1936), Dst Port: http (80), Seq: 1, Ack: 2, Len: 0

	Source port: jetcmeserver (1936) Destination port: http (80) Sequence number: 1 (relative sequence number) Acknowledgement number: 2 (relative ack number) Header length: 20 bytes Flags: 0x10 (ACK) Window size: 65400 Checksum: 0x2e84 [correct] [SEQ/ACK analysis]
6	No. Time Source Destination Protocol Info 6 15.949877 194.179.1.100 88.30.180.33 DNS Standard query response, No such name Frame 6 (149 bytes on wire, 149 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.100 (194.179.1.100), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 115 Checksum: 0xbb9d [correct] Domain Name System (response) Transaction ID: 0x879 Flags: 0x8183 (Standard query response, No such name) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0 Queries www.ii.uam.hhh: type A, class IN Name: www.ii.uam.hhh Type: A (Host address) Class: IN (0x0001) Authoritative nameservers
7	No. Time Source Destination Protocol Info 7 18.025498 88.28.102.153 88.30.180.33 TCP snac > epmap [SYN] Seq=0 Win=16384 Len=0 MSS=1460 Frame 7 (62 bytes on wire, 62 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 88.28.102.153 (88.28.102.153), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: snac (3536), Dst Port: epmap (135), Seq: 0, Len: 0 Source port: snac (3536) Destination port: epmap (135) Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) Window size: 16384 Checksum: 0xd706 [correct] Options: (8 bytes)
8	No. Time Source Destination Protocol Info 8 18.034527 88.30.180.33 88.28.102.153 TCP epmap > snac [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 Frame 8 (62 bytes on wire, 62 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 88.28.102.153 (88.28.102.153) Transmission Control Protocol, Src Port: epmap (135), Dst Port: snac (3536), Seq: 0, Ack: 1, Len: 0 Source port: epmap (135) Destination port: snac (3536) Sequence number: 0 (relative sequence number) Acknowledgement number: **ACK** (relative ack number) Header length: 28 bytes Flags: 0x12 (SYN, ACK) Window size: 65535 Checksum: 0x9075 [correct] Options: (8 bytes) [SEQ/ACK analysis]
9	No. Time Source Destination Protocol Info 9 18.769872 88.28.102.153 88.30.180.33 TCP snac > epmap [ACK] Seq=1 Ack=1 Win=17040 Len=0 Frame 9 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 88.28.102.153 (88.28.102.153), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: snac (3536), Dst Port: epmap (135), Seq: 1, Ack: 1, Len: 0 Source port: snac (3536)

	Destination port: epmap (135) Sequence number: 1 (relative sequence number) Acknowledgement number: 1 (relative ack number) Header length: 20 bytes Flags: 0x10 (ACK) Window size: 17040 Checksum: 0x7a81 [correct] [SEQ/ACK analysis]
10	No. Time Source Destination Protocol Info 10 19.748995 88.28.102.153 88.30.180.33 DCERPC Bind: call_id: 0 REMACT V0.0 Frame 10 (126 bytes on wire, 126 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 88.28.102.153 (88.28.102.153), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: snac (3536), Dst Port: epmap (135), Seq: 1, Ack: 1, Len: 72 Source port: snac (3536) Destination port: epmap (135) Sequence number: 1 (relative sequence number) [Next sequence number: 73 (relative sequence number)] Acknowledgement number: 1 (relative ack number) Header length: 20 bytes Flags: 0x18 (PSH, ACK) Window size: 17040 Checksum: 0x1c65 [correct] DCE RPC Bind, Fragment: Single, FragLen: 72, Call: 0
11	No. Time Source Destination Protocol Info 11 19.749999 88.30.180.33 88.28.102.153 DCERPC Bind_ack: call_id: 0 accept max_xmit: 5840 max_recv: 5840 Frame 11 (114 bytes on wire, 114 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 88.28.102.153 (88.28.102.153) Transmission Control Protocol, Src Port: epmap (135), Dst Port: snac (3536), Seq: 1, Ack: 73, Len: 60 Source port: epmap (135) Destination port: snac (3536) Sequence number: 1 (relative sequence number) [Next sequence number: 61 (relative sequence number)] Acknowledgement number: 73 (relative ack number) Header length: 20 bytes Flags: 0x18 (PSH, ACK) Window size: 65463 Checksum: 0x57f7 [correct] [SEQ/ACK analysis] DCE RPC Bind_ack, Fragment: Single, FragLen: 60, Call: 0
12	No. Time Source Destination Protocol Info 12 21.424339 88.28.102.153 88.30.180.33 TCP [TCP segment of a reassembled PDU] Frame 12 (1474 bytes on wire, 1474 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 88.28.102.153 (88.28.102.153), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: snac (3536), Dst Port: epmap (135), Seq: 73, Ack: 61, Len: **LONGITUD** Source port: snac (3536) Destination port: epmap (135) Sequence number: 73 (relative sequence number) [Next sequence number: 1493 (relative sequence number)] Acknowledgement number: 61 (relative ack number) Header length: 20 bytes Flags: 0x10 (ACK) Window size: 16980 Checksum: 0xc654 [correct] [SEQ/ACK analysis] TCP segment data (**LONGITUD** bytes) [DCE RPC: 1420 bytes left, desegmentation might follow]
13	No. Time Source Destination Protocol Info 13 21.481522 88.28.102.153 88.30.180.33 REMACT RemoteActivation request CLSID=NULL IID[1]=IUnknown Frame 13 (308 bytes on wire, 308 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 88.28.102.153 (88.28.102.153), Dst: 88.30.180.33 (88.30.180.33) Transmission Control Protocol, Src Port: snac (3536), Dst Port: epmap (135), Seq: 1493, Ack: 61, Len: 254 Source port: snac (3536) Destination port: epmap (135) Sequence number: 1493 (relative sequence number) [Next sequence number: 1747 (relative sequence number)]

	Acknowledgement number: 61 (relative ack number) Header length: 20 bytes Flags: 0x18 (PSH, ACK) Window size: 16980 Checksum: 0xa5be [correct] TCP segment data (254 bytes) [Reassembled TCP Segments (1674 bytes): #12(1420), #13(254)] DCE RPC Request, Fragment: Single, FragLen: 1674, Call: 0 Ctx: 0 DCOM IRemoteActivation, RemoteActivation
14	No. Time Source Destination Protocol Info 14 21.481522 88.30.180.33 88.28.102.153 TCP epmap > snac [ACK] Seq=61 Ack=1747 Win=65535 Len=0 Frame 14 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 88.28.102.153 (88.28.102.153) Transmission Control Protocol, Src Port: epmap (135), Dst Port: snac (3536), Seq: 61, Ack: 1747, Len: 0 Source port: epmap (135) Destination port: snac (3536) Sequence number: 61 (relative sequence number) Acknowledgement number: 1747 (relative ack number) Header length: 20 bytes Flags: 0x10 (ACK) Window size: 65535 Checksum: 0xb603 [correct] [SEQ/ACK analysis]
15	No. Time Source Destination Protocol Info 15 21.486538 194.179.1.100 88.30.180.33 DNS Standard query response, Server failure Frame 15 (91 bytes on wire, 91 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.100 (194.179.1.100), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 57 Checksum: 0x4951 [correct] Domain Name System (response) Transaction ID: 0x83a4 Flags: 0x8182 (Standard query response, Server failure) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.cpqcorp.net Type: A (Host address) Class: IN (0x0001)
16	No. Time Source Destination Protocol Info 16 21.486538 194.179.1.100 88.30.180.33 DNS Standard query response, Server failure Frame 16 (91 bytes on wire, 91 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.100 (194.179.1.100), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 57 Checksum: 0x4951 [correct] Domain Name System (response) Transaction ID: 0x83a4 Flags: 0x8182 (Standard query response, Server failure) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.cpqcorp.net Type: A (Host address) Class: IN (0x0001)
17	No. Time Source Destination Protocol Info 17 21.529675 194.179.1.100 88.30.180.33 DNS Standard query response, Server failure

	Frame 17 (91 bytes on wire, 91 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.100 (194.179.1.100), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 57 Checksum: 0x4951 [correct] Domain Name System (response) Transaction ID: 0x83a4 Flags: 0x8182 (Standard query response, Server failure) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.cpqcorp.net Type: A (Host address) Class: IN (0x0001)
18	No. Time Source Destination Protocol Info 18 21.551746 194.179.1.101 88.30.180.33 DNS Standard query response, Server failure Frame 18 (91 bytes on wire, 91 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 57 Checksum: 0x4950 [correct] Domain Name System (response) Transaction ID: 0x83a4 Flags: 0x8182 (Standard query response, Server failure) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.cpqcorp.net Type: A (Host address) Class: IN (0x0001)
19	No. Time Source Destination Protocol Info 19 21.557765 194.179.1.101 88.30.180.33 DNS Standard query response, Server failure Frame 19 (91 bytes on wire, 91 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 57 Checksum: 0x4950 [correct] Domain Name System (response) Transaction ID: 0x83a4 Flags: 0x8182 (Standard query response, Server failure) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.cpqcorp.net Type: A (Host address) Class: IN (0x0001)
20	No. Time Source Destination Protocol Info 20 22.135608 194.179.1.101 88.30.180.33 DNS Standard query response, No such name Frame 20 (159 bytes on wire, 159 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061)

	Length: 125 Checksum: 0x9a93 [correct] Domain Name System (response) Transaction ID: 0x5d0b Flags: 0x8183 (Standard query response, No such name) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0 Queries www.ii.uam.hhh.EMEA.hpqcorp.net: type A, class IN Name: www.ii.uam.hhh.EMEA.hpqcorp.net Type: A (Host address) Class: IN (0x0001) Authoritative nameservers
21	No. Time Source Destination Protocol Info 21 23.363525 194.179.1.101 88.30.180.33 DNS Standard query response, No such name Frame 21 (155 bytes on wire, 155 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 121 Checksum: 0x984d [correct] Domain Name System (response) Transaction ID: 0xf7cb Flags: 0x8183 (Standard query response, No such name) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0 Queries www.ii.uam.hhh.hpqcorp.net: type A, class IN Name: www.ii.uam.hhh.hpqcorp.net Type: A (Host address) Class: IN (0x0001) Authoritative nameservers
22	No. Time Source Destination Protocol Info 22 23.610312 194.179.1.101 88.30.180.33 DNS Standard query response, No such name Frame 22 (155 bytes on wire, 155 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 121 Checksum: 0x984e [correct] Domain Name System (response) Transaction ID: 0xf7cb Flags: 0x8183 (Standard query response, No such name) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0 Queries www.ii.uam.hhh.hpqcorp.net: type A, class IN Name: www.ii.uam.hhh.hpqcorp.net Type: A (Host address) Class: IN (0x0001) Authoritative nameservers
23	No. Time Source Destination Protocol Info 23 23.795904 194.179.1.101 88.30.180.33 DNS Standard query response, No such name Frame 23 (162 bytes on wire, 162 bytes captured) Ethernet II, Src: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00), Dst: 02:00:02:00:00:00 (02:00:02:00:00:00) Internet Protocol, Src: 194.179.1.101 (194.179.1.101), Dst: 88.30.180.33 (88.30.180.33) User Datagram Protocol, Src Port: domain (53), Dst Port: kiosk (1061) Source port: domain (53) Destination port: kiosk (1061) Length: 128 Checksum: 0x6719 [correct]

	Domain Name System (response) Transaction ID: 0xbe38 Flags: 0x8183 (Standard query response, No such name) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0 Queries www.ii.uam.hhh.cpqcorp.net: type A, class IN Name: www.ii.uam.hhh.cpqcorp.net Type: A (Host address) Class: IN (0x0001) Authoritative nameservers
24	No. Time Source Destination Protocol Info 24 23.795904 88.30.180.33 255.255.255.255 NBNS Name query NB WWW.II.UAM.HHH<00> Frame 24 (92 bytes on wire, 92 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 255.255.255.255 (255.255.255.255) User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137) Source port: netbios-ns (137) Destination port: netbios-ns (137) Length: 58 Checksum: 0xbf3e [correct] NetBIOS Name Service
25	No. Time Source Destination Protocol Info 25 24.546298 88.30.180.33 255.255.255.255 NBNS Name query NB WWW.II.UAM.HHH<00> Frame 25 (92 bytes on wire, 92 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 255.255.255.255 (255.255.255.255) User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137) Source port: netbios-ns (137) Destination port: netbios-ns (137) Length: 58 Checksum: 0xbf3e [correct] NetBIOS Name Service
26	No. Time Source Destination Protocol Info 26 25.296691 88.30.180.33 255.255.255.255 NBNS Name query NB WWW.II.UAM.HHH<00> Frame 26 (92 bytes on wire, 92 bytes captured) Ethernet II, Src: 02:00:02:00:00:00 (02:00:02:00:00:00), Dst: 9a:a0:20:00:02:00 (9a:a0:20:00:02:00) Internet Protocol, Src: 88.30.180.33 (88.30.180.33), Dst: 255.255.255.255 (255.255.255.255) User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137) Source port: netbios-ns (137) Destination port: netbios-ns (137) Length: 58 Checksum: 0xbf3e [correct] NetBIOS Name Service