

APELLIDOS (MAYÚSCULAS) \_\_\_\_\_

NOMBRE (MAYÚSCULAS): \_\_\_\_\_

GRUPO: \_\_\_\_\_

**Tiempo: Dos horas**

**Sin libros ni apuntes, 36 preguntas.**

**Calificación: todas las preguntas tienen el mismo peso en la nota:**

**Respuesta correcta: +3**

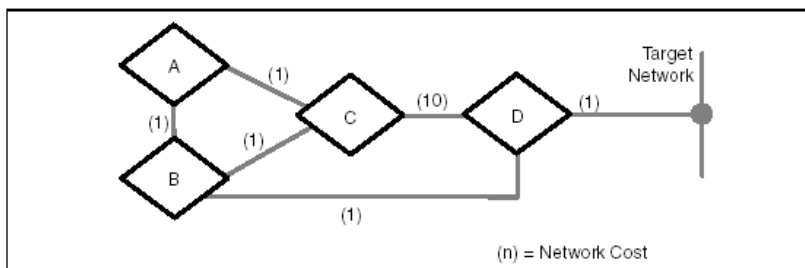
**Respuesta errónea: -1**

**El alumno entregará el examen junto con la hoja de lectura óptica.**



## CUESTIONES

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

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

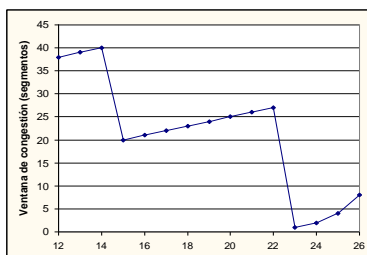


En un momento dado, el enlace entre el router B y el D falla. Cuando el router B se da cuenta, empieza a enviar mensajes utilizando el algoritmo mencionado. La siguiente tabla refleja esquemáticamente la información que tienen los routers A, B, C y D sobre la distancia que tiene la ruta para alcanzar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

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

Indicar cuál de las siguientes afirmaciones es cierta:

- El algoritmo basado en el vector distancia no puede tener este comportamiento, hay algún error
  - Es un ejemplo de que “las buenas noticias vuelan”
  - Es un ejemplo de que “las malas noticias van despacio”
  - Ninguna de las anteriores
18. Los routers utilizan habitualmente un algoritmo denominado Random Early Detect (RED) para mejorar el comportamiento frente a situaciones de congestión en una red IP. Dicho algoritmo se basa en que cuando la ocupación de la cola de salida de un router supera un determinado umbral (inferior a la ocupación máxima), el router descarta aleatoriamente paquetes. Con esto se consigue:
- Que los sistemas finales reduzcan su ritmo de envío, al reducirse el tamaño de la ventana de congestión CWD por detectarse la pérdida de un segmento.
  - Que los sistemas finales se envíen mensajes ICMP para que reduzcan su velocidad de transferencia.
  - Que los sistemas finales busquen una ruta alternativa que pierda menos paquetes.
  - Ninguna de las anteriores
19. La pila TCP de un servidor tiene una conexión en estado LISTEN en el puerto 23. La conexión pasará al estado SYN\_RCVD tras recibir un segmento con los siguientes valores:
- SYN=1, ACK=1, puerto origen=23, puerto destino= 1234.
  - SYN=1, ACK=0, puerto origen=1234, puerto destino= 23.
  - SYN=1, ACK=0, puerto origen=23, puerto destino 1234.
  - Ninguna de las anteriores
20. Un sistema cliente se conecta a un servidor remoto utilizando TCP/IP para descargar un fichero de 10Mbytes. La velocidad neta que se obtiene es de 1.0 Kbytes/segundo. Para obtener mayor eficiencia, se duplica la ventana ofrecida por el nivel TCP en el sistema cliente sin cambiar ningún otro parámetro y la velocidad que se obtiene es de 1.2 Kbytes/segundo. Indicar cuál de las siguientes afirmaciones es cierta:
- Es imposible el resultado anterior, al duplicar la ventana debería duplicarse aproximadamente la velocidad neta
  - El tamaño de la ventana no tiene nada que ver con la velocidad neta de transmisión, por lo que no puede tener influencia nunca en la velocidad de transmisión
  - El comportamiento se explica porque al aumentar el tamaño de ventana, ésta ha dejado de ser un freno para utilizar toda la capacidad de la pipa y por tanto se ha alcanzado la máxima velocidad neta
  - Ninguna de las anteriores
21. El campo de cabecera Last-Modified de HTTP:
- Lo envía el cliente al servidor para pedir las actualizaciones de una página respecto a una fecha.
  - Lo envía el servidor al cliente para que éste la incluya en su caché y evite posteriores descargas si no se ha modificado la página.
  - Lo envía el servidor al cliente sólo cuando el cliente incluye el campo de cabecera If-Modified-Since.
  - Ninguna de las anteriores
22. El motivo de usar un campo de tiempo de vida (TTL) en la cabecera IP v4 es:
- Para llevar control del tiempo que tarda en llegar un datagrama al destino
  - Para informar al temporizador Keepalive
  - Para evitar que un datagrama se quede en un bucle de reencaminamientos infinito
  - Ninguna de las anteriores
23. El campo OPCODE de la cabecera DNS sirve:
- Para indica qué opciones hay que utilizar
  - Para distinguir entre preguntas directas e inversas
  - Relleno de bytes. Su uso es opcional
  - Ninguna de las anteriores
24. La figura representa el tamaño de la ventana de congestión (CWD) de una conexión TCP en función del tiempo:



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

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

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

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

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

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

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

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

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

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

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

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

- a) SYN\_RCVD
- b) SYN\_SENT
- c) ESTABLISHED
- d) Ninguna de las anteriores

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**FIN DEL EXAMEN**

# Arquitectura de Redes I Todos los modelos

## Examen Final 12 de enero de 2013

---

### TRAZA

La captura se ha realizado en la maquina CLIENTE.

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

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

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

<p>Trama 4 (239 bytes), Arrival Time: Sep 14, 2007 10:00:54.335268000</p> <p>Ethernet II, Src: 00:09:7b:e5:d4:40, Dst: 00:19:21:45:b0:8a</p> <p>Internet Protocol, Src: 140.24.58.100, Dst: 140.24.56.169</p> <p>User Datagram Protocol, Src Port: 53, Dst Port: 1034</p> <p>Domain Name System (response)</p> <p>Transaction ID: 0x3478</p> <p>Flags: 0x8580 (Standard query response, No error)</p> <p>Questions: 1</p> <p>Answer RRs: 1</p> <p>Authority RRs: 5</p> <p>Additional RRs: 3</p> <p>Queries</p> <p>efetepe.ii.uam.es: type A, class IN</p> <p>Answers</p> <p>efetepe.ii.uam.es: type A, class IN, addr 140.24.57.113</p> <p>Authoritative nameservers</p> <p>uam.es: type NS, class IN, ns ns2.uam.es</p> <p>uam.es: type NS, class IN, ns sun.rediris.es</p> <p>uam.es: type NS, class IN, ns chico.rediris.es</p> <p>uam.es: type NS, class IN, ns ns.uam.es</p> <p>uam.es: type NS, class IN, ns ns0.uam.es</p> <p>Additional records</p> <p>ns.uam.es: type A, class IN, addr 140.24.58.200</p> <p>ns0.uam.es: type A, class IN, addr 140.24.58.226</p> <p>ns2.uam.es: type A, class IN, addr 140.24.58.100</p>
<p>Trama 5 (42 bytes), Arrival Time: Sep 14, 2007 10:00:54.363611000</p> <p>Ethernet II, Src: 00:19:21:45:b0:8a, Dst: ff:ff:ff:ff:ff:ff</p> <p>Address Resolution Protocol (request)</p> <p>Hardware type: Ethernet (0x0001)</p> <p>Protocol type: IP (0x0800)</p> <p>Hardware size: 6</p> <p>Protocol size: 4</p> <p>Opcode: request (0x0001)</p> <p>Sender MAC address: 00:19:21:45:b0:8a</p> <p>Sender IP address: 140.24.56.169</p> <p>Target MAC address: 00:00:00:00:00:00</p> <p>Target IP address: 140.24.57.113</p>
<p>Trama 6 (60 bytes), Arrival Time: Sep 14, 2007 10:00:54.363755000</p> <p>Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a</p> <p>Address Resolution Protocol (reply)</p> <p>Hardware type: Ethernet (0x0001)</p> <p>Protocol type: IP (0x0800)</p> <p>Hardware size: 6</p> <p>Protocol size: 4</p> <p>Opcode: reply (0x0002)</p> <p>Sender MAC address: 00:18:8b:18:6b:ae</p> <p>Sender IP address: 140.24.57.113</p> <p>Target MAC address: 00:19:21:45:b0:8a</p> <p>Target IP address: 140.24.56.169</p>
<p>Trama 7 (62 bytes), Arrival Time: Sep 14, 2007 10:00:54.363784000</p> <p>Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae</p> <p>Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113</p> <p>Transmission Control Protocol</p> <p>Src Port: 1143, Dst Port: 21, Seq: 0, Len: 0</p> <p>Hdr Len: 28 bytes, Flags: 0x02 (SYN), Window size: 65535, Checksum: 0xc84e</p> <p>Options: (8 bytes)</p> <p>Maximum segment size: 1460 bytes</p> <p>NOP</p> <p>NOP</p> <p>SACK permitted</p>

<p>Trama 8 (62 bytes), Arrival Time: Sep 14, 2007 10:00:54.363954000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol    Src Port: 21, Dst Port: 1143, Seq: 0, Ack: 1, Len: 0    Hdr Len: 28 bytes, Flags: 0x12 (SYN, ACK), Window size: 17520, Checksum: 0x6455    Options: (8 bytes)      Maximum segment size: 1460 bytes      NOP      NOP      SACK permitted</p>
<p>Trama 9 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.363991000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol    Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 1, Len: 0    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65535, Checksum: 0xd589</p>
<p>Trama 10 (96 bytes), Arrival Time: Sep 14, 2007 10:00:54.366899000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol    Src Port: 21, Dst Port: 1143, Seq: 1, Ack: 1, Len: 42    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17520, Checksum: 0x2c28  File Transfer Protocol (FTP)    220-FileZilla Server version 0.9.23 beta\r\n</p>
<p>Trama 11 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.552466000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol    Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 43, Len: 0    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65493, Checksum: 0xd589</p>
<p>Trama 12 (160 bytes), Arrival Time: Sep 14, 2007 10:00:54.552673000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol    Src Port: 21, Dst Port: 1143, Seq: 43, Ack: 1, Len: 106    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17520, Checksum: 0x177a  File Transfer Protocol (FTP)    220-written by Tim Kosse (Tim.Kosse@gmx.de)\r\n    220 Please visit <a href="http://sourceforge.net/projects/filezilla/">http://sourceforge.net/projects/filezilla/</a>\r\n</p>
<p>Trama 13 (54 bytes), Arrival Time: Sep 14, 2007 10:00:54.753621000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol    Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 149, Len: 0    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65387, Checksum: 0xd589</p>
<p>Trama 14 (66 bytes), Arrival Time: Sep 14, 2007 10:00:56.170722000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol    Src Port: 1143, Dst Port: 21, Seq: 1, Ack: 149, Len: 12    Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65387, Checksum: 0x3684  File Transfer Protocol (FTP)    USER jorge\r\n</p>
<p>Trama 15 (60 bytes), Arrival Time: Sep 14, 2007 10:00:56.337523000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol    Src Port: 21, Dst Port: 1143, Seq: 149, Ack: 13, Len: 0    Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17508, Checksum: 0x9085</p>

<p>Trama 16 (87 bytes), Arrival Time: Sep 14, 2007 10:00:59.640578000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 149, Ack: 13, Len: 33  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17508, Checksum: 0x8819  File Transfer Protocol (FTP)  33l Password required for jorge\r\n</p>
<p>Trama 17 (54 bytes), Arrival Time: Sep 14, 2007 10:00:59.782589000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 13, Ack: 182, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65354, Checksum: 0xd57d</p>
<p>Trama 18 (68 bytes), Arrival Time: Sep 14, 2007 10:01:01.387513000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 13, Ack: 182, Len: 14  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65354, Checksum: 0xb71a  File Transfer Protocol (FTP)  PASS enrique\r\n</p>
<p>Trama 19 (60 bytes), Arrival Time: Sep 14, 2007 10:01:01.567693000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 182, Ack: 27, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17494, Checksum: 0x9064</p>
<p>Trama 20 (69 bytes), Arrival Time: Sep 14, 2007 10:01:05.643223000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 182, Ack: 27, Len: 15  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17494, Checksum: 0x7c42  File Transfer Protocol (FTP)  230 Logged on\r\n</p>
<p>Trama 21 (54 bytes), Arrival Time: Sep 14, 2007 10:01:05.817346000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 27, Ack: 197, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65339, Checksum: 0xd56f</p>
<p>Trama 22 (81 bytes), Arrival Time: Sep 14, 2007 10:01:08.866831000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 27, Ack: 197, Len: 27  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65339, Checksum: 0x0fb2  File Transfer Protocol (FTP)  PORT 150,244,56,169,4,121\r\n</p>
<p>Trama 23 (60 bytes), Arrival Time: Sep 14, 2007 10:01:09.010690000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 197, Ack: 54, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 17467, Checksum: 0x9055</p>
<p>Trama 24 (83 bytes), Arrival Time: Sep 14, 2007 10:01:13.639891000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 197, Ack: 54, Len: 29  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17467, Checksum: 0xb633  File Transfer Protocol (FTP)  200 Port command successful\r\n</p>



<p>Trama 25 (60 bytes), Arrival Time: Sep 14, 2007 10:01:13.670615000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 54, Ack: 226, Len: 6  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 65310, Checksum: 0x269c  File Transfer Protocol (FTP)  LIST\r\n</p>
<p>Trama 26 (62 bytes), Arrival Time: Sep 14, 2007 10:01:13.671578000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 20, Dst Port: <b>PUERTO</b>, Seq: 0, Len: 0  Hdr Len: 28 bytes, Flags: 0x02 (SYN), Window size: 65535, Checksum: 0xb774  Options: (8 bytes)  Maximum segment size: 1460 bytes  NOP  NOP  SACK permitted</p>
<p>Trama 27 (100 bytes), Arrival Time: Sep 14, 2007 10:01:13.671803000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 226, Ack: 60, Len: 46  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0x02ca  File Transfer Protocol (FTP)  150 Opening data channel for directory list.\r\n</p>
<p>Trama 28 (54 bytes), Arrival Time: Sep 14, 2007 10:01:13.863690000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 60, Ack: <b>SECUENCIA</b>, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65264, Checksum: 0xd54e</p>
<p>Trama 29 (87 bytes), Arrival Time: Sep 14, 2007 10:01:24.640290000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: <b>SECUENCIA</b>, Ack: 60, Len: 33  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0xf5e7  File Transfer Protocol (FTP)  425 Can't open data connection.\r\n</p>
<p>Trama 30 (54 bytes), Arrival Time: Sep 14, 2007 10:01:24.826833000  Ethernet II, Src: 00:19:21:45:b0:8a, Dst: 00:18:8b:18:6b:ae  Internet Protocol, Src: 140.24.56.169, Dst: 140.24.57.113  Transmission Control Protocol  Src Port: 1143, Dst Port: 21, Seq: 60, Ack: 305, Len: 0  Hdr Len: 20 bytes, Flags: 0x10 (ACK), Window size: 65231, Checksum: 0xd54e</p>
<p>Trama 31 (114 bytes), Arrival Time: Sep 14, 2007 10:05:06.633776000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 305, Ack: 60, Len: 60  Hdr Len: 20 bytes, Flags: 0x18 (PSH, ACK), Window size: 17461, Checksum: 0x23f0  File Transfer Protocol (FTP)  421 No-transfer-time exceeded. Closing control connection.\r\n</p>
<p>Trama 32 (60 bytes), Arrival Time: Sep 14, 2007 10:05:06.633921000  Ethernet II, Src: 00:18:8b:18:6b:ae, Dst: 00:19:21:45:b0:8a  Internet Protocol, Src: 140.24.57.113, Dst: 140.24.56.169  Transmission Control Protocol  Src Port: 21, Dst Port: 1143, Seq: 365, Ack: 60, Len: 0  Hdr Len: 20 bytes, Flags: 0x14 (RST, ACK), Window size: 0, Checksum: 0xd3de</p>

---

FIN DE LA TRAZA

**Esta hoja puede ser conservada por el alumno para referencia:**

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