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.

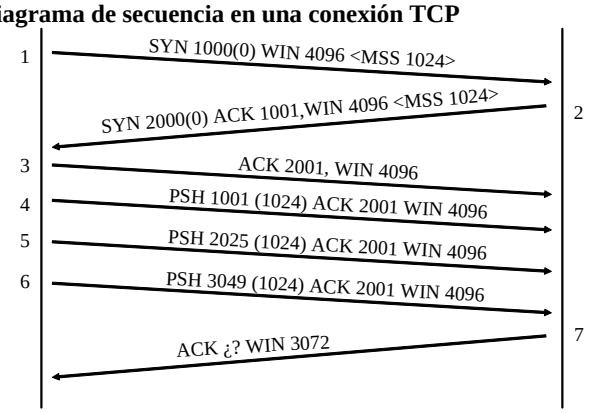
20. **Un usuario está utilizando para acceder a su correo. una aplicación webmail disponible comercialmente y que está conectada a un servidor externo a través de un cortafuegos que solo deja pasar paquetes con destino al puerto 80 ¿Qué protocolo o protocolos se estarán empleando en el ordenador de dicho 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

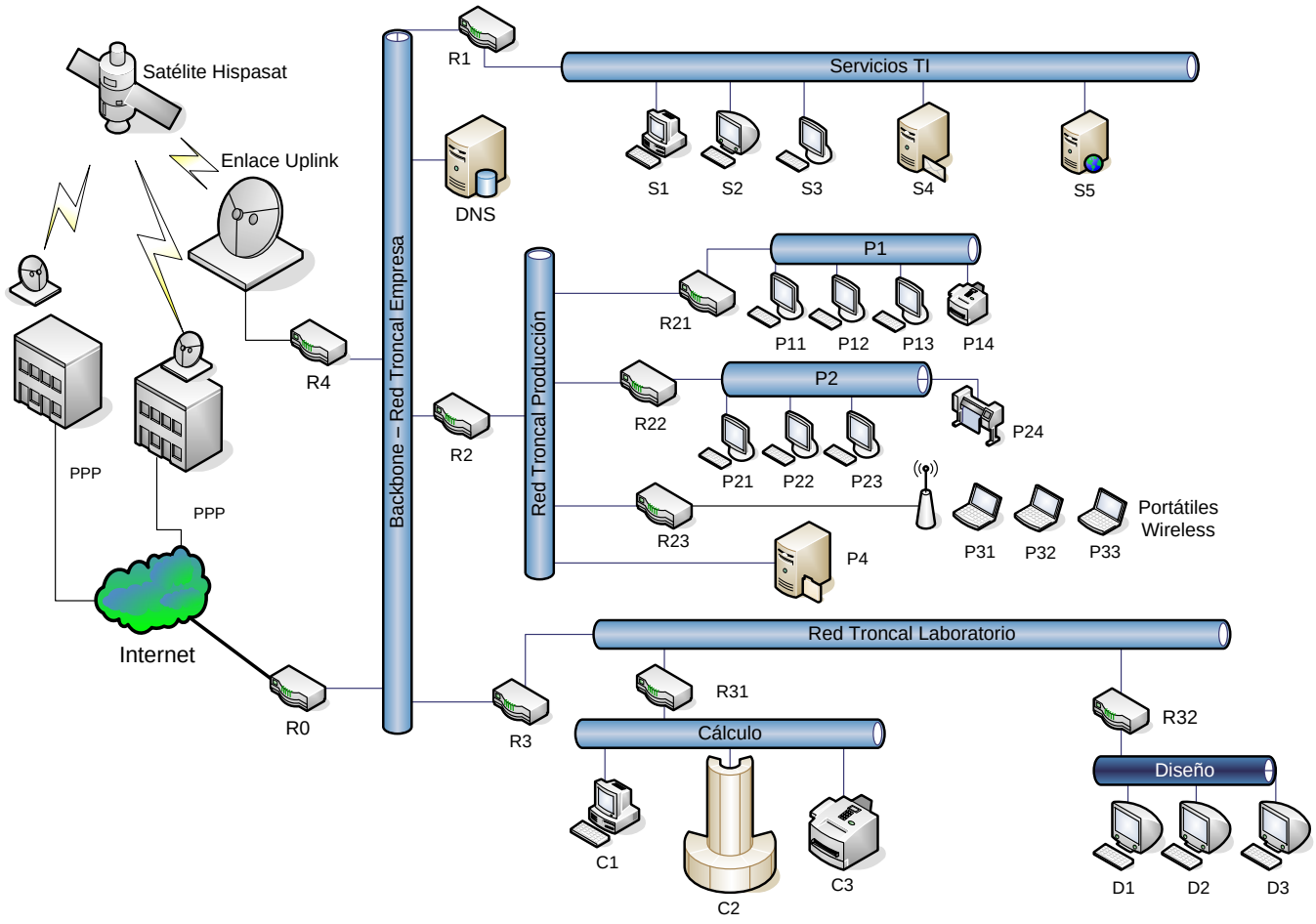
36. **Se ha observado que el tiempo de encaminamiento de los datagramas IP en los routers es aproximadamente independiente del tamaño de los datos. ¿Cuál de las siguientes alternativas mejoraría más el throughput de la red?**
    a) Aumentar la MTU hasta el máximo que sea posible
    b) Disminuir la 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