

EXAMEN DE REDES TEORÍA. SEGUNDO PARCIAL. JUNIO 2013.

Esta parte debe realizarse sin material de consulta. Puede utilizar una calculadora.

1 Pregunta 1 (4 puntos):

Responda en la hoja adjunta. Solo debe marcar una opción en cada pregunta; si cree que hay varias correctas debe elegir la que a su juicio mejor se ajuste a la pregunta. Lea los enunciados con atención.

Puntuación:	Bien: +1 punto	Mal: -1/3 puntos	En blanco: 0 puntos
-------------	----------------	------------------	---------------------

- 1.1 ¿Cuál de las siguientes características de IPv6 no estaba presente en IPv4?
- A) La posibilidad de comprobar, mediante el CRC de la trama a nivel 2, que no ha habido errores en la transmisión de los paquetes por los cables
 - B) La posibilidad de asignar la dirección de red automáticamente a partir de la dirección MAC
 - C) La posibilidad de limitar el número máximo de saltos que un paquete da por la red
 - D) La posibilidad de fragmentar los paquetes
- 1.2 Las siglas RFC corresponden a:
- A) Routing First Copy: un protocolo de routing, hoy en desuso, utilizado inicialmente en la Internet
 - B) Request For Comments: la denominación que se utiliza para referirse a los documentos oficiales de Internet
 - C) Return Forward Channel: un mecanismo de devolución de mensajes de error cuando no hay ninguna ruta utilizable
 - D) Repeat For Clarity: Procedimiento seguido por algunos protocolos de routing cuando un comando es ambiguo
- 1.3 Un ordenador tiene un servidor web activo y el puerto 80 en modo listen. ¿Cuántos clientes se pueden conectar a él?
- A) Uno
 - B) 64511
 - C) 65535
 - D) Ilimitado (es decir la limitación, si la hay, vendrá impuesta por factores ajenos)
- 1.4 ¿Qué ventaja tiene TCP frente a UDP?:
- A) Permite la multiplexación, es decir la comunicación simultánea de múltiples procesos del nivel de aplicación utilizando un único proceso del nivel de transporte
 - B) Garantiza la recepción correcta de los datos, aun en el caso de que se pierdan paquetes
 - C) Es más ligero, y por tanto más eficiente
 - D) Utiliza una cabecera más pequeña, lo cual reduce el overhead
- 1.5 ¿Qué flags llevan puestos los tres mensajes que normalmente se intercambian en el saludo a tres vías de TCP?:
- A) El primero SYN, el segundo ACK y el tercero ACK
 - B) El primero SYN y ACK, el segundo SYN y el tercero ACK
 - C) El primero SYN, el segundo SYN y ACK, el tercero ACK
 - D) El primero SYN y ACK, el segundo SYN y ACK, el tercero ACK
- 1.6 ¿Qué campo de la cabecera TCP se utiliza para ejercer el control de flujo?
- A) El tamaño de ventana
 - B) El Maximum Segment Size
 - C) El flag FLC
 - D) El factor de escala
- 1.7 ¿Qué debe hacer TCP si recibe un segmento duplicado?
- A) Debe descartarlo y no hacer nada más
 - B) Debe descartarlo y enviar el ACK correspondiente al emisor
 - C) Debe pasarlo al buffer de la aplicación y enviar el ACK correspondiente al emisor
 - D) Debe pasarlo al buffer de la aplicación y no hacer nada más

- 1.8** ¿Qué ocurre cuando, al enviar varios datagramas UDP a un mismo puerto y una misma IP de destino, la red los entrega en un orden distinto al de salida?
- A) En el receptor el nivel IP los reordena y los entrega en el orden correcto al nivel UDP
 - B) El nivel UDP en el receptor los reordena y los entrega en el orden correcto al proceso del nivel de aplicación que está escuchando en ese puerto.
 - C) El nivel UDP en el receptor los entrega desordenados al proceso que está escuchando en ese puerto.
 - D) Esto no puede ocurrir ya que en UDP siempre se respeta el orden de los datagramas.
- 1.9** El 'timer de persistencia' se utiliza para fijar:
- A) El tiempo que un TCP servidor espera antes de 'provocar' a un cliente inactivo, para saber si éste sigue conectado
 - B) El tiempo que un TCP, bloqueado por ventana cerrada, espera antes de 'tantear' al otro, por si la ventana no estaba realmente cerrada
 - C) El tiempo que un TCP, pendiente de recibir un ACK, espera antes de reenviar un segmento
 - D) El tiempo que un TCP espera, cuando se cierra una conexión, antes de liberar el socket.
- 1.10** ¿Para qué sirve el 'factor de escala', que se negocia en algunas conexiones TCP?
- A) Para que se pueda tener más datos pendientes de confirmación por parte del receptor, mejorando el rendimiento en redes con elevado caudal y elevado retardo
 - B) Para que se puedan enviar segmentos mayores de 64 KBytes, mejorando el rendimiento en todo tipo de redes
 - C) A y B**
 - D) Para poder enviar segmentos mayores que la MTU del trayecto.
- 1.11** Cuando ponemos en marcha un servicio en un host para recibir conexiones entrantes ¿En qué caso utilizaremos un número de puerto inferior al 1024?
- A) Cuando se trate de un servicio de alta disponibilidad
 - B) Cuando el servicio deba estar abierto solo a determinados clientes
 - C) Cuando queramos que el servicio solo lo pueda iniciar un usuario o proceso con privilegios
 - D) Cuando se trate de un servicio permanente, que deba estar en marcha siempre que el host esté levantado
- 1.12** ¿Qué ventaja aporta la opción SACK en el funcionamiento de TCP?
- A) Permite confirmar la recepción de varios segmentos conjuntamente, no teniendo que enviar un ACK por cada segmento recibido.**
 - B) Permite confirmar la recepción de segmentos no consecutivos
 - C) A y B
 - D) Permite enviar segmentos de mayor tamaño que la ventana anunciada por el receptor
- 1.13** En un router que tiene solo dos interfaces, E0 y S0, queremos aplicar una ACL al tráfico que discurre en sentido E0 → S0. Diga cuál de las siguientes afirmaciones es correcta:
- A) La ACL puede aplicarse indistintamente al sentido entrante en E0 o al saliente en S0. El rendimiento del router será el mismo en ambos casos
 - B) La ACL puede aplicarse indistintamente al sentido entrante en E0 o al saliente en S0, pero el rendimiento del router será mayor si se aplica en E0
 - C) La ACL puede aplicarse indistintamente al sentido entrante en E0 o al saliente en S0, pero el rendimiento del router será mayor si se aplica en S0
 - D) La ACL debe aplicarse tanto en sentido entrante en E0 como saliente en S0.
- 1.14** En una red local tenemos 500 ordenadores con direcciones privadas que queremos que tengan salida a Internet, para lo cual disponemos de una única IP pública. Sabemos que nunca más del 20% estarán conectados simultáneamente y que las conexiones siempre se iniciarán desde la red privada. ¿Qué tipo de NAT debemos utilizar?
- A) NAT básico estático
 - B) NAT básico dinámico
 - C) NAT básico estático
 - D) NAT básico dinámico

- 1.15** Si estoy en un ordenador de laboratorio de la Universidad de Valencia y me conecto a la página web www.google.com capturaré los siguientes tipos de paquetes (sin importar el orden):
- A) TCP, UDP
 - B) TCP, ICMP
 - C) UDP, ICMP
 - D) ICMP, DNS
- 1.16** He hecho una consulta a un DNS y obtengo los Registros de Recursos con un campo tipo AAAA. ¿Qué tipo de consulta he realizado?
- A) He pedido el nombre de una máquina
 - B) He pedido la IP de una máquina
 - C) He pedido la IPv6 de una máquina
 - D) He pedido la dirección del MailExchanger (campo MX) del dominio
- 1.17** Tengo mi correo en el servidor correo.uv.es de la universidad de Valencia, ¿qué me permite hacer el protocolo ESMTP?
- A) Enviar y recibir correos electrónicos
 - B) Conectarme a mi buzón de correo y gestionar mis e-mails
 - C) Trabajar sobre el contenido de los correos electrónicos
 - D) Todo lo anterior
- 1.18** ¿Cuál es la utilidad de la codificación MIME Entrecomillada Imprimible?
- A) Poder trabajar en formato hexadecimal y agrupar los bits de datos en bytes
 - B) Poder enviar mensajes que tienen unos pocos caracteres no ASCII puros con bastante ahorro de ancho de banda
 - C) Poder enviar cualquier tipo de byte a través de una red pensada para enviar hasta agrupaciones de 7 bits
 - D) Poder enviar mensajes de texto puro (ASCII 7) como adjunto a un correo electrónico
- 1.19** ¿Para qué sirve SNMP?
- A) SNMP permite gestionar vía UDP cada dispositivo de una red recibiendo información de una base de datos MIB con un formato SMI
 - B) SNMP es un protocolo orientado al dispositivo y enviará información vía TCP de cada dispositivo a la estación desde la que se administra el dispositivo, mostrándose estadísticas de uso de puertos e interfaces
 - C) SNMP permite gestionar vía UDP la información de alarmas o interrupciones TRAP y vía TCP haciendo sondeos (o pooling) de diferentes dispositivos de una red
 - D) SNMP está orientado al dispositivo y la información generada nunca se guarda en él, sino que cada vez que se genera un cambio (por ejemplo en una interfaz de un router) se envía mediante un "demonio" a una estación administradora
- 1.20** ¿Cuál es la primera información que envía un servidor SSH a un cliente la primera vez que se conecta a él?
- A) El compendio del password (en SHA-1 o MD-5) que es modificado con el password del cliente
 - B) Un certificado donde el cliente podrá poner su password y devolver al servidor
 - C) La clave pública del servidor
 - D) La clave simétrica de sesión que deberá usarse durante toda la comunicación para encriptar los mensajes
- 1.21** Los cifrados por sustitución siempre tienen el mismo problema:
- A) Que dado cualquier texto de entrada siempre podré encontrar repeticiones
 - B) Que son bastante fáciles de descifrar por fuerza bruta
 - C) Que siempre se puede adivinar una palabra del mensaje de entrada
 - D) Que se pueden romper mediante el análisis de las propiedades estadísticas de los lenguajes naturales
- 1.22** Si A envía a B un mensaje encriptado con la clave pública de B:
- A) B está seguro que el mensaje lo ha enviado A
 - B) B está seguro que el mensaje no ha podido modificarse por el camino
 - C) B está seguro de la confidencialidad del mensaje sin importar quién lo haya enviado
 - D) Nadie puede haber enviado este mensaje excepto el mismo B

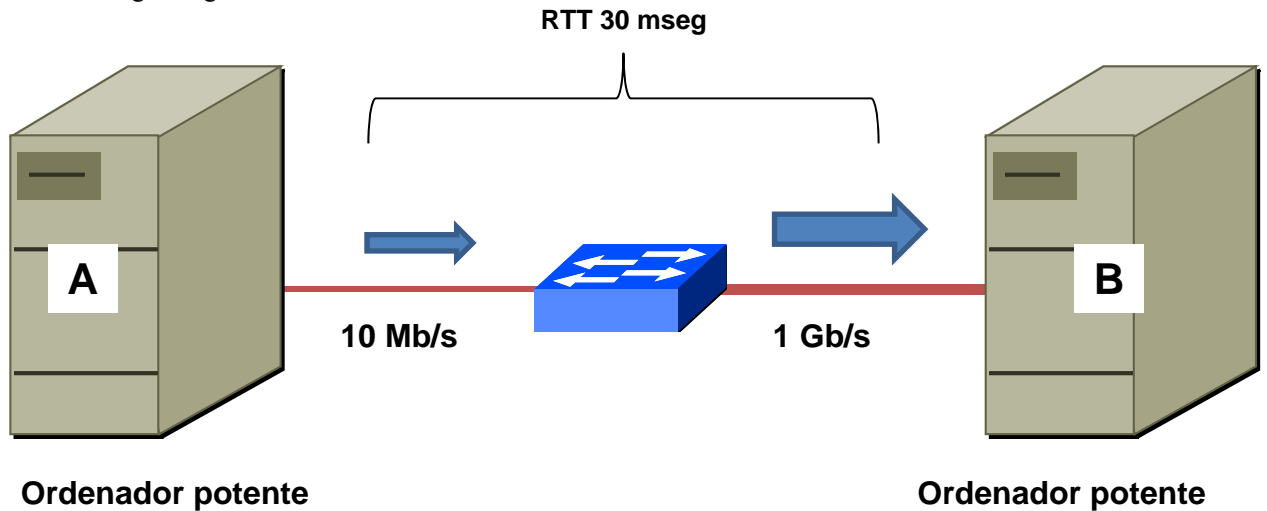
- 1.23** Si A envía a B un mensaje encriptado con la clave privada de A:
- A) B está seguro que el mensaje lo ha enviado A y nadie más podrá ver el contenido
 - B) B está seguro que el mensaje lo ha enviado A pero cualquiera que esté escuchando el canal de comunicaciones podrá ver el contenido usando la clave pública de A
 - C) Cualquiera puede haber enviado el mensaje
 - D) Esto se usa para guardar de forma local (o remota) la información encriptada y solo el usuario A podrá desencriptarla
- 1.24** Si A envía a B un mensaje encriptado con la clave pública de A:
- A) B no podrá hacer nada con el mensaje, cualquiera podrá haber enviado el mensaje y solo A podrá desencriptarlo
 - B) B no podrá modificar el mensaje pero está seguro que solo A lo puede haber enviado y por lo tanto lo podrá usar como prueba (firma)
 - C) B no podrá modificar el mensaje pero está seguro que viene de A y por lo tanto se trata de una prueba de no repudio
 - D) B no podrá modificar el mensaje y además no está seguro que haya llegado desde A. Este mensaje lo usará B para guardar las claves públicas de todas las entidades con las que se comunica
- 1.25** Un usuario A quiere enviar con PGP un correo electrónico encriptado a un usuario B.
- A) A necesita usar su clave privada y la clave pública del destinatario
 - B) A necesita usar tanto su clave pública como la del destinatario
 - C) A necesita usar tanto su clave privada como la clave privada del destinatario
 - D) A necesita usar tanto su clave pública como la privada del destinatario
- 1.26** El algoritmo Diffie-Hellman permite
- A) Validar una clave pública entre 2 entidades que no se han comunicado con anterioridad
 - B) Validar las identidades de 2 entidades que no se han comunicado con anterioridad
 - C) Intercambiar una clave secreta entre 2 entidades que no se han comunicado con anterioridad
 - D) Intercambiar una clave pública sin necesidad de usar certificados digitales
- 1.27** ¿Qué incluye un certificado digital?
- A) La clave privada de una entidad firmada con la clave pública de la entidad que certifica
 - B) La clave privada de una entidad firmada con la clave privada de la entidad que certifica
 - C) La clave pública de una entidad firmada con la clave pública de la entidad que certifica
 - D) La clave pública de una entidad firmada con la clave privada de la entidad que certifica
- 1.28** La firma digital con clave simétrica:
- A) Solamente se puede usar cuando son muchas las entidades que tienen que comunicarse entre sí para que salga rentable tener un centro de distribución de claves
 - B) Solamente se puede usar en sistemas en los que se disponga de tiempo suficiente para realizar todas las fases de encriptado y desencriptado
 - C) No permite comprobar la integridad del contenido de la comunicación
 - D) Necesita una autoridad donde se depositan todas las claves o que la clave haya sido enviada previamente a la entidad con la que me quiero comunicar

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES TEORÍA. SEGUNDO PARCIAL. JUNIO 2013.

Pregunta 2.1 (1 punto):

En la red de la figura siguiente:



Se está realizando, como muestra la figura, una transferencia de un fichero de gran tamaño desde A hacia B, utilizando para ello el protocolo FTP sobre TCP. El MSS se ha negociado a 1024 bytes.

Explique de qué manera evolucionará el tráfico durante la conexión, y cuál(es) será(n) el(los) factor(es) limitante(s) del rendimiento. Explique cómo afectaría a dicho rendimiento la utilización de un MSS de 512 o de 1480 bytes. Explique también como cambiaría el rendimiento si se utilizara un factor de escala 4x.

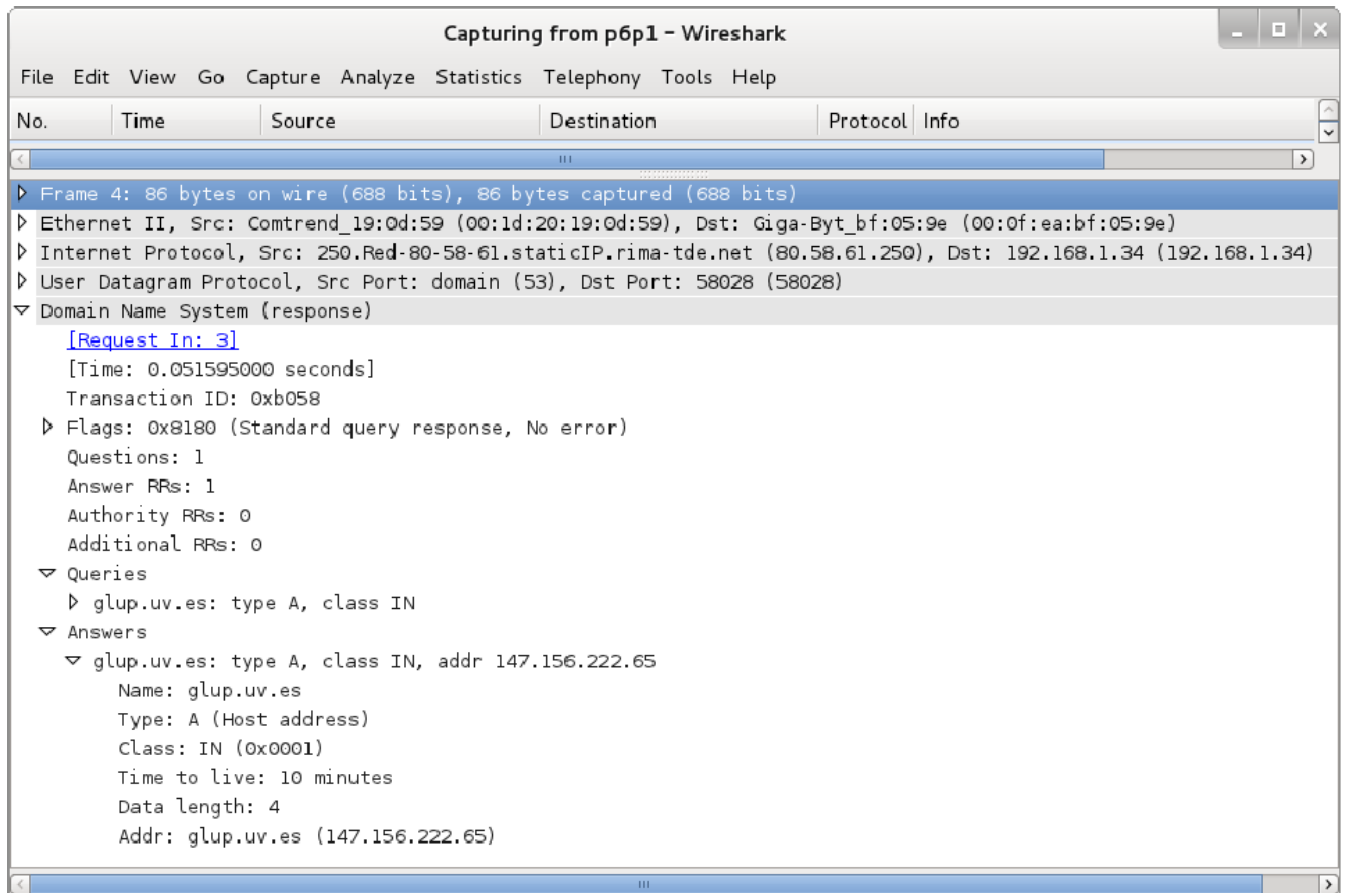
Los dos ordenadores implicados en la conexión TCP son potentes y tienen poca carga. Se supone por tanto que sus recursos (CPU y memoria) no son un factor limitante en el rendimiento de la transferencia.

Respuesta:

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES TEORÍA. SEGUNDO PARCIAL. JUNIO 2013.

Pregunta 2.2 (1 punto) Sin apuntes:



Responde a las siguientes preguntas:

- ¿De qué se trata la captura anterior?
- ¿Quién ha preguntado y qué ha preguntado?
- ¿Quién ha respondido y cuál ha sido la respuesta?

Respuesta:

EXAMEN DE REDES LABORATORIO. SEGUNDO PARCIAL. JUNIO 2013.

Esta parte debe realizarse sin material de consulta. Puede utilizar una calculadora.

Pregunta L1 (8 puntos).

Responda en la hoja adjunta. Solo debe marcar una opción en cada pregunta; si cree que hay varias correctas debe elegir la que a su juicio mejor se ajuste a la pregunta. Lea los enunciados con atención.

Puntuación:	Bien: +1 punto	Mal: -1/3 puntos	En blanco: 0 puntos
-------------	----------------	------------------	---------------------

L.1-1Cuál de los siguientes códigos es correcto funcionalmente (sintácticamente lo son todos) para la implementación de un cliente de daytime bajo protocolo de transporte UDP.

- A)

```
if ((n=recv(sock, buf, lbuf, 0))<0)
    strncpy(buf, "Error en recv... %n", lbuf);
else
    if (n==0)
        strncpy(buf, "Timeout... %n", lbuf);
    else
        if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
            strncpy(buf, "Error en select... %n", lbuf);
        else
            buf[n]=' \0' ;
```
- B)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
    strncpy(buf, "Error en select... %n", lbuf);
else
    if ((n=recv(sock, buf, lbuf, 0))<0)
        strncpy(buf, "Error en recv... %n", lbuf);
    else
        if (n==0)
            strncpy(buf, "Timeout... %n", lbuf);
        else
            buf[n]=' \0' ;
```
- C)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
    strncpy(buf, "Error en select... %n", lbuf);
else
    if (n==0)
        strncpy(buf, "Timeout... %n", lbuf);
    else
        if ((n=recv(sock, buf, lbuf, 0))<0)
            strncpy(Error en recv... %n", lbuf);
        else
            buf[n]=' \0' ;
```
- D)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))>=0)
    strncpy(buf, "Error en select... %n", lbuf);
else
    if ((n=recv(sock, buf, lbuf, 0))<=0)
        strncpy(buf, "Timeout... %n", lbuf);
    else
        buf[n]=' \0' ;
```

- L.1-2** ¿ Que significado tiene poner un timeout en el cliente del servicio daytime bajo el protocolo de transporte TCP?
- A) El mismo significado que en UDP, que el segmento solo posee cabecera.
 - B) Que TCP funciona a veces, mientras que el UDP garantiza la entrega segura.
 - C) Ninguno, ya que no necesitamos timeout en esta práctica para daytime sobre TCP.
 - D) Que se decidió realizar de esa forma el diseño de ese programa en la práctica.
- L.1-3** En el servidor TCP para IRC se requiere la creación de un socket, señale el orden correcto de las primitivas de C/C++:
- A) socket, ioctl, bind, listen
 - B) socket, bind, ioctl, listen
 - C) socket, listen, bind, ioctl
 - D) socket, select, bind, ioctl
- L.1-4** Diga cuál de las siguientes afirmaciones es verdadera referida a la aplicación de ACLs:
- A) En cada interfaz se puede aplicar como máximo una ACL.
 - B) Se pueden aplicar tantas ACLs por interfaz como se quiera, de entrada o de salida, estándar o extendidas, sin limitación.
 - C) Con las ACL estándar no es posible filtrar paquetes por la dirección de destino.
 - D) Si se trata de ACLs estándar se pueden aplicar por interface dos como máximo, una de entrada y otra de salida. Si son ACLs extendidas no hay limitación.
- L.1-5** Suponga que tiene un router con una interfaz LAN y una WAN. La instrucción `access-list 100 deny tcp any eq www any` aplicada en la interfaz WAN al tráfico entrante:
- A) No permite el acceso a servidores FTP externos a mi LAN.
 - B) No permite que los PCs de mi LAN envíen intentos de conexión a servidores web externos.
 - C) Permite a los PCs de mi LAN intentar conectarse a servidores web externos, pero el router no dejará pasar la respuesta de estos.
 - D) No está bien escrita ya que se trata de una lista de acceso estándar y sin embargo tiene el número 100.
- L.1-6** La seguridad de LINUX se basa en 3 capas (cortafuegos, TCP wrappers y xinetd) de forma que si en la más interna (xinetd) no se habilita explícitamente ningún servicio no habrá ninguno abierto al exterior:
- A) Correcto. Poniendo `disable=yes` en todos los ficheros de configuración de xinetd todos los servicios quedarán cerrados al exterior.
 - B) Falso, ya que hay servicios que no pasan a través de xinetd.
 - C) Correcto. Si no ponemos `enable=yes` en ningún fichero de configuración todos los servicios quedarán cerrados.
 - D) Falso, ya que los TCP wrappers prevalecen sobre xinetd, de forma que aunque hayamos cerrado los servicios en xinetd los TCP wrappers pueden abrirlos.
- L.1-7** Suponga que tiene los siguientes ficheros `/etc/hosts.allow` y `/etc/hosts.deny`:

```
# Fichero /etc/hosts.allow
sshd: ALL : spawn /bin/echo "conectado" %h a las $(/bin/date)" >> /tmp/fich.txt
```

```
# Fichero /etc/hosts.deny
ALL: ALL
```

Esto significa que:

- A) El servicio SSH está totalmente inhabilitado para todos los ordenadores que no son de mi red local.
- B) El servicio SSH está deshabilitado para todos los ordenadores y además estaré registrando en un fichero la dirección IP y la hora de quien intente conectarse a mi ordenador.
- C) El servicio SSH está habilitado solo para los ordenadores de mi red de área local y además estaré registrando en un fichero la dirección IP y la hora a que se ha conectado cualquier ordenador de mi red local.
- D) El servicio SSH está habilitado para cualquier ordenador.

L.1-8 El OID no estándar 1.3.6.1.4.1.9.2.1.57.0 se usa para monitorizar el consumo de CPU de los routers de la práctica de clase. Si la OID correspondiente a la MIB-II contiene la secuencia 1.3.6.1.2.1, ¿Cómo resolvería inmediatamente el problema de monitorizar el consumo de CPU de los routers usando el `cfgmaker`?

- A) No podríamos hacerlo al no formar ese OID parte del conjunto de MIBs-II estándar.
- B) Ese OID no está asociado a ninguna interfaz del equipo. Habría que asociarlo manualmente a algún puerto estándar de la interfaz
- C) Esa variable, al no ser estándar, habría que incorporarla manualmente al fichero de configuración generado por la utilidad `cfgmaker`.
- D) Habría que modificar la versión de la utilidad `cfgmaker` que se utilizaba en la práctica ya que era antigua y este OID se ha incorporado recientemente.

L.1-9 Si quiero capturar con el wireshark el tráfico SNMP que pasa por la interfaz de mi ordenador debo utilizar el filtro:

- A) `snmp and port 80`.
- B) `tcp and port 161`
- C) `udp and port 161`
- D) `udp and port 80`

L.1-10 Si el fichero `/etc/sysconfig/iptables` contiene las siguiente líneas (los números han sido añadidos solo para numerar las líneas y no estarían en el fichero):

```
1  *filter
2  :INPUT ACCEPT [0:0]
3  :FORWARD ACCEPT [0:0]
4  :OUTPUT ACCEPT [0:0]
5  -A INPUT -i lo -j ACCEPT
6  -A INPUT -p tcp -j ACCEPT
7  -A INPUT -j REJECT
8  -A OUTPUT -o lo -j ACCEPT
9  -A OUTPUT -p tcp -j ACCEPT
10 -A OUTPUT -j REJECT
11 COMMIT
```

El comando `ping gong.uv.es`:

- A) Se ejecutará correctamente.
- B) Se ejecutará correctamente añadiendo las líneas siguientes entre la posición 4 y 5:
 - A INPUT -p udp --sport 53 --dport 1024: -j ACCEPT
 - A OUTPUT -p udp --dport 53 --sport 1024: -j ACCEPT
- C) Se ejecutará correctamente añadiendo las líneas siguientes entre la posición 4 y 5:
 - A INPUT -p udp --dport 53 --sport 1024: -j ACCEPT
 - A OUTPUT -p udp --sport 53 --dport 1024: -j ACCEPT
- D) No se ejecutará correctamente.

NOMBRE Y APELLIDOS: _____

Pregunta L 2. (2 puntos):

Dado el siguiente prototipo de una función de C/C++:

```
/* Función que acepta una conexión pendiente de aceptar y la almacena en el vector de conexiones existentes.
```

```
Parametros:  int sock    Socket bloqueante de aceptación de conexiones.
              int vector[TAM_VECTOR]  Vector con las conexiones aceptadas.
              int num     Numero de conexiones existentes.
```

```
Return:  int Número de conexiones después de ejecutar la función. */
int AceptarConexion(int sock,int vector[TAM_VECTOR],int num) ;
```

Escribir el código necesario para que la función acepte conexiones esperando un tiempo máximo de 1 milisegundo, las almacene en el vector y devuelva el valor adecuado tal y como se hizo en la práctica del servidor de IRC. Como ayuda se os proporcionan los siguientes prototipos de funciones, macros y estructuras:

```
int select(int n, fd_set *readfds, fd_set *writefds,
           fd_set *exceptfds, struct timeval *timeout);
int accept(int s, struct sockaddr *addr, int *addrlen);
```

```
FD_ZERO(fd_set *set);
FD_SET(int fd, fd_set *set);
FD_CLR(int fd, fd_set *set);
FD_ISSET(int fd, fd_set *set);
```

```
struct timeval
{
    unsigned long int tv_sec; /* Segundos */
    unsigned long int tv_usec; /* Millonésimas de segundo */
};
```

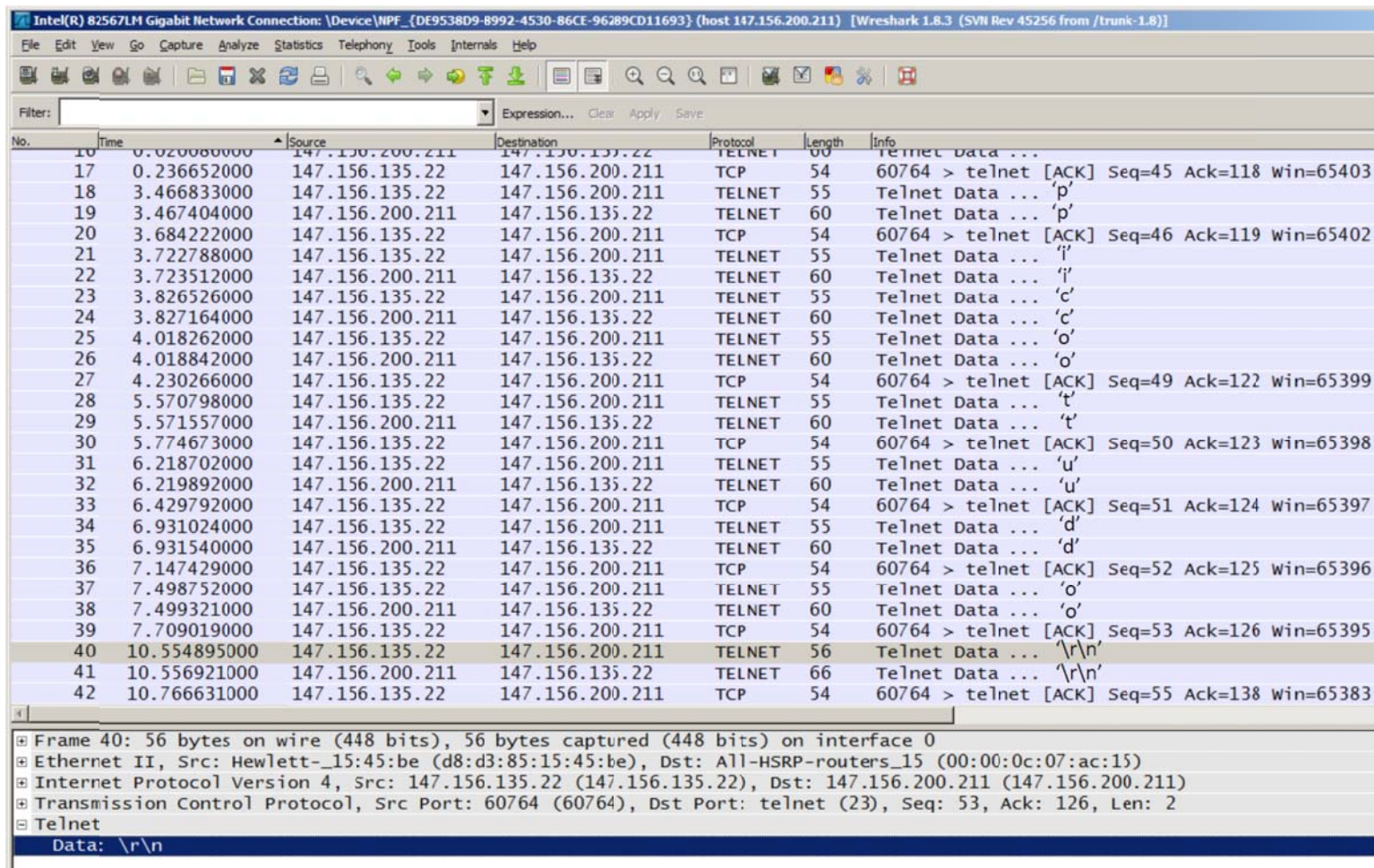
Respuesta:

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES PROBLEMAS. SEGUNDO PARCIAL. JUNIO 2013.

Problema 1 (2 puntos):

Un usuario en el ordenador 147.156.135.22 tiene una sesión telnet establecida con el ordenador 147.156.200.211. En un momento determinado escribe la palabra 'picotudo' seguida de la tecla 'Enter' (nueve teclas en total). A continuación se muestra la sesión, capturada con el programa Wireshark, donde los paquetes generados por las nueve pulsaciones son los que aparecen numerados del 18 al 42. En los paquetes de datos Telnet se ha añadido entrecomillada, en el campo 'Info', la representación en ASCII del contenido de dichos paquetes.



No.	Time	Source	Destination	Protocol	Length	Info
10	0.020000000	147.156.200.211	147.156.135.22	TCP	60	Telnet Data ...
17	0.236652000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=45 Ack=118 win=65403
18	3.466833000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'p'
19	3.467404000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'p'
20	3.684222000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=46 Ack=119 win=65402
21	3.722788000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'i'
22	3.723512000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'i'
23	3.826526000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'c'
24	3.827164000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'c'
25	4.018262000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'o'
26	4.018842000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'o'
27	4.230266000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=49 Ack=122 win=65399
28	5.570798000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 't'
29	5.571557000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 't'
30	5.774673000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=50 Ack=123 win=65398
31	6.218702000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'u'
32	6.219892000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'u'
33	6.429792000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=51 Ack=124 win=65397
34	6.931024000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'd'
35	6.931540000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'd'
36	7.147429000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=52 Ack=125 win=65396
37	7.498752000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'o'
38	7.499321000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'o'
39	7.709019000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=53 Ack=126 win=65395
40	10.554895000	147.156.135.22	147.156.200.211	TELNET	56	Telnet Data ... '\r\n'
41	10.556921000	147.156.200.211	147.156.135.22	TELNET	66	Telnet Data ... '\r\n'
42	10.766631000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=55 Ack=138 win=65383

Frame 40: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: Hewlett-15:45:be (d8:d3:85:15:45:be), Dst: All-HSRP-routers_15 (00:00:0c:07:ac:15)
Internet Protocol Version 4, Src: 147.156.135.22 (147.156.135.22), Dst: 147.156.200.211 (147.156.200.211)
Transmission Control Protocol, Src Port: 60764 (60764), Dst Port: telnet (23), Seq: 53, Ack: 126, Len: 2
Telnet
Data: \r\n

- Explique por qué aparecen dos paquetes asociados con la transmisión de cada carácter (la 'p' en 18-19, la 'i' en 21-22, etc.)
- Explique por qué algunos envíos van seguidos de ACK (18-19, 25-26, ...) y otros no (21-22, 23-24)
- Explique que indican los contadores 'Seq', 'Ack' y 'Win' que aparecen en los paquetes ACK y porque evolucionan de esa manera
- Explique qué se transmite en los paquetes 40 y 41
- Calcule, con la información disponible, el valor medio del RTT para esta conexión TCP. Se supone que tanto el cliente como el servidor tienen sobrados recursos de CPU y memoria, por lo que el tiempo de proceso de la aplicación telnet en los hosts es despreciable.

Respuesta: _____

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES PROBLEMAS. SEGUNDO PARCIAL. JUNIO 2013.

Problema 2 (2 puntos):

El usuario A le envía al usuario B un mensaje P en texto plano (sin encriptar). Además A calcula el hash del mensaje P y luego lo encripta con la clave pública de B y también se lo envía. Es decir que A le envía a B lo siguiente:

P
 $E_B(\text{hash}(P))$

- a.- ¿Para qué sirve esto? ¿Qué puede hacer B con la información recibida?
- b.- El usuario B, ¿estará seguro que la información le ha llegado desde el usuario A?
- c.- Si el mensaje lo recibe o captura otra persona que no sea B, ¿qué podrá hacer con el mensaje?
- d.- Y si A en lugar de enviar la segunda parte envía además del mensaje P, encriptado con su clave privada lo siguiente: $D_A(E_B(\text{hash}(P)))$, ¿qué ha cambiado?

Respuesta:

EXAMEN DE REDES TEORÍA. FINAL. JUNIO 2013.

Esta parte debe realizarse sin material de consulta. Puede utilizar una calculadora.

1 Pregunta 1 (4 puntos):

Responda en la hoja adjunta. Solo debe marcar una opción en cada pregunta; si cree que hay varias correctas debe elegir la que a su juicio mejor se ajuste a la pregunta. Lea los enunciados con atención.

Puntuación: Bien: 1 punto Mal: -1/3 puntos En blanco: 0 puntos

- 1.1** ¿Qué ventaja supone utilizar en las tramas un CRC de 32 bits frente a uno de 16?
- A) La probabilidad de que se produzcan errores de transmisión en el medio físico es menor
 - B) La probabilidad de que los errores del medio físico pasen desapercibidos es menor
 - C) La carga útil de los paquetes es mayor
 - D) El caudal útil de datos transmitidos (en Mb/s por ejemplo) es mayor
- 1.2** Qué hace un conmutador LAN (que no tiene configuradas VLANs) cuando recibe tráfico multicast?
- A) Lo descarta
 - B) Lo envía por todas las interfaces activas, excepto aquella por la que le llegó.
 - C) Lo envía por todas las interfaces activas que tienen activado el spanning tree, excepto aquella por la que le llegó.
 - D) Lo envía por todas las interfaces activas que tienen desactivado el spanning tree, excepto aquella por la que le llegó.
- 1.3** ¿Qué campo de la cabecera Ethernet utilizan los puentes transparentes para construir la tabla CAM?:
- A) La dirección de origen
 - B) La dirección de destino
 - C) El protocolo o 'Ethertype'
 - D) La longitud
- 1.4** ¿Qué ocurre si utilizamos el protocolo spanning-tree en una red de conmutadores que no tiene bucles?
- A) El protocolo funciona normalmente, pero al no haber bucles no se bloquea ningún puerto.
 - B) Al no haber bucles no se puede elegir el puente raíz y el protocolo se desactiva automáticamente, por lo que no se envían BPDUs
 - C) Sin spanning tree no hay tráfico, ya que es el protocolo que se encarga de establecer la ruta que siguen las tramas por la red
 - D) Al no haber bucles spanning tree asocia el mismo costo a todos los puertos independientemente de su velocidad, ya que solo hay una ruta posible a cada destino
- 1.5** Se han interconectado cinco conmutadores (sin VLANs) con seis cables en una topología que desconocemos. Los cinco tienen activado el spanning tree. Se desconoce el número de interfaces de cada uno ¿Cuántos puertos se desactivan?
- A) Uno
 - B) Dos
 - C) Tres
 - D) No hay suficientes datos para responder a la pregunta
- 1.6** El principio de optimalidad establece que:
- A) La ruta óptima A->B es igual a la ruta óptima B->A
 - B) La ruta óptima A->C es la unión de las rutas óptimas A->B y B->C
 - C) Si B está en la ruta óptima A->C entonces la ruta óptima B->C está incluida en la ruta óptima A->C
 - D) Siempre existe una y sólo una ruta óptima A->B
- 1.7** Una línea de 2048 Kb/s tiene una ocupación media del 50%. Su tiempo de servicio será equivalente al de una línea sin tráfico de:
- A) 64 Kb/s
 - B) 1024 Kb/s
 - C) 1536 Kb/s
 - D) 1984 Kb/s

- 1.8** ¿Cuál de los campos siguientes no se modifica nunca en la cabecera de un datagrama IP cuando pasa por un router?
- A) TTL (Time To Live)
 - B) Protocolo
 - C) Checksum
 - D) Ninguno de los anteriores (es decir, se modifican los tres)
- 1.9** Diga cuál de las siguientes afirmaciones es verdadera referida a los mensajes 'ICMP Time Exceeded' que provoca el comando 'traceroute':
- A) Las IPs de origen y de destino son siempre las mismas en todos los comandos ICMP Time Exceeded generados por una invocación del comando traceroute
 - B) La IP de origen es la misma en todos, pero la IP de destino va cambiando
 - C) La IP de origen va cambiando, pero la IP de destino es siempre la misma
 - D) Tanto la IP de origen como la de destino van cambiando
- 1.10** ¿Cuál de las siguientes combinaciones puede darse en una tabla ARP cache?
- A) A una misma MAC le pueden corresponder varias IPs
 - B) A una misma IP le pueden corresponder varias MACs
 - C) A y B, es decir a una MAC le pueden corresponder varias IPs y viceversa
 - D) La correspondencia es biunívoca, es decir a cada MAC solo le puede corresponder una IP y viceversa
- 1.11** ¿Cuál de los siguientes campos de la cabecera IP podría suprimirse sin que por ello se viera afectado el mecanismo de fragmentación de IP?
- A) Identificación
 - B) DF (Don't Fragment)
 - C) MF (More Fragments)
 - D) Fragment Offset
- 1.12** Un host tiene la dirección 130.206.90.15 con máscara 255.255.224.0 ¿Cuál de las siguientes no sería una dirección válida para su router por defecto?
- A) 130.206.89.255
 - B) 130.206.99.255
 - C) 130.206.65.0
 - D) 130.206.76.255
- 1.13** Cuando se envía un 'BOOTP Request' de un cliente a un servidor remoto a través de un 'BOOTP Relay Agent' el mensaje se envía en modo broadcast:
- A) Solo en la LAN del cliente
 - B) En la LAN del cliente y en la del servidor, pero no en las intermedias
 - C) En todas las LANs por las que pasa el cliente, incluidas la del cliente y la del servidor
 - D) Solo en la LAN del cliente, y no siempre, Algunas implementaciones envían el BOOTP Request en broadcast y otras en unicast
- 1.14** Suponiendo que podemos observar todo el tráfico en una red ¿Cómo podríamos detectar que se está produciendo el ataque del servidor DHCP furtivo?:
- A) Porque todos los DHCP Reply provienen del mismo servidor
 - B) Porque un DHCP Request recibe dos o más DHCP Reply de servidores diferentes, con distinta información
 - C) Porque un DHCP Request no recibe ningún DHCP Reply
 - D) Porque los DHCP Reply se envían a la dirección broadcast
- 1.15** Si tuvieras que elegir un protocolo de routing moderno y estándar, para utilizar dentro de un sistema autónomo ¿Cuál elegirías?:
- A) EIGRP
 - B) RIP
 - C) OSPF
 - D) BGP

- 1.16** ¿Cuál de las rutas que aparecen a continuación se utilizaría para enviar un paquete cuya IP de destino fuera la 30.1.1.160?:
- A) A 30.1.0.0 255.255.254.0 métrica 347 d.a. 110
 - B) A 30.1.0.0 255.255.255.0 métrica 568 d.a. 120
 - C) A 30.1.0.0 255.255.255.128 métrica 427 d.a. 120
 - D) A 30.1.0.0 255.255.255.128 métrica 390 d.a. 120
- 1.17** ¿Cuál de las siguientes características de IPv6 no estaba presente en IPv4?
- A) La posibilidad de comprobar, mediante el CRC de la trama a nivel 2, que no ha habido errores en la transmisión de los paquetes por los cables
 - B) La posibilidad de asignar la dirección de red automáticamente a partir de la dirección MAC
 - C) La posibilidad de limitar el número máximo de saltos que un paquete da por la red
 - D) La posibilidad de fragmentar los paquetes
- 1.18** Las siglas RFC corresponden a:
- A) Routing First Copy: un protocolo de routing, hoy en desuso, utilizado inicialmente en la Internet
 - B) Request For Comments: la denominación que se utiliza para referirse a los documentos oficiales de Internet
 - C) Return Forward Channel: un mecanismo de devolución de mensajes de error cuando no hay ninguna ruta utilizable
 - D) Repeat For Clarity: Procedimiento seguido por algunos protocolos de routing cuando un comando es ambiguo
- 1.19** Un ordenador tiene un servidor web activo y un puerto en modo listen. ¿Cuántos clientes se pueden conectar a él?
- A) Uno
 - B) 64511
 - C) 65535
 - D) Ilimitado (es decir la limitación, si la hay, vendrá impuesta por factores ajenos)
- 1.20** ¿Qué flags llevan puestos los tres mensajes que normalmente se intercambian en el saludo a tres vías de TCP?:
- A) El primero SYN, el segundo ACK y el tercero ACK
 - B) El primero SYN y ACK, el segundo SYN y el tercero ACK
 - C) El primero SYN, el segundo SYN y ACK, el tercero ACK
 - D) El primero SYN y ACK, el segundo SYN y ACK, el tercero ACK
- 1.21** ¿Qué debe hacer TCP si recibe un segmento duplicado?
- A) Debe descartarlo y no hacer nada más
 - B) Debe descartarlo y enviar el ACK correspondiente al emisor
 - C) Debe pasarlo al buffer de la aplicación y enviar el ACK correspondiente al emisor
 - D) Debe pasarlo al buffer de la aplicación y no hacer nada más
- 1.22** ¿Qué ocurre cuando al enviar varios datagramas UDP a un mismo puerto y una misma dirección IP de destino la red los entrega en un orden distinto al de salida?
- A) El nivel IP en el receptor los reordena y los entrega en el orden correcto al nivel UDP
 - B) El nivel UDP en el receptor los reordena y los entrega en el orden correcto al proceso del nivel de aplicación que está escuchando en ese puerto.
 - C) El nivel UDP en el receptor los entrega desordenados al proceso que está escuchando en ese puerto.
 - D) Esto no puede ocurrir ya que en UDP siempre se respeta el orden de los datagramas.
- 1.23** ¿Para qué sirve el ‘factor de escala’, que se negocia en algunas conexiones TCP?
- A) Para que se pueda tener más datos pendientes de confirmación por parte del receptor, mejorando el rendimiento en redes con elevado caudal y elevado retardo
 - B) Para que se puedan enviar segmentos mayores de 64 KBytes, mejorando el rendimiento en todo tipo de redes
 - C) A y B
 - D) Para poder enviar segmentos mayores que la MTU del trayecto.

- 1.24** En una red local tenemos 500 ordenadores con direcciones privadas que queremos que tengan salida a Internet, para lo cual disponemos de una única IP pública. Sabemos que nunca más del 20% estarán conectados simultáneamente y que las conexiones siempre se iniciarán desde la red privada. ¿Qué tipo de NAT debemos utilizar?
- A) NAT básico estático
 - B) NAT básico dinámico
 - C) NAT básico estático
 - D) NAT básico dinámico
- 1.25** Si estoy en un ordenador de laboratorio de la Universidad de Valencia y me conecto a la página web www.google.com capturaré los siguientes tipos de paquetes (sin importar el orden)
- A) TCP, UDP
 - B) TCP, ICMP
 - C) UDP, ICMP
 - D) ICMP, DNS
- 1.26** ¿Cuál es la utilidad de la codificación MIME Entrecomillada Imprimible?
- A) Poder trabajar en formato hexadecimal y agrupar los bits de datos en bytes
 - B) Poder enviar mensajes que tienen unos pocos caracteres no ASCII puros con bastante ahorro de ancho de banda
 - C) Poder enviar cualquier tipo de byte a través de una red pensada para enviar hasta agrupaciones de 7 bits
 - D) Poder enviar mensajes de texto puro (ASCII 7) como adjunto a un correo electrónico
- 1.27** ¿Para qué sirve SNMP?
- A) SNMP permite gestionar vía UDP cada dispositivo de una red recibiendo información de una base de datos MIB con un formato SMI
 - B) SNMP es un protocolo orientado al dispositivo y enviará información vía TCP de cada dispositivo a la estación desde la que se administra el dispositivo, mostrándose estadísticas de uso de puertos e interfaces
 - C) SNMP permite gestionar vía UDP la información de alarmas o interrupciones TRAP y vía TCP haciendo sondeos (o pooling) de diferentes dispositivos de una red
 - D) SNMP está orientado al dispositivo y la información generada nunca se guarda en él, sino que cada vez que se genera un cambio (por ejemplo en una interfaz de un router) se envía mediante un "demonio" a una estación administradora
- 1.28** ¿Cuál es la primera información que envía un servidor SSH a un cliente la primera vez que se conecta a él?
- A) El compendio del password (en SHA-1 o MD-5) que es modificado con el password del cliente
 - B) Un certificado donde el cliente podrá poner su password y devolver al servidor
 - C) La clave pública del servidor
 - D) La clave simétrica de sesión que deberá usarse durante toda la comunicación para encriptar los mensajes
- 1.29** Si A envía a B un mensaje encriptado con la clave pública de B:
- A) B está seguro que el mensaje lo ha enviado A
 - B) B está seguro que el mensaje no ha podido modificarse por el camino
 - C) B está seguro de la confidencialidad del mensaje sin importar quién lo haya enviado
 - D) Nadie puede haber enviado este mensaje excepto el mismo B
- 1.30** Si A envía a B un mensaje encriptado con la clave privada de A:
- A) B está seguro que el mensaje lo ha enviado A y nadie más podrá ver el contenido
 - B) B está seguro que el mensaje lo ha enviado A pero cualquiera que esté escuchando el canal de comunicaciones podrá ver el contenido usando la clave pública de A
 - C) Cualquiera puede haber enviado el mensaje
 - D) Esto se usa para guardar de forma local (o remota) la información encriptada y solo el usuario A podrá desencriptarla

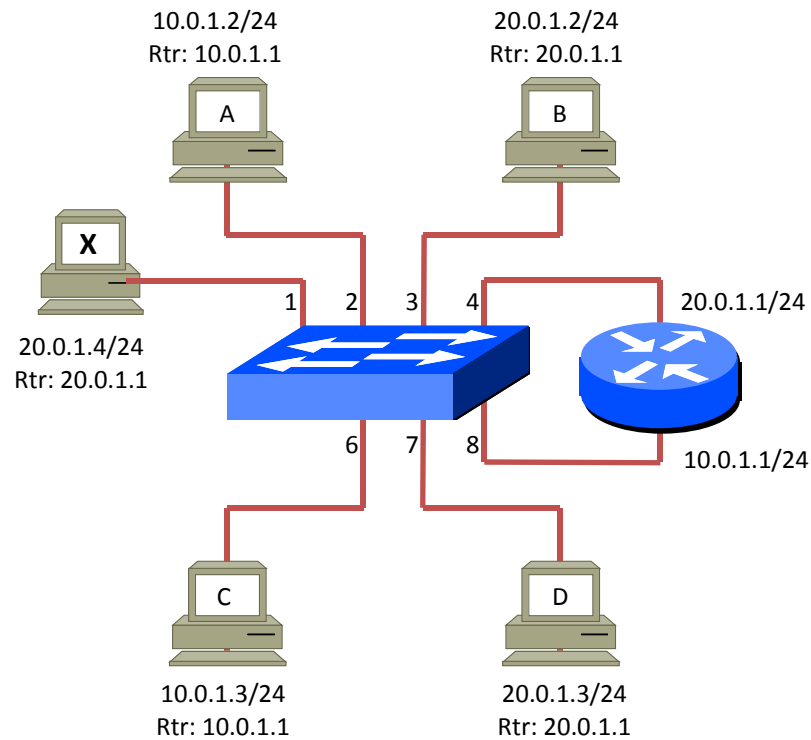
- 1.31** Si A envía a B un mensaje encriptado con la clave pública de A:
- A) B no podrá hacer nada con el mensaje, cualquiera podrá haber enviado el mensaje y solo A podrá desencriptarlo
 - B) B no podrá modificar el mensaje pero está seguro que solo A lo puede haber enviado y por lo tanto lo podrá usar como prueba (firma)
 - C) B no podrá modificar el mensaje pero está seguro que viene de A y por lo tanto se trata de una prueba de no repudio
 - D) B no podrá modificar el mensaje y además no está seguro que haya llegado desde A. Este mensaje lo usará B para guardar las claves públicas de todas las entidades con las que se comunica
- 1.32** La firma digital con clave simétrica:
- A) Solamente se puede usar cuando son muchas las entidades que tienen que comunicarse entre sí para que salga rentable tener un centro de distribución de claves
 - B) Solamente se puede usar en sistemas en los que se disponga de tiempo suficiente para realizar todas las fases de encriptado y desencriptado
 - C) No permite comprobar la integridad del contenido de la comunicación
 - D) Necesita una autoridad donde se depositan todas las claves o que la clave haya sido enviada previamente a la entidad con la que me quiero comunicar

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES TEORÍA. FINAL. JUNIO 2013

Pregunta 2.1 (1 punto):

En la red de la figura adjunta:



se está ejecutando en el ordenador X el programa Wireshark, que captura paquetes en modo promiscuo. A continuación se enciende el router, los conmutadores y los ordenadores, y en el ordenador A se ejecuta el comando:

```
ping -n -c 1 20.0.1.2
```

que recibe un paquete de respuesta.

La red utiliza ARP. El conmutador tiene activado SpanningTree. No hay configuradas VLANs.

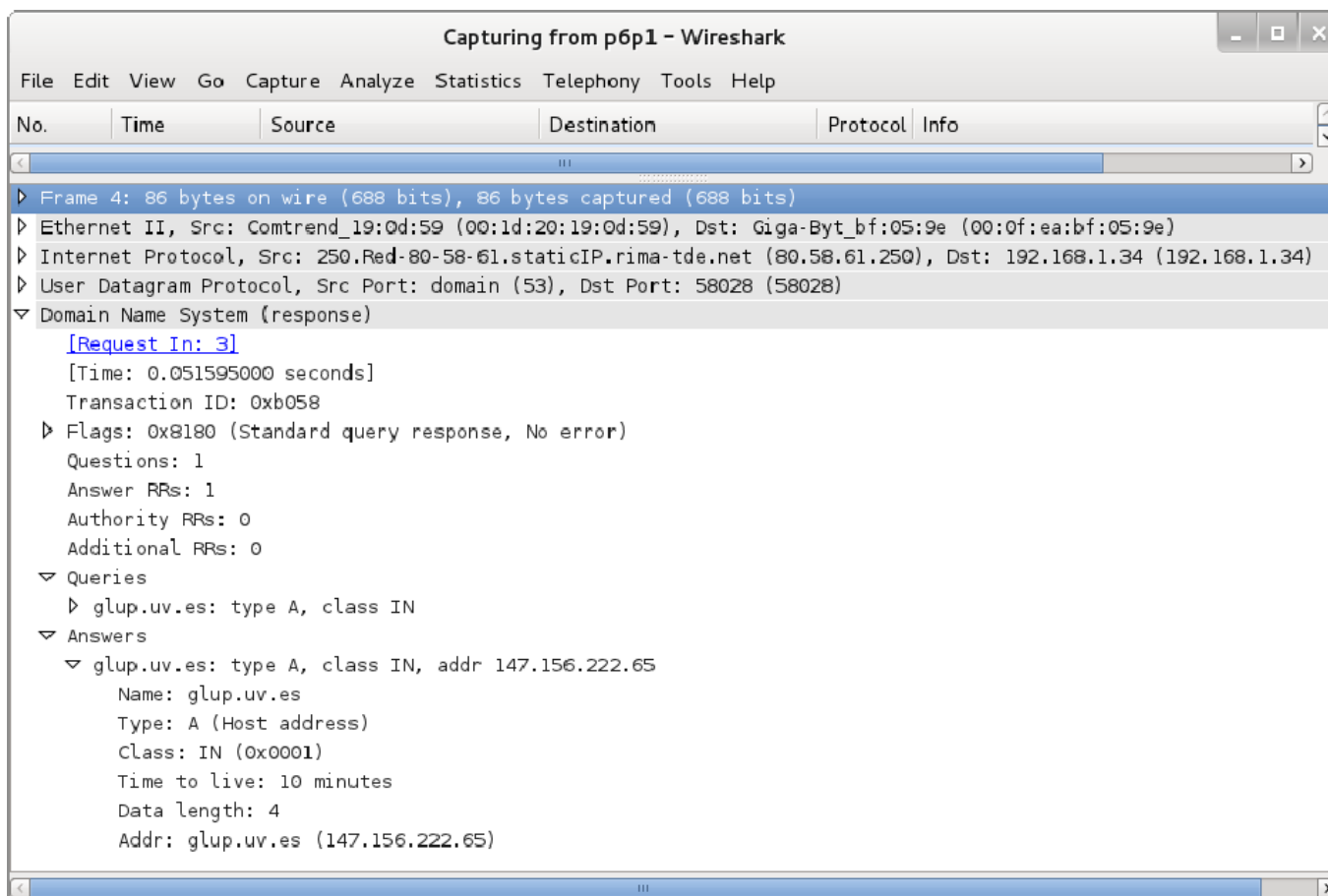
Diga cuantos paquetes se capturan en X y describa brevemente su contenido. Explique su respuesta.

Respuesta:

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES TEORÍA. FINAL. JUNIO 2013.

Pregunta 2.2 (1 punto) Sin apuntes:



Responde a las siguientes preguntas:

- ¿De qué se trata la captura anterior?
- ¿Quién ha preguntado y qué ha preguntado?
- ¿Quién ha respondido y cuál ha sido la respuesta?

Respuesta:

EXAMEN DE REDES LABORATORIO. FINAL. JUNIO 2013.

Pregunta L1 (6 puntos). Responda en la hoja adjunta.

Puntuación: Bien: 1 punto Mal: -1/3 puntos En blanco: 0 puntos

L.1-1 En la práctica de conmutadores, al configurarlos les ponemos a cada uno una dirección IP. El objetivo de esto es:

- A) Reducir el dominio de broadcast y que haya menos colisiones en la red
- B) Que el Spanning Tree pueda establecer cuál es el conmutador raíz
- C) Que podamos hacerle ping o que nos podamos conectar al conmutador desde cualquier ordenador usando telnet o http
- D) Poder configurar esa dirección IP como router por defecto en los hosts

L.1-2 Si las entradas en la tabla CAM no caducaran nunca:

- A) Se podrían perder tramas cuando cambiamos un ordenador del puerto en el que fue conectado inicialmente
- B) No haría falta enviar por inundación las tramas broadcast
- C) Los conmutadores no podrían auto-negociar la velocidad ni el modo dúplex
- D) El Spanning tree no podría establecer cuál es el conmutador raíz

L.1-3 El comando 'Bandwidth' utilizado en algunas interfaces durante la práctica de routers sirve para:

- A) Establecer la señal de reloj y con ello la velocidad real de transmisión de los datos; si se modifica su valor se modifica la velocidad de transmisión
- B) Calcular el costo de la interfaz para los cálculos de rutas del protocolo de routing OSPF
- C) A y B, es decir para establecer la señal de reloj y calcular el costo de la interfaz
- D) Solo tiene efectos documentales, para indicar la velocidad teórica de la interfaz

L.1-4 En la práctica de routers hay un momento en que tecleamos un comando como el siguiente (en RP por ejemplo):

```
RP(config)#IP ROute 10.0.2.0 255.255.255.0 10.0.4.2 200
```

El valor 200 que aparece al final del comando establece:

- A) La distancia administrativa
- B) El ancho de banda
- C) La métrica
- D) El costo

L.1-5 ¿Para qué sirve el modo promiscuo en el Wireshark?:

- A) Para capturar y analizar el tráfico broadcast que llega a nuestra interfaz LAN
- B) Para poder inspeccionar en detalle el contenido de los paquetes capturados por la interfaz LAN
- C) Para indicar al conmutador LAN que nos envíe todo el tráfico que le llegue, sin filtrar nada
- D) Para capturar y analizar todo el tráfico que llega a nuestra interfaz LAN, aunque no vaya dirigido a ella

L.1-6Cuál de los siguientes códigos es correcto funcionalmente (sintácticamente lo son todos) para la implementación de un cliente de daytime bajo protocolo de transporte UDP.

- A)

```
if ((n=recv(sock, buf, lbuf, 0))<0)
    strncpy(buf, " Error en recv... %n", lbuf);
else
    if (n==0)
        strncpy(buf, " Timeout... %n", lbuf);
    else
        if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
            strncpy(buf, " Error en select... %n", lbuf);
        else
            buf[n]=' %0' ;
```
- B)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
    strncpy(buf, " Error en select... %n", lbuf);
else
    if ((n=recv(sock, buf, lbuf, 0))<0)
        strncpy(buf, " Error en recv... %n", lbuf);
    else
        if (n==0)
            strncpy(buf, " Timeout... %n", lbuf);
        else
            buf[n]=' %0' ;
```
- C)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))<0)
    strncpy(buf, " Error en select... %n", lbuf);
else
    if (n==0)
        strncpy(buf, " Timeout... %n", lbuf);
    else
        if ((n=recv(sock, buf, lbuf, 0))<0)
            strncpy(buf, " Error en recv... %n", lbuf);
        else
            buf[n]=' %0' ;
```
- D)

```
if ((n=select(sock+1, &conjunto, NULL, NULL, &timeout))>=0)
    strncpy(buf, " Error en select... %n", lbuf);
else
    if ((n=recv(sock, buf, lbuf, 0))<=0)
        strncpy(buf, " Timeout... %n", lbuf);
    else
        buf[n]=' %0' ;
```

L.1-7 ¿ Que significado tiene poner un timeout en el cliente del servicio daytime bajo el protocolo de transporte TCP?

- A) El mismo significado que en UDP, que el segmento solo posee cabecera.
- B) Que TCP funciona a veces, mientras que el UDP garantiza la entrega segura.
- C) Ninguno, ya que no necesitamos timeout en esta práctica para daytime sobre TCP.
- D) Que se decidió realizar de esa forma el diseño de ese programa en la práctica.

L.1-8 En el servidor TCP para IRC se requiere la creación de un socket, señale el orden correcto de las primitivas de C/C++:

- A) socket, ioctl, bind, listen
- B) socket, bind, ioctl, listen
- C) socket, listen, bind, ioctl

D) socket, select, bind, ioctl

L.1-9 Diga cuál de las siguientes afirmaciones es verdadera referida a la aplicación de ACLs:

- A) En cada interfaz se puede aplicar como máximo una ACL.
- B) Se pueden aplicar tantas ACLs por interfaz como se quiera, de entrada o de salida, estándar o extendidas, sin limitación.
- C) Con las ACL estándar no es posible filtrar paquetes por la dirección de destino.
- D) Si se trata de ACLs estándar se pueden aplicar por interfaz dos como máximo, una de entrada y otra de salida. Si son ACLs extendidas no hay limitación.

L.1-10 Suponga que tiene un router con una interfaz LAN y una WAN. La instrucción `access-list 100 deny tcp any eq www any` aplicada en la interfaz WAN al tráfico entrante:

- A) No permite el acceso a servidores FTP externos a mi LAN.
- B) No permite que los PCs de mi LAN envíen intentos de conexión a servidores web externos.
- C) Permite a los PCs de mi LAN intentar conectarse a servidores web externos, pero el router no dejará pasar la respuesta de estos.
- D) No está bien escrita ya que se trata de una lista de acceso estándar y sin embargo tiene el número 100.

L.1-11 La seguridad de LINUX se basa en 3 capas (cortafuegos, TCP wrappers y xinetd) de forma que si en la más interna (xinetd) no se habilita explícitamente ningún servicio no habrá ninguno abierto al exterior:

- A) Correcto. Poniendo `disable=yes` en todos los ficheros de configuración de xinetd todos los servicios quedarán cerrados al exterior.
- B) Falso, ya que hay servicios que no pasan a través de xinetd.
- C) Correcto. Si no ponemos `enable=yes` en ningún fichero de configuración todos los servicios quedarán cerrados.
- D) Falso, ya que los TCP wrappers prevalecen sobre xinetd, de forma que aunque hayamos cerrado los servicios en xinetd los TCP wrappers pueden abrirlos.

L.1-12 Suponga que tiene los siguientes ficheros `/etc/hosts.allow` y `/etc/hosts.deny`:

```
# Fichero /etc/hosts.allow
sshd: ALL : spawn /bin/echo "conectado" %h a las $(/bin/date)" >> /tmp/fich.txt
```

```
# Fichero /etc/hosts.deny
ALL: ALL
```

Esto significa que:

- A) El servicio SSH está totalmente inhabilitado para todos los ordenadores que no son de mi red local.
- B) El servicio SSH está deshabilitado para todos los ordenadores y además estará registrando en un fichero la dirección IP y la hora de quien intente conectarse a mi ordenador.
- C) El servicio SSH está habilitado solo para los ordenadores de mi red de área local y además estará registrando en un fichero la dirección IP y la hora a que se ha conectado cualquier ordenador de mi red local.
- D) El servicio SSH está habilitado para cualquier ordenador.

L.1-13 El OID no estándar 1.3.6.1.4.1.9.2.1.57.0 se usa para monitorizar el consumo de CPU de los routers de la práctica de clase. Si la OID correspondiente a la MIB-II contiene la secuencia 1.3.6.1.2.1, ¿Cómo resolvería inmediatamente el problema de monitorizar el consumo de CPU de los routers usando el `cfgmaker`?

- A) No podríamos hacerlo al no formar ese OID parte del conjunto de MIBs-II estándar.
- B) Ese OID no está asociado a ninguna interfaz del equipo. Habría que asociarlo manualmente a algún puerto estándar de la interfaz.
- C) Esa variable, al no ser estándar, habría que incorporarla manualmente al fichero de configuración generado por la utilidad `cfgmaker`.
- D) Habría que modificar la versión de la utilidad `cfgmaker` que se utilizaba en la práctica ya que era antigua y este OID se ha incorporado recientemente.

L.1-14 Si quiero capturar con el wireshark el tráfico SNMP que pasa por la interfaz de mi ordenador debo utilizar el filtro:

- A) snmp and port 80.
- B) tcp and port 161
- C) udp and port 161
- D) udp and port 80

L.1-15 Si el fichero `/etc/sysconfig/iptables` contiene las siguiente líneas (los números han sido añadidos solo para numerar las líneas y no estarían en el fichero):

```
1 *filter
2 :INPUT ACCEPT [0:0]
3 :FORWARD ACCEPT [0:0]
4 :OUTPUT ACCEPT [0:0]
5 -A INPUT -i lo -j ACCEPT
6 -A INPUT -p tcp -j ACCEPT
7 -A INPUT -j REJECT
8 -A OUTPUT -o lo -j ACCEPT
9 -A OUTPUT -p tcp -j ACCEPT
10 -A OUTPUT -j REJECT
11 COMMIT
```

El comando `ping gong.uv.es`:

- A) Se ejecutará correctamente.
- B) Se ejecutará correctamente añadiendo las líneas siguientes entre la posición 4 y 5:
 - A INPUT -p udp --sport 53 --dport 1024: -j ACCEPT
 - A OUTPUT -p udp --dport 53 --sport 1024: -j ACCEPT
- C) Se ejecutará correctamente añadiendo las líneas siguientes entre la posición 4 y 5:
 - A INPUT -p udp --dport 53 --sport 1024: -j ACCEPT
 - A OUTPUT -p udp --sport 53 --dport 1024: -j ACCEPT
- D) No se ejecutará correctamente.

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES LABORATORIO. FINAL. JUNIO 2013

Pregunta L 2.1 (2 puntos):

En la práctica de routers se ejecuta en algún momento el comando 'show IP Route', obteniendo el siguiente resultado:

```
RS2#Show IP Route
...

20.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C    10.0.0.8/30 is directly connected, serial1
C    20.0.3.0/24 is directly connected, FastEthernet0
O    20.0.0.0/24 [110/782] via 10.0.0.5, 00:00:35, Serial0
O    20.0.2.0/24 [110/782] via 10.0.0.9, 00:00:35, Serial1
C    10.0.0.4/30 is directly connected, Serial0
O    20.0.0.0/24 [110/782] via 10.0.0.5, 00:00:35, Serial0
O    10.0.0.0/30 [110/1562] via 10.0.0.5, 00:00:35, Serial0
                        [110/1562] via 10.0.0.9, 00:00:35, Serial1
RS2#
```

Explica que son y para qué sirven los números entre corchetes que aparecen en algunas rutas (los destacados en negrita).

Respuesta:

Pregunta L 2.2 (2 puntos):

Dado el siguiente prototipo de una función de C/C++:

```
/* Función que acepta una conexión pendiente de aceptar y la almacena en el vector de conexiones existentes.
```

```
Parametros:  int sock    Socket bloqueante de aceptación de conexiones.
              int vector[TAM_VECTOR]  Vector con las conexiones aceptadas.
              int num     Numero de conexiones existentes.
```

```
Return:  int Número de conexiones después de ejecutar la función. */
int AceptarConexion(int sock,int vector[TAM_VECTOR],int num) ;
```

Escribir el código necesario para que la función acepte conexiones esperando un tiempo máximo de 1 milisegundo, las almacene en el vector y devuelva el valor adecuado tal y como se hizo en la práctica del servidor de IRC. Como ayuda se os proporcionan los siguientes prototipos de funciones, macros y estructuras:

```
int select(int n, fd_set *readfds, fd_set *writefds,
           fd_set *exceptfds, struct timeval *timeout);
int accept(int s, struct sockaddr *addr, int *addrlen);

FD_ZERO(fd_set *set);
FD_SET(int fd, fd_set *set);
FD_CLR(int fd, fd_set *set);
FD_ISSET(int fd, fd_set *set);

struct timeval
{
    unsigned long int tv_sec; /* Segundos */
    unsigned long int tv_usec; /* Millonésimas de segundo */
};
```

Respuesta:

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES PROBLEMAS. FINAL. JUNIO 2013

Problema 1 (1 punto):

Un usuario en el ordenador 147.156.135.22 tiene una sesión telnet establecida con el ordenador 147.156.200.211. En un momento determinado escribe la palabra 'picotudo' seguida de la tecla 'Enter' (nueve teclas en total). A continuación se muestra la sesión, capturada con el programa Wireshark, donde los paquetes generados por las nueve pulsaciones son los que aparecen numerados del 18 al 42. En los paquetes de datos Telnet se ha añadido entrecomillada, en el campo 'Info', la representación en ASCII del contenido de dichos paquetes.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.020080000	147.156.200.211	147.156.135.22	TCP	60	Telnet Data ...
17	0.236652000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=45 Ack=118 win=65403
18	3.466833000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'p'
19	3.467404000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'p'
20	3.684222000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=46 Ack=119 win=65402
21	3.722788000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'i'
22	3.723512000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'i'
23	3.826526000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'c'
24	3.827164000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'c'
25	4.018262000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'o'
26	4.018842000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'o'
27	4.230266000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=49 Ack=122 win=65399
28	5.570798000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 't'
29	5.571557000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 't'
30	5.774673000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=50 Ack=123 win=65398
31	6.218702000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'u'
32	6.219892000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'u'
33	6.429792000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=51 Ack=124 win=65397
34	6.931024000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'd'
35	6.931540000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'd'
36	7.147429000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=52 Ack=125 win=65396
37	7.498752000	147.156.135.22	147.156.200.211	TELNET	55	Telnet Data ... 'o'
38	7.499321000	147.156.200.211	147.156.135.22	TELNET	60	Telnet Data ... 'o'
39	7.709019000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=53 Ack=126 win=65395
40	10.554895000	147.156.135.22	147.156.200.211	TELNET	56	Telnet Data ... '\r\n'
41	10.556921000	147.156.200.211	147.156.135.22	TELNET	66	Telnet Data ... '\r\n'
42	10.766631000	147.156.135.22	147.156.200.211	TCP	54	60764 > telnet [ACK] Seq=55 Ack=138 win=65383

Frame 40: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: Hewlett-15:45:be (d8:d3:85:15:45:be), Dst: All-HSRP-routers_15 (00:00:0c:07:ac:15)
Internet Protocol Version 4, Src: 147.156.135.22 (147.156.135.22), Dst: 147.156.200.211 (147.156.200.211)
Transmission Control Protocol, Src Port: 60764 (60764), Dst Port: telnet (23), Seq: 53, Ack: 126, Len: 2
Telnet
Data: \r\n

- Explique por qué aparecen dos paquetes asociados con la transmisión de cada carácter (la 'p' en 18-19, la 'i' en 21-22, etc.)
- Explique por qué algunos envíos van seguidos de ACK (18-19, 25-26, ...) y otros no (21-22, 23-24)
- Explique que indican los contadores 'Seq', 'Ack' y 'Win' que aparecen en los paquetes ACK y porque evolucionan de esa manera
- Explique qué se transmite en los paquetes 40 y 41
- Calcule, con la información disponible, el valor medio del RTT para esta conexión TCP. Se supone que tanto el cliente como el servidor tienen sobrados recursos de CPU y memoria, por lo que el tiempo de proceso de la aplicación telnet en los hosts es despreciable.

Respuesta: _____

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES PROBLEMAS. FINAL. JUNIO 2013.

Problema 2 (1 punto):

El usuario A le envía al usuario B un mensaje P en texto plano (sin encriptar). Además A calcula el hash del mensaje P y luego lo encripta con la clave pública de B y también se lo envía. Es decir que A le envía a B lo siguiente:

P
 $E_B(\text{hash}(P))$

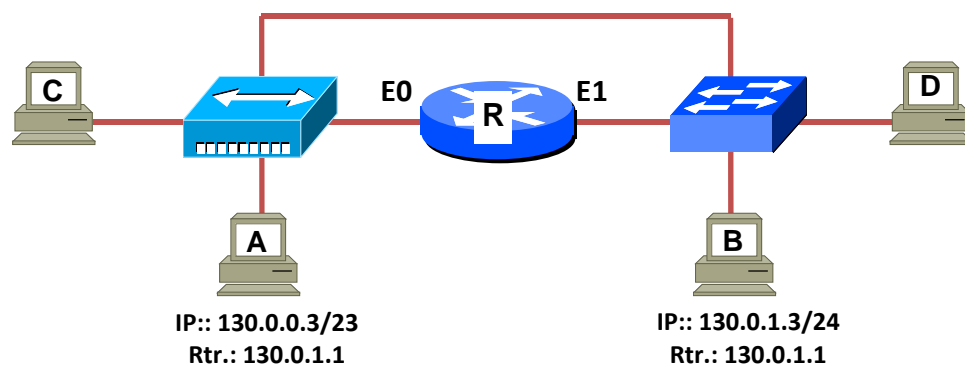
- a.- ¿Para qué sirve esto? ¿Qué puede hacer B con la información recibida?
- b.- El usuario B, ¿estará seguro que la información le ha llegado desde el usuario A?
- c.- Si el mensaje lo recibe o captura otra persona que no sea B, ¿qué podrá hacer con el mensaje?
- d.- Y si A en lugar de enviar la segunda parte envía además del mensaje P, encriptado con su clave privada lo siguiente: $D_A(E_B(\text{hash}(P)))$, ¿qué ha cambiado?

NOMBRE Y APELLIDOS: _____

EXAMEN DE REDES PROBLEMAS. FINAL. JUNIO 2013.

Problema 3 (2 puntos):

En la red de la siguiente figura:



Tenemos como puede verse los ordenadores A y C conectados a un hub y B y D a un switch.

El hub y el switch no tienen ninguna configuración. Tampoco la tienen los ordenadores C y D, que se utilizan únicamente para monitorizar el tráfico de la red mediante el programa Wireshark actuando en modo promiscuo.

Los ordenadores A y B tienen la configuración mostrada en la figura. Desconocemos que configuración tiene el router R, aunque sabemos que cada interfaz tiene una dirección IP con una máscara /24.

En un momento determinado, no habiendo ningún otro tráfico en la red, A envía un paquete ping a la dirección 130.0.1.3 y recibe una respuesta. Entretanto C ha capturado nueve paquetes y D tres.

Rellene la tabla siguiente indicando el contenido de cada una de las tramas emitidas en la red. Indique cuales de dichas tramas son capturadas por C, y cuales por D. Indique una posible configuración del router R que sea coherente con los resultados observados.

Num. Paq.	MAC origen	MAC destino	Ethertype	Contenido paquete
1				
2				
3				
4				
5				
6				
7				
8				
9				
...				
...				

